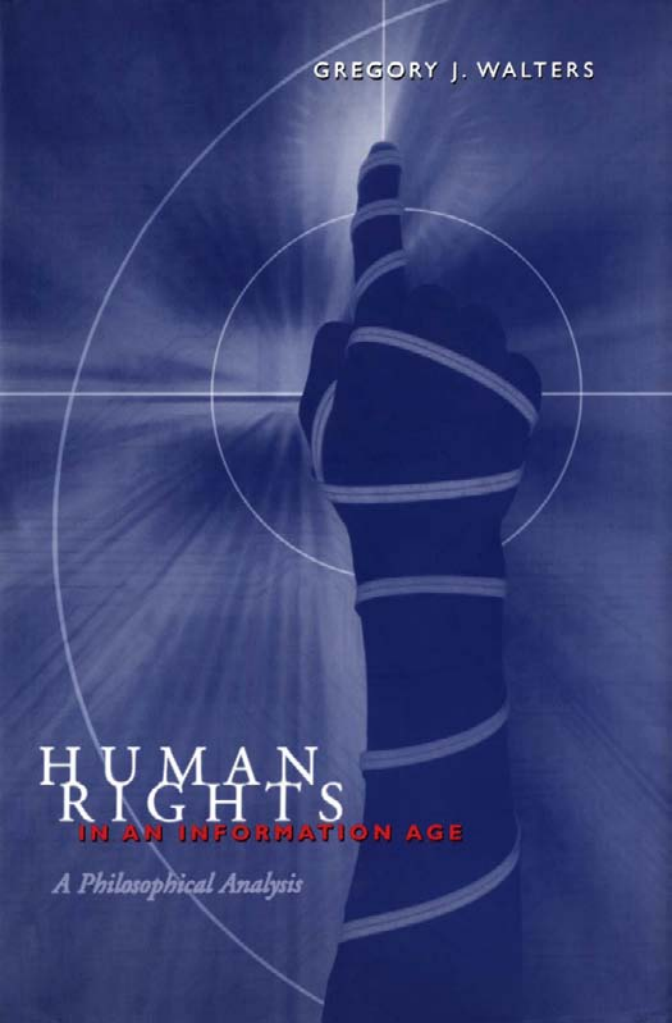
GREGORY J. WALTERS
HUMAN RIGHTS
IN AN INFORMATION AGE
A Philosophical Analysis

HUMAN RIGHTS IN AN INFORMATION AGE
A Philosophical Analysis

This page intentionally left blank

Human Rights in an Information Age

A Philosophical Analysis

GREGORY J. WALTERS

UNIVERSITY OF TORONTO PRESS
Toronto Buffalo London

www.utppublishing.com

Toronto Buffalo London

Printed in Canada

ISBN 0-8020-3583-3

Printed on acid-free paper

National Library of Canada Cataloguing in Publication Data

Walters, Gregory J. (Gregory John), 1956–
Human rights in an information age : a philosophical analysis

Includes bibliographical references and index.
ISBN 0-8020-3583-3

1. Information society. 2. Information technology – Social aspects. 3. Human rights – Moral and ethical aspects. 4. Human rights – Philosophy. I. Title.

HM851.W34 2001 303.48'23 C2001-930510-9

This book has been published with the help of a grant from the Humanities and Social Sciences Federation of Canada, using funds provided by the Social Sciences and Humanities Research Council of Canada.

The University of Toronto Press acknowledges the financial assistance to its publishing program of the Canada Council for the Arts and the Ontario Arts Council.

University of Toronto Press acknowledges the financial support for its publishing activities of the Government of Canada through the Book Publishing Industry Development Program (BPIDP).

In Loving Memory

Clarence Joseph Walters
6 April 1925 – 6 November 1998

This page intentionally left blank

Contents

This page intentionally left blank

Foreword

It has become a commonplace that ours is an age of technological revolution. The unprecedented development of means of communication and knowledge has forced a drastic reorientation of the ways in which contemporary humans relate to the world and to one another. Francis Bacon's thesis that knowledge is power has received superlative exemplification in the enormous power that information technology has given human beings. This power is at once physical, intellectual, and political, and the individuals and groups who use it for their own purposes represent drastic challenges to our moral and political heritage.

It is a great merit of Gregory J. Walters's magisterial treatise that these challenges are analysed comprehensively and cogently. For this purpose he makes critical and perceptive use of the arsenal of moral philosophy. The information revolution raises deep problems for democracy and human rights. Professor Walters calls emphatic attention to these problems; but, far from adopting a neutral or non-committal stance, he goes beyond reportage and description, valuable as these are, to take a morally committed position both on the sources of the problems and on the morally justified ways of dealing with them.

Critics have sometimes complained that the idea of human rights has been overworked; they have urged 'quality control' regarding the conditions that have been held to be objects of human rights. In boldly invoking human rights in his critique of the contemporary developments of information technology, Walters shows himself to be aware of these criticisms while at the same time providing abundant validation for his own appeals to human rights. Technological developments pose severe threats to autonomy, privacy, and the physical and economic

preconditions of human well-being; they exacerbate the class divisions whereby a minority prospers while vast numbers of humans suffer from poverty and its pervasive consequences. Walters shows, with both compassion and analytic insight, how, in order to deal with these disasters, appeals must be made to the full panoply of human rights: political, civil, economic, social and cultural.

Walters's ambitious book provides an unusual and fascinating combination of empirical and ethical analysis. He shows himself to be thoroughly familiar with developments like the Canadian 'information highway' that contribute to setting the deep ethical problems of our era. He attacks those problems both directly and profoundly by showing how the human rights framework can be decisively relevant to morally enlightened ways of dealing with them. All who read this book will come away from it with a deepened appreciation and understanding of the central structure and problems of our modern society.

Alan Gewirth
Edward Carson Waller Distinguished Service Professor of Philosophy, University of Chicago

Acknowledgments

This work has been six years in the making. I wish to thank the Saint Paul University Research Council, which generously provided grants for earlier related projects on 'The Ethical Implications of the Information Highway' in 1995–96 and 'Privacy Rights and New Technologies in Canada' in 1996–97. I must acknowledge the excellent graduate research assistance of Alan Bulley, Adam DeVille, Peter Monette, Hubert Sirois, Mark Slatter, and Melissa Trono in conjunction with the Saint Paul University Ethics Centre and these two early research projects.

The bulk of the research for this book was completed during my tenure as the Gordon F. Henderson Chair holder in Human Rights at the Human Rights Research and Education Centre, University of Ottawa, in 1998. I wish to thank Professor Errol Mendes, director of the Human Rights Centre, Alan Fleichman, Human Rights Documents Specialist, and Robin Wentzell, the centre's program manager, for their collegial assistance. Jeffrey Clark, Micheline Ducharme, Anne Gabriel, Miguel Guardado, Robin Hay, Marie-Claude Langlois, Susan Lecorre, Jean-François Rioux, Saku Sri Ghanthan, Anne-Marie Traeholt, and Joaquin Zuckerberg made my sojourn at the Human Rights Centre a joy.

I was able to discuss the ideas developed herein in a variety of academic fora. Some of the material for chapter 1 was read at the annual meeting of the Society of Christian Philosophers / Société des philosophes chrétiens – Canada. Will Sweet provided invaluable feedback on my treatment of the MacIntyre-Gewirth debate and the debate between liberalism and communitarianism generally. He has been a faithful dialogue partner on the importance and philosophy of human rights for many years.

Material for chapter 3 was first read at the annual meeting of the Canadian Association for the Study of International Development (CASID) / Association canadienne d'études du développement international. An earlier and shorter version was published in the *Canadian Journal of Development Studies / Revue canadienne d'études du développement* 20, 1 (1999):1–30. Special thanks to Barry Myers, Myron Frankman, Anastassia Khouri, Sam Lanfranco, Wayne Nelles, and Thérèse Paquet-Sévigny for their engaging economic expertise and comments. Earlier versions of chapters 4 and 5 were read at the conference, 'Building a Human Rights Agenda for the 21st Century,' a celebration of the 50th anniversary of the Universal Declaration of Human Rights on Parliament Hill, Ottawa, 4–7 October 1998, and at the 'Privacy and New Technologies' Round Table held at the Twentieth World Congress of Philosophy, Boston, in August 1998. Heartfelt thanks to Valerie Steeves, Reg Whitaker, A. Wayne MacKay, and Gerald Kernerman for their 'official' and unofficial feedback at the UDHR conference and to Simon Rogerson and James Stacey Taylor, who provided both technical and philosophical feedback on emerging new technologies and conceptions of privacy at the World Congress of Philosophy.

Chapter 6 contains material from the Gordon F. Henderson Annual Lecture given at the Faculty of Law, University of Ottawa, in 1998. Academic reflection is a social and community event, and John Arquilla, Scott Bennett, A.C. Garin, Alex Gavrilovich, Brad Hicks, Jason Husiak, Jim Robbins, Andrew MacSkimming, Peter Monette, Holly Porteous, Ted Itani, LeRoy Pearce, Sean Henry, Frank Spafford, Jean-Marc Larouche, Jim Pambrun, Heather Eaton, Marita Moll, Anne Vespry, and Sonia Williams gave imaginative feedback at a time when the concept of information warfare and its ethical implications were largely unknown. An earlier version of chapter 7 was read at the meeting of the Canadian Association of Security and Intelligence Studies (CASIS) / Association canadienne pour l'étude de la sécurité et du renseignement in June 1998. The paper was reworked for the conference on 'International Relations in the Information Age,' sponsored by the Centre for Foreign Policy Studies, Dalhousie University, Halifax, N.S., in October 1998. I wish to thank Holly Porteous for her invitation to the CASIS meeting and Frank Harvey and Gregory Witol of the Centre for Foreign Policies Studies, who extended a gracious invitation to Halifax. Alan Applehans, Brian Buckley, Simon Goldsmith, Eric Leahry, Dan Middlemiss, David Mussington, Richard Reynolds, Winn Schwartau, Timothy Shaw, Sara Siebert, Doug Thomas, Ed Tummers,

Michael Vlahos, and H. Bradford Westerfield sharpened my reflections on the ethical implications of deterrence in the information age. Joan Walters provided invaluable editorial assistance and has lent loving support every step of the way.

Kurt Salamun, chair of the Institut für Philosophie, Karl Franzens Universität, and president of the Austrian Karl Jaspers Society, graciously invited me to share my empirical and ethical analyses with international scholars interested in the philosophical implications of the information age. Special thanks to Andreas Cesana, Young Do Chung, Alfons Grieder, Sawako Hanyu, Murray McLachlan, R.A. Mall, Alan Olson, Filiz Peach, Andreas Rinofner, Hans Saner, Reinhard Schulz, Harald Stelzer, Bernhard Weidmann, Rainer Wiehl, and Maria Weinhofer. Leonard Ehrlich, Edith Ehrlich, and George Pepper, co-founders of the Karl Jaspers Society of North America, have been vital conversation partners every step of the way.

Special thanks to Simon Lapointe at the Aid to Scholarly Publications Programme / Programme d'aide à l'édition savante and to Virgil Duff at the University of Toronto Press for their careful and rigorous review process. The encouragement and expertise of Virgil Duff have been crucial, and I am grateful for his commitment to showcase innovative approaches to ethics and public policy in an information age. I am exceedingly grateful to Catherine Frost, copy-editor at University of Toronto Press, who carefully edited the manuscript and saved my prose from redundancy and ambiguity in some key instances.

I owe a profound intellectual debt to Alan Gewirth, the Edward Carson Waller Distinguished Service Professor of Philosophy at the University of Chicago. His *Reason and Morality* and *The Community of Rights* are two remarkable, yet underrated, achievements of contemporary ethical theory and social-political philosophy, which vindicate the ancient adage: *οὐ πόλλὰ πολύ* (not quantity but quality). Gewirth's personal mutuality and communication have been a tremendous source of encouragement to me throughout the long formulation of this research and writing. I assume, of course, all responsibility for any errors of interpretation in the application of the principle of human rights to the ethical challenges of Canadian information highway policy, e-commerce strategy, the informational economy, privacy and security policy, and information warfare and deterrence.

This page intentionally left blank

Abbreviations

The following abbreviations and acronyms are used throughout the text, notes, and references.

APC	Association for Progressive Communications
BCCLA	British Columbia Civil Liberties Association
C^4I	Command, Control, Communications, Computer Applications and Intelligence Processing
CA	Certification authority
CAI	Commission d'accès à l'information
CAIP	Canadian Association of Internet Providers
CCTC	Closed-circuit television camera
CECS	Canadian Electronic Commerce Strategy
CFRS	Computerized Facial Recognition System
CHANGE	Charities and Non-profit Groups in Europe
CMA	Canadian Medical Association
CNTFUA	Call for a National Task Force on Universal Access
COCOM	Coordinating Committee for Multilateral Strategic Export Controls
COMINT	Communications Intelligence
CPI	Coalition for Public Information
CRTC	Canadian Radio-television and Telecommunications Commission
CSA	Canadian Standards Association
CSE	Communications Security Establishment
CSI	Computer Security Institute (San Francisco)
CSIS	Canadian Security Intelligence Service
CUSO	Canadian Services Overseas

CWC	Chemical Weapons Convention
DBK	Dominant Battle Space Knowledge
DND	Department of National Defence (Canada)
DOD	Department of Defense (U.S.A.)
DSD	Defence Signals Directorate (Australia)
EC	European Commission
EDMA	European Direct Marketing Association
EFDIM	European Federation of Direct Marketing
EM	Electronic monitoring
EP	European Parliament
EPIC	Electronic Privacy Information Center
EU	European Union
FIPA	Freedom of Information and Privacy Association
FLIR	Forward Looking Infrared Radar
GAO	Government Accounting Office (U.S.A.)
GCHQ	Government Communications Headquarters (Great Britain)
GCSB	Government Communications Security Bureau (New Zealand)
GILC	Global Internet Liberty Campaign
GOC	Government of Canada
HC	House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities / Comité Permanent des Droits de la Personne et de la Condition des Personnes Handicapées
HRDC	Human Resources Development Corporation
IC	Industry Canada / Industrie Canada
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social and Cultural Rights
ICTs	Information and communications technologies
IGC	Institute for Global Communications
IHAC	Information Highway Advisory Council
ILO	International Labour Organization
IO	Information operations
IOS	Interorganizational Systems
ISR	Intelligence, Surveillance, and Reconnaisance
IT	Information technology
ITA	Information Technology Agreement
ITAC	Information Technology Association of Canada

ITC	International Trade Commission
IW	Information warfare
I-way	Information highway
IWCF	*Information Warfare and the Canadian Forces*
IWD	Information warfare deterrence
JSTARS	Joint Surveillance Target Attack Radar System
MAD	Mutually Assured Destruction
MAID	Mutually assured information destruction
MIRV	Multiple independently retargetable re-entry vehicle
MMWD	Massive Millimeter Wave Dectector
MTR	Military technical revolution
NATO	North Atlantic Treaty Organization
NEPSSG	National Electronic Public Space Steering Group
NPHIRA	National Personal Health Information Research Act
NSA	National Security Agency (U.S.A.)
OECD	Organization for Economic Co-operation and Development
OMSGCS	Ontario Ministry of the Solicitor General and Correctional Services / Ministère du Soliciteur général et des Services correctionnels
PCC	Privacy Commissioner of Canada
PCCIP	President's Commission on Critical Infrastructure Protection
PETs	Privacy-enhancing technologies
PGC	Principle of Generic Consistency
PGMs	Precision-guided-munitions
PHI	Personal Health Information
PIAC	Public Interest Advocacy Centre
PKI	Public key infrastructure
PPA	Prospective purposive agent
PRC	Privacy Rights Clearinghouse
RCMP	Royal Canadian Mounted Police
RFLP	Restriction fragment length polymorphism
RMA	Revolution in military affairs
SAR	Synthetic aperture radar
SCEPSP	Steering Committee for the Electronic Public Space Project
SET	Secure Electronic Transaction
SIS	Strategic Information Systems
SIW	Strategic Information Warfare
STOA	Scientific and Technological Options Assessment

TCO	Transnational criminal organization
UAVs	Unmanned Aerial Vehicles
UDHR	Universal Declaration of Human Rights
UNCESCR	United Nations Committee on Economic, Social and Cultural Rights
UNCSTD	United Nations Commission on Science and Technology for Development
UNDP	United Nations Development Program
USAF	United States Air Force
USAP	United States Army Pamphlet
USCC	United States Catholic Conference of Bishops
USOTA	United States Congress, Office of Technology Assessment
WIPO	World Intellectual Property Organization

HUMAN RIGHTS IN AN INFORMATION AGE
A Philosophical Analysis

This page intentionally left blank

Introduction

Information technology has rapidly changed our world, created a global informational economy, and radically affected our images of self, community, and culture. It is commonly acknowledged that digital information technologies, especially the information highway or Internet, has brought about a 'Third Industrial Revolution.' The First Industrial Revolution was heralded in 1776 by the steam engine, which replaced horse-driven wagons and exceeded the power of animals and humans by an order of magnitude. During the Second Industrial Revolution, between 1860 and the First World War, oil and electricity, especially the invention of the dynamo in 1867, created new energy sources that made instant communication between individuals possible. During this second wave of mass industrialization the burden of economic activity shifted even further from 'man to machine.' The Third Industrial Revolution took place immediately after the Second World War with the evolution of advanced computers and software, stored-program abstraction, and the idea of physical systems embodying purpose (Waldrop, 1998; Rosenblueth et al., 1943). Computers are now able to perform conceptual, managerial, and administrative functions, as well as coordinate the flow of production from the extraction of raw materials to the marketing and distribution of final goods and services. As a greater percentage of goods have become 'knowledge,' the nature of production has made resource-exhaustive, labour-consuming, and scarcity-bound production ever more obsolete (Davis and Stack, 1997). Digitally controlled robots, expert software systems, artificial intelligence, and new technoscience practices increasingly blur the distinction between mind and machine. Biotechnologies, in a dangerous precedent, give some human beings rights in other individuals that they do not

have in themselves, thereby risking what Paul Virilio calls the 'colonization of the body' (cited in Der Derian, 1996; Haraway, 1997).

The Information Age Revolution

While the information age revolution has had significant impacts on space (the shrinking of physical distance), time (time compression), the (declining) role of the state, politics, global economics, culture, and identity, the real meaning of the information age, especially its implications for human interpersonal communication and community, are by no means clear. For the president of IBM corporation, Lou Gerstner, the real meaning of the 'information revolution isn't about the end-user experience, and it's not even about the technology. [It's] about banks, universities, government agencies and commercial enterprises making fundamental changes in the way they currently do things' (Shniad, 1998). From the policy perspective of Industry Canada, the information highway, or Internet, is the necessary condition of possibility for both economic and social empowerment and enrichment, and the market should ultimately decide the economic 'winners' and 'losers.' For many scholars working from diverse, but often complementary, academic disciplines, the information age has turned knowledge into a commodity that undermines the use of information as a communal and public resource. In the process, the university itself has been transformed into a networking enterprise of 'digital capitalism' (Schiller, 1999). During the past two decades the campus has been identified as a site of capital accumulation. Commodification of the research function of the university has transformed scientific and engineering knowledge into commercial proprietary products that can be bought and sold on the market. The commodification of the education function of the university has transformed courses into courseware and the activity of instruction into commercially viable products such as copyrighted videos, CD-ROMS, and Web sites; as a result, the university has become a 'digital diploma mill' (Noble, 1998). Business pressures and government policy have sold out the taxpayer's public information to multinational information corporations such as Disney, Microsoft, News Corporation, and Thomson Corporation, whose broadcasting sorties commercially carpetbomb Canadian culture. Democratic community is the real loser in this expanding commodification of information, because democracy is founded on the free exchange of public information and full economic, social, and cultural

participation by citizens in the decision-making process (Gutstein, 1999; Mosco, 1989).

Robert McChesney of the Institute of Communications Research and the Graduate School of Library and Information Science at the University of Illinois argues that the media have actually become a significant *anti-democratic* force in North America and worldwide. The profit-driven, hyper-commercialized media of the corporate giants have led to the implosion of public life and to the demoralization of social movements and the public sector alike. Much-needed media reform is highly unlikely without a broader movement to democratize the core institutions of society. Both labour and the political 'left' should use media reform as a unifying issue among environmentalists, feminists, civil rights activists, journalists, artists, educators, librarians, and parents who would gain from such reform. Without a broader movement to realize the idea of democracy and social justice, conservative, neo-liberal media elites will continue to benefit by maintaining the status quo. They view their privileges and power as natural and immutable, and they desire to control social decision-making and power. Our present historical situation is characterized by a dominant view of democracy as the individual freedom to buy and sell property or the right to invest for profit. We pay lip-service to free speech, free press, and free assembly, while market rights become commonly equated with political freedom, capitalism becomes equated with democracy, and populism drifts to the margins. While the right to vote still remains, it is a very thin reed indeed, when elections function like auctions and electoral posts go to the wealthiest bidders. An earlier idealism that the Internet might provide a new golden age of competitive capitalism is rapidly fading away. Instead, the 'big are getting bigger' and the Internet is actually stimulating monopolies and oligopolies. The Web exponentially has extended commercial synergies, especially the role of advertising. This does not mean that the Internet may not positively help to reconfigure the way we lead our lives. No doubt it will do so, but 'those who think the technology can produce a viable democractic public sphere by itself where policy has failed to do so are deluding themselves. And the dominant forces in cyberspace are producing the exact type of depoliticized culture that some Internet utopians claimed the technology would slay' (McChesney, 1999, 183). The Internet has been almost completely incorporated into the corporate media and communications system, and the political left has been relegated to the margins of cyberspace

In his remarkable work, *The Information Age: Economy, Society and*

Culture, Manuel Castells, professor of sociology at the University of California, Berkeley, argues that the information technology (IT) revolution has been instrumental in restructuring the capitalist system from the 1980s onward.[1] The immediate economic background of capitalist restructuring is the crisis of the Keynesian model of economic growth in the early 1970s as manifested in rampant inflation. Deregulation, privatization, and the dismantling of the social contract between capital and labour began to destabilize the previous growth model. Institutions and management sought to restructure by 'deepening the capitalist logic of profit-seeking in capital-labour relationships; by enhancing the productivity of labour and capital; by globalizing production, circulation, and markets, seizing the opportunity of the most advantageous conditions for profit-making everywhere; and by marshalling the state's support for productivity gains and competitiveness of national economies, often to the detriment of social production and public interest regulations' (Castells, 1996, 19). The restructuring of capitalism and the diffusion of informationalism have been global, but with a wide variety of cultural and institutional diversity among and between informational societies.

Castells distinguishes 'modes of production' (capitalism, statism) from 'modes of development' (industrialism, informationalism). 'Informationalism' is the new mode of development shaped by the restructuring of the capitalist mode of production in the later part of the twentieth century. Soviet statism failed because of its incapacity to assimilate and use the principles of informationalism embodied in new information technologies. The interface between macro-research programs and large markets developed by the state, on the one hand, and decentralized innovation stimulated by a culture of technological creativity and role models of fast personal success, on the other hand, has allowed new information technologies to blossom. Modes of development refer to the element that is fundamental in fostering *productivity* in the production process. In an agrarian mode of development, quantitative increases of labour and natural resources result in increasing surplus. In an industrial mode of production, productivity lies in the introduction of new energy sources and the ability to decentralize the use of energy throughout the production and circulation processes. Now, in our informational mode of development, the source of productivity lies in the technology of knowledge generation, information processing, and symbol communication. The action of 'knowledge upon knowledge' is today the main source of productivity (Castells,

1996, 17). Whereas industrialism is oriented towards economic growth, 'informationalism' is oriented towards technological development, the accumulation of knowledge, and increasingly differentiated levels of complexity in information processing. Because informationalism is based on the technology of knowledge and information, there exists a close linkage between culture and productive forces, between spirit and matter, in the informational mode of development. More important, the new informational economy affects the whole planet either by 'inclusion' or 'exclusion' in the processes of production, circulation, and consumption. As such, we may expect radical new forms of social interaction, social control, and social change in the informational age.

Politics and democracy have also been radically transformed by the information age revolution. During the 1990s we witnessed the mobilization of a substantial proportion of civil society against the welfare state and social safety net, leading to the segmentation of society and the weakening of the state. Recent cultural emphases on community 'volunteerism' and 'charity' as substitutes for the welfare state are disingenuous, 'an ideological screen not to face the cynical abandonment of collective responsibility under the pretext of exercising individual responsibility' (Castells, 1997, 294). Liberal democracy has been traditionally based on the existence of a clear political sphere in which *collective solidarity* could operate. Today, the atomization and fragmentation of modern societies have weakened historical memory and human solidarity.

The globalization and interlocking of ownership, the flexibility and pervasiveness of technology, and the autonomy and diversity of the media challenge the nation-state. We see an irreversible sharing of sovereignty in the management of major economic, environmental, and security issues. The nation-state has become entrenched in a web of entangled political institutions that erode its power in exchange for durability. We have entered the realm of 'informational politics' where 'electronic media (including not only television and radio, but all forms of communication, such as newspapers and the Internet), have become the privileged space of politics' (Castells, 1997, 311). Without the use of new information technology, there is no chance of winning or exercising power. Electronic media do not dominate politics, however, since media are rooted in society, and their interaction with the political process is dependent on context, the strategic action of politicians, and the interaction of a broad array of social, cultural, and political features. Television does not *causally* determine the vote of the

people, nor does the largest media market capitalization win the day; nevertheless, informational politics are captured in the space of the media, and outside the media there is only political marginality. The state plays a key role in effecting the relationship between technology and society. The state can either stall, unleash, or lead in the area of technological innovation. Technology and information public policy become all important.

The construction of social action and politics takes shape around primary identities rooted in history, geography, or new forms of meaning and spirituality. In the midst of global networks of instrumentality and computer-mediated communications, identity is constructed as 'the process by which a social actor recognizes itself and constructs meaning primarily on the basis of a given cultural attribute or set of attributes, to the exclusion of a broader reference to other social structures' (Castells, 1996, 22). Fundamentalisms arise in our present historical situation because networks of wealth and power have excluded large segments of societies, regions, and even entire countries. The information age is marked by the rise of various forms of nationalism; the women's, gay, and civil rights movements; widespread currents of racism and xenophobia; the emergence of religious fundamentalism; and sects such as Aum Shinrikyo in Japan, American Militia groups, and Islamic and Christian fundamentalists. The social, political, and economic bottom has fallen out of the space of the computer illiterate, of consumptionless groups, and of marginalized territories, as patterns of social communication groan under tremendous stress. When communication breaks down altogether, when individuals can no longer even agree to disagree, then social groups and individuals become alienated from one another. The 'other' becomes a stranger at best or viewed as subhuman or even the 'enemy.' One of Castells's most insightful theses is that a fundamental split has arisen between historically rooted, particularistic identities, on the one hand, and the abstract, universal instrumentalism of information-based network flows, on the other hand. Societies have become structured around the bipolar opposition between the Net and the self. 'When the Net switches off the Self, the Self, individual or collective, constructs its meaning without global, instrumental reference: the process of disconnection becomes reciprocal, after the refusal by the excluded of the one-sided logic of structural domination and social exclusion' (Castells, 1996, 25).

Statism – the social system that is organized around the appropriation of the economic surplus produced in society by the holders of power in

the state apparatus – has increasingly disintegrated. To be sure, oppressive societies can potentially become even more tyrannical with the new surveillance tools at their disposal. Yet Orwell's prophecy was incorrect, because 'Big Brother' has not finally arrived, and the liberal, capitalist state has followed a different trajectory. Democratic, participatory societies *may* increase their openness, achieve greater representation, and further distribute political power by means of the new, powerful information technologies; but we do not seem to be headed in this direction. Surveillance capacities have grown more diffuse. The consequence has been increased power for violence outside the state institution and even beyond the borders of any particular nation. Castells maintains that the powers of surveillance and violence are dispersing into society at large, even as organized transnational crime expands its activities to target the security and economies of numerous countries.

A third commentator on our present historical situation, Francis Fukuyama (1999), argues that the information age began with the deindustrialization of the Rust Belt in the United States and comparable movements away from manufacturing in western industrialized countries from the mid-1960s to the early 1990s. This shift led to a 'great disruption' in social values and moral life marked by deteriorating social conditions in the industrialized world. Human trust and confidence in social, economic, political, and religious institutions went into a forty-year decline. Although a majority of people in the United States and Europe expressed confidence in their governments and fellow citizens during the late 1950s, only a small minority did so by the early 1990s. The nature of communal and societal interaction also changed, marked by 'less permanent, looser, and smaller groups of people' (Fukuyama, 1999, 55–6). The weakening of community and civil society occurred simultaneously during the information age revolution.

The analyses by McChesney, Castells, and Fukuyama reveal that privatization, deregulation, the hyper-commercialization of global markets, economic polarization, and the rise of national and global surveillance practices have brought about renewed concern with human rights, social justice, privacy, and political and economic democracy. Beyond mere millennial speculation about the 'end of history' and Y2K hype, there exists real anxiety over a broad spectrum of information technology (IT) policy challenges. How can we balance existing and new information technology practices with human rights – especially individual privacy – in the information age? Is the commodification of information undermining a vibrant, participatory

democracy? What kind of intersubjective communication will human beings realize in an age where globally networked communications provide new technological possibilities, but paradoxically have led to exclusion, disconnection, and communicative ruptures? Have technologies of light and silicon outstripped our ethics?

Purpose and Methodology

This book is offered as a philosophical response to these guiding questions. It contributes to the ongoing debates and dialogue over the meaning, ethics, and policy challenges of the information age and presents a vision of a more just, liberal democratic community and society. The work is more visionary than programmatic and offers no explicit policy agenda. Instead, we are guided from the outset by the meaning of our historical and technological *situation*, on the philosophical assumption that reflection must be informed by the use of 'historical knowledge, empirical data, and the potentialities of individuals in their historicity, relationality, and beliefs' (Jaspers, 1951 [1933], 24). Standing within a given historical situation, an author constructs a narrative, a story that functions as a horizon of meaning in the interplay of subjectivity and objectivity. He seeks to understand both self and the historical and technological situation within the constraints of temporality and finitude.

The book's methodology is necessarily *interdisciplinary*, because its central concern is to situate the information age within the broader historical and technological situation of modernity and to illuminate, from a human rights philosophical framework, IT practices surrounding the Internet, e-commerce, public safety and health, and security and military concerns. Scholarly treatments of the political economy of information,[2] IT practices and their privacy implications,[3] and even information warfare have been on the rise in recent years.[4] There are few authors, if any, who analyse these ethical and policy concerns from a human rights framework and none that does so in direct dialogue with Canadian information policy.

Three Ethical Challenges of Canadian Information Highway Policy

In March 1994 the Industry Canada minister, John Manley, created the Information Highway Advisory Council (IHAC) to assist the federal government in developing and implementing a strategy for the Cana-

dian information highway. The 'information highway' denotes 'the advanced information and communications infrastructure that is essential for Canada's emerging information economy. Building on existing and planned communications networks, this infrastructure will become a "network of networks," linking Canadian homes, business, governments and institutions to a wide range of interactive services from entertainment, education, cultural products and social services to data banks, computers, electronic commerce, banking and business services' (IC, 1994a,1).

The concept of an information highway dates back to 1993, when Stentor Telecom Policy Inc. announced its Beacon Initiative. The initiative proposed the building of a national information highway 'capable of carrying voice, text, data, graphics and video services to and from all Canadians' (Stentor, 1993, 5). Over $8 billion would be invested over the coming decade to upgrade Canada's local and long-distance networks, stimulate new business opportunities, and build partnerships with government and other industries in order to ensure that all Canadians would benefit from the information highway. From its inception, IHAC has held three key policy objectives: (1) creating jobs through innovation and investment, (2) reinforcing Canadian sovereignty and cultural identity, and (3) ensuring universal access at reasonable cost. IHAC's five guiding principles include (1) building an interconnected and interoperable network of networks, (2) collaborative public/private development, (3) competition in facilities, products and services, (4) privacy protection and network security, and (5) lifelong learning (IC, 1994a).

The Impact of Information Technology on Jobs and Growth

The most difficult ethical and policy issue concerned the impact of information technology on jobs and growth. Although during the first phase of IHAC's policy development the Canadian Labour Congress vice-president, Jean-Claude Parrot, published a minority report concerning the negative impact of IT on employment and the workplace (IC, 1995b), in subsequent policy formulations the creation of a legal and policy environment that promotes e-commerce was viewed as the only way to ensure the economic future for all Canadians (IC, 1997a). The e-commerce debate is part of the larger controversy about neoliberal globalization, competing moral visions of the Internet (e-commerce vs. e-commons), and IT regulatory standards and governance.

Previous policy studies have addressed the ethics of information management in the public (Grace, 1991; Mason et al., 1995) and private sectors (Bowden, 1991), the ethics of disclosing personal information held in government archives (MacNeill, 1991; Morton, 1996), the impact of IT on interest group behaviour (Stanbury and Vertinsky, 1995), and gendered perspectives on access to the Canadian information infrastructure (Shade, 1997, 1998a,b). While macroeconomic (Globerman, 1996; Babe, 1995) and microeconomic analyses of information highway policy do exist (Howitt, 1996), *ethical analysis* is conspicuously absent. This lacuna is not surprising. In a knowledge-intensive environment aspects of social policy are often indistinguishable from economic policy (Courchene, 1995; Howitt, 1996). Some authors suggest that international trade and copyright acts endorsed by the World Trade Organization (WTO) and the Multilateral Agreement on Investment (MAI) have insidious effects on the nature of content in information systems and on cultural sovereignty and identity (Clarke and Barlow, 1997). Canadians should be concerned about a shift from active citizenship to a privatized and commercialized infosphere for consumers. In a discussion of the impact of IT on the dwindling state, a government official flippantly remarked, 'Since when has the government been concerned with Democracy?' Concerned citizens know well, however, that there is little room for cynicism when the stakes of the information age for human dignity and rights are so high.

Privacy and Security

Privacy and security issues constitute a second major realm of ethical and policy concern. The use of smart cards, biometrics, closed-circuit television cameras (CCTCs), electronic monitoring, genetic testing, and global surveillance and encryption technologies dramatically illustrate the potential opposition between individual civil and political human rights, on the one hand, and legitimate public safety and health, and national and international security interests, on the other hand. Cryptography is a technology that is used to scramble computer files and communications to prevent them from being read by unauthorized users. It is enlisted to ensure authenticity and privacy of everything from medical records to e-mail to ATM transactions. Encryption is also being used by networked, transnational criminal groups for securities fraud and money laundering (Porteous, S., 1998). The Canadian cryptography policy debate has taken on new urgency in the light of the

government's public key infrastructure policy (CSE, 1998) as well as international encryption policy debates (GILC, 1996, 1998a,b). Some technologists oppose key recovery schemes on both technological and pragmatic grounds (Abelson et al., 1998). Governments and the military generally view encryption as a 'munition,' while human rights organizations have opposed key recovery as a violation of free speech and a threat to privacy (Pokempner, 1997). What should we do?

Whatever the specific technological developments, the ethics of privacy and security policy turn back on the meaning and nature of privacy and privacy rights. The government has called upon academics for assistance in the attempt to balance core ethical and privacy principles with societal protections (HC, 1997). The ethical challenges of the information age, however, must not to be reduced to norms of privacy or fair information practices alone. Privacy – or lack thereof – remains an extremely serious and ongoing human rights and ethical issue. Yet the ethics of informational privacy is both too large and too small: too large, because we are only now bringing into place legislation for the protection of personal information; too small, because policy analysis must make larger connections with the informational economy and international surveillance and security challenges. All the while, information or data overload forces many individuals into a type of 'departmentalized,' specialized thinking as the amount of printed material increases exponentially (Strawson, 1980) and connections to a larger whole of knowledge are lost.

Information Warfare and Deterrence

During the five years of policy formation, Canadian information highway analysts addressed business concerns with network security and law enforcement concerns with public safety, but problems surrounding the protection of critical information infrastructures and 'information warfare' (IW) practices have evolved with little, if any, policy and ethical reflection. The adoption of the Universal Declaration of Human Rights (UDHR) by the United Nations General Assembly in 1948 came on the heels of the Second World War and the demise of the principle of unrestricted state sovereignty. This declaration was motivated in large part by the effects of mass warfare such as carpet bombing and Nazi genocidal practices (Walters, 1995a). We are now witnessing the rise of a different kind of warfare through the use of smart bombs, laser-guided munitions, and IW weapons (Campen, 1992; Walters,

1995b, 1998b). The post–Cold War 'revolution in military affairs' (RMA) has shifted national security concerns from nuclear weapons use and deterrence to information warfare weapons and deterrence involving nation-states, criminal groups, and individuals (Arquilla and Ronfeldt, 1997a,b). Policy makers and strategic military analysts are preparing for cyberwar by rethinking military organization, doctrine, and strategy. Governments are spending millions of dollars on new databases, network architectures, and advanced software under the rubric of IW. The *ethical* aspects of information warfare, alas, often have been reduced to technical aspects of network security (Schwartau, 1994), and in this work we seek to make a major contribution to the ways we should be thinking about the ethical aspects of IW.

Aims and Terminological Presuppositions

The point of departure of this book thus is taken from the foregoing ethical and policy concerns; the question is asked: *How, if at all, can we balance existing and emerging information technology practices surrounding e-commerce, public safety and health, and national and international security concerns with human rights?* The aims of the research are threefold: first, to historically contextualize the foregoing policy domains addressed by the work of the Canadian Information Highway Advisory Council between 1993 and 1998 and subsequent e-commerce strategy; second, to bring a human rights and ethical analysis to bear on the information policy debates, especially the ethical justification of privacy rights; and third, to bring philosophical reflection to the policy debates, especially the role of mutuality and human communication for economic and political democracy in the information age. Digital interactivity does not guarantee quality human communication.

The concept of 'balance' noted above should be problematized at this point, since 'balance' has a number of different connotations, depending on who is doing the 'balancing' and for what purposes. What do privacy regulators, data users, or data subjects actually do when they 'balance' privacy against other important interests? How do we know when 'balance' is reached, if ever? These are important questions, which reveal that privacy protection, both in law and in practice, involves balancing *competing values* in order to safeguard individual rights while trying to accommodate other important social, political or economic ends. Raab (1999), for example, criticizes the doctrine of balancing personal claims against the public interest. The model is inade-

quate, in his view, because if we take rights seriously, then governments must respect the dignity of individuals and equality. The public interest side of the equation typically involves a moral appeal to efficiency, the maintenance of law and order, or access to goods and services, which does not give sufficient warrant for the balancing process. Privacy policy is, in turn, absorbed by consumerism. Interests and values may be incommensurate, and privacy is traded for managing surveillance. Given the de facto unequal power positions of players, privacy is always the lightweight fighter in the policy ring. 'The onus of proof,' he writes, 'is on the other side that to relinquish a rights claim in pursuing a pragmatic strategy of accommodating other interests or policies is not to give a hostage to the fortunes of politics, government, and commerce' (Raab, 1999, 76). Raab prefers the concept of 'steering' as the essential aspect of the decision-making process. 'Steering' rests on an elaborate cybernetic conception of movement in a particular direction, perhaps governed by a controller who aims at a desired state of privacy affairs. Regulatory agencies should be examined in terms of their ability to know and to steer, while participants should be examined in terms of their capacity to learn and change. Technologies should be steered toward the application of better encryption standards and access protocols. Interventions should help data subjects to become better privacy maximizers and stronger negotiators, even as whistleblowers should be encouraged to report on poor adherence to privacy standards within a given industry, firm, or agency.

Raab's steering metaphor, however, begs the question of what specific privacy goals *ought* to be, what substantive privacy rights we *ought* to 'steer' towards, and on what justificatory basis we *ought* to do so. For without a substantive philosophical discussion of the justificatory ground of privacy, it is mere semantics to advocate steering over a doctrine of balance.[5] It might well be possible to steer privacy policy down a course of action that eventually could be detrimental to the very dignity and equality of individuals that Raab wishes to uphold. The human rights framework set forth in the next chapter helps us to determine more clearly the forms of personal data that ought to be subject to collection by state and private organizations in accordance with the necessary conditions of human action. The framework is not meant to be an information policy panacea. It does provide a thicker philosophical justification for privacy rights, however, as well as a doctrine of 'balance' that will continue to be at the core of privacy policy well into this century.

Let us now turn to the terminological presuppositions that inform our research, and show how and why the ethical analysis is situated in the discipline of social and political philosophy.

Technology entails not only the tools, machines, and artefacts required for production, but also workers' skills and the organization of production. Barbour's (1993, 3) definition of technology as 'the application of organized knowledge to practical tasks by ordered systems of people and machines' provides a useful working definition. The 'real world of technology' is more than the sum total of what people do or fabricate, yet the redemption of technology in the service of human dignity and human rights ultimately will come only from changes in what people, individually and collectively, do or refrain from doing (Franklin, 1994). We hold a contextualist view of technology, which rejects technological and economic determinism and insists on human freedom and alternatives and choices operative in a two-way interaction between technology and society. Our age is in search of an Aristotlean mean between the demonization of technology and technotopian world views.

Information technology refers to computer hardware and component manufacturing, computer software development, and various computer-related services combined with communications equipment, component manufacturing and telecommunications services (Gera et al., 1998). Policy definitions often define IT as an enabling resource that allows things to be done differently and that is capable of being applied across a variety of sectors (ITAC, 1989). Industry Canada's definition encompasses a wide range of products and services across four main industries: consumer electronics, telecommunications and electronic components, computers, and instrumentation. Within these four types of industries, electronic computers and peripherals account for almost 33 per cent, and telephone and telecommunications services 20 per cent of all IT goods and services (Lafleur and Lok, 1997). Some philosophers argue that the key value of IT is its use as a means to transform data into information and usable knowledge as expeditiously as possible (Spinello, 1995, 2). Industry Canada sees the main value of IT as enhancing 'a country's ability to apply technology creatively in devising new and consumer-valued information products and services' (IC, 1997b, 3). In addition to these technologically oriented definitions, IT ought to serve the dignity and rights of individuals in community, since people are of far more value than things.

We are living through a major historical transformation of material

culture that is a direct function of a new 'information technology paradigm' (Castells, 1996). Information is the raw material of the new paradigm. New information technologies act directly upon information, rather than being simply information that acts on technology, as was the case in previous technology revolutions. The effects of the new technologies are pervasive. There is a networking logic at work in any system or set of relationships that use the new technologies. Networking morphology is a creative medium for adapting increasingly complex interactions and unpredictable patterns of development. This unstructured nature of networks and network logic now affects various processes and organizations in a fashion analogous to the unstructured nature of creativity that drives innovation in human activity. The new IT paradigm is also based on flexibility. Organizations, institutions, and processes can be modified and fundamentally altered by rearranging different components, and such reconfiguring may work for good or ill. Business-to-business e-commerce may save time and money, but global criminal groups can and do intentionally network against those entrusted to protect and serve law-abiding citizens. Networks are created not only to communicate, but also 'to gain position, to outcommunicate' (Mulgan, 1991, 21). The IT paradigm involves a growing convergence of microelectronics, telecommunications, optoelectronics, and computers into one information system. Convergence also extends to the biotechnological revolution, where the Human Genome Project that is mapping all human genes is possible only because of massive computing power.

If information is the basic material of the new IT paradigm, then what, precisely, is information? Fritz Machlup's definition of information as raw, unprocessed data from which knowledge is constructed and that provides increments to knowledge raises the problem that knowledge is variable from one person to the next (Machlup, 1980). So is the interpretation of what constitutes an increment to knowledge. Information has also been defined as what provokes a response in, or in some way affects or transforms, a recipient (Wiener, 1967 [1950]). Information relates not only to the message, but to the conduit of transmission and reception; hence, McLuhan's (1994 [1964]) oft-quoted insight that 'the medium is the message' (cf. Kroker, 1984). If a receiver does not record the stimuli, she has not been touched or 'in-formed' by the information. Information then remains either invisible, or is simply a form of incomprehensible noise. In another definition information is seen as a limitation of or selection from possibilities, a 'closing of

entropy' (Klapp, 1978); information orders or forms the randomness and chaos of data. This definition of information as a selection and arrangement of data resembles that of a 'compilation,' which is found in many copyright statutes, including the Canadian Copyright Act (section 2, R.S.C. 1985, c.C-42, as amended). Hence, the conscientious selection and arrangement of data combined with other data form a proprietary information legal right.

To what end ought information and the new information technology paradigm be directed? One of the great demands of the information age is not merely to search for information and filter it from the massive amounts of data or noise, but also to turn information into knowledge and, ultimately, ethical wisdom. As we move from data to information, we come a step closer to knowledge as a clear and distinct mental apprehension. Wisdom is the highest level of information that, at least ideally, leads to prudential judgment and rational action. The value and quality of understanding increases as we move from disorganized raw data and facts to organized information, to refined knowledge, and, finally, to wisdom, where self-awareness, truth, and justice represent the highest possible form of human understanding.[6]

Wisdom helps us to live and act well. Mill argued that individuals should not live by mere conjecture and common opinion. Instead, we need exposure to a variety of viewpoints in order to discover truth and have it play a vigorous role in our lives. Freedom from censorship develops the best type of people, because it allows individuals to create or evaluate ideas in accordance with truth. We have a duty to self to discover the truth, and each of us should seek to acquire wisdom for which our human nature suits us. Only by considering other individuals' opinions and ideas are we able to determine which, if any, contain partial or greater truth. Once truth is willed, then we seek it in earnest; once truth is partially found, then wisdom can follow and make us better moral agents than we would be otherwise (Mill, 1972 [1859], 85–142).

The Conceptual Importance of Information to Human Rights

What is the conceptual importance of information to human rights? The analytical link between information and human rights and information and human action will become clear in the next chapter. Suffice it to say here that modes of access to information, work, commerce, transportation, health care, law enforcement, security and intelligence practices, and military information operations are being revolutionized

by advancing technological change. Information is an integral part of all human activity, and all processes of our individual and collective existence are directly shaped by the new technological paradigm. More important, it is with human actions that all moralities or moral precepts, including moral and legal rights, deal either directly or indirectly. Ethical precepts, as a type of wisdom, tell human beings how they *ought* to act towards one another and within social and political institutions. The virtues tell us what kind of individuals we ought to be. Since to have a virtue is, among other things, to be disposed to act in certain ways, actions figure at least indirectly in ethical frameworks that focus on the virtues for the development of individual character and the flourishing of a good society (MacIntyre, 1984). This has been true throughout human history, whether individuals live in an agrarian, industrial, or informational society. Moroever, as noted earlier, the self is increasingly shaped by the split between a particular local identity, on the one hand, and the mediation of the self by means of universal information networks and the conditions of possibility for freedom and well-being that such networks entail, on the other hand. For these reasons, then, there exists a vital conceptual link between information and human rights.

Human rights scholars have been concerned for decades with the implications of information and information technologies for human rights on both pragmatic and theoretical grounds. In the early 1980s Paul Sieghart, a member of the United Kingdom Data Protection Committee, called for an International Convention on the Flow of Information, arguing that 'one of the fundamental human rights should be access to as much accurate, complete, relevant and up-to-date information as everyone needs for the free and full development of their personality [cf. article 29 (1), UDHR], the enjoyment of their lawful rights and the performance of their lawful duties, and protection from the adverse consequences of the misuse of information by others' (Sieghart, 1983, 27). A large percentage of the scholarly human rights literature has been focused on the human right to privacy or legal codes known as 'data protection' in Europe and Canada and 'privacy protection' in the United States. Whatever the terminology, the central premise and concern have been that organizations that collect personal information about individuals have certain responsibilities, and individuals have rights against organizations that possess personal information. However, the question to which the data-protection model was the answer has changed significantly. The pervasive spread and

merging of databases, practices of data mining and warehousing, the global flow of information across jurisdictional boundaries, and the rise of new 'privacy-enhancing technologies' (PETs) have created an even larger gap between the technical concept of data protection and legal and moral rights to privacy (Agre and Rotenberg, 1998).

Still other human rights scholars have examined how non-governmental organizations, governments, and the United Nations can *positively* use electronic mail, computer conferencing, and on-line database information to promote human rights (Metzl, 1996). IT use in the service of human rights work is not simply about information gathering and dissemination tools. Improved computers and software undeniably expand the ability of human rights organizations to uncover and analyse patterns and trends in human rights violations. There are negative human rights implications of computerized information systems as well. Norms of privacy, non-discrimination, and consent are profoundly affected by the types of information systems developed and instituted, the ways in which access is regulated, and the way the data are used. Computerization makes more data about individuals available to a wider range of users. Data are being linked and used in ways for which they were never intended, such as the prejudicial use of medical records in prison sentencing of individuals who provided information in good faith (Ball et al., 1997, 859; Metzl, 1997).

The social, economic, and cultural revolution brought about by the new IT paradigm means, in the words of Industry Canada, that 'a new game is starting, and the older rules new longer apply' (IC, 1997b, 1). Have the new rules of the game been defined fairly? Do they involve the participation of as many players as possible? Will human rights be excluded from the new rules? The gap between information haves and have-nots has widened, and the pay gap between CEOs and workers is unconscionable. The ratio of top executive to factory worker pay has exponentially increased during the decade of the 1990s. If the average production worker pay had risen as rapidly as CEO pay, then 'a worker would be making $110,000 a year today, instead of the $29,000 a worker actually makes. Put another way, the minimum wage today would be $22.08 an hour, rather than the $5.15 it actually is.' The average CEO pay was $10.6 million in 1998, a fivefold increase from the $1.8 million of 1990. CEO pay rose 36 per cent, compared with only 2.7 per cent for the average blue-collar worker.[7] Much of the CEO increase came from the robust performance of the bull stock market, since most corporations offer generous stock options. Defenders of corporate lar-

gesse argue that intense competition for talent drives compensation packages in a way analogous to the situation of free-agent sports stars. These gaps may widen even further in the future, since no economic decision is devoid of 'the market value system' now being transformed by automated trading systems in the informational economy (McMurty, 1998).

Another human rights concern is the impact of IT on the distribution of power in society. We urgently need to restore and preserve a more balanced distribution in the technological infrastructure and operating system of the informational economy. The power to operate and program the digital economy should be broadly and democratically distributed. Health, education, and culture ought to remain public resources, not merely profit-seeking commercial enterprises. These societal goods serve individuals in community and support or hinder human freedom and well-being. The IT policies we undertake on the cusp of the twenty-first century ought to cover the needs of the most vulnerable members of our society and enable all individuals to develop their own abilities of productive agency. Solutions to human economic and social needs in the informational age pose the major challenge to social and political philosophy.

Philosophical Parameters and Thesis

Social and ethical analyses of computerization today span a very broad array of utopian, anti-utopian, and empirical strategies and genres across a variety of academic disciplines (Kling, 1997). Philosophers of technology have been thinking about the historical traditions and analytical issues in the engineering philosophy of technology and humanities philosophy of technology traditions since at least the early eighteenth and nineteenth centuries (Mitcham, 1994).[8] The humanities philosophy of technology tradition now includes environmental ethics, bioethics, science-technology policy studies, and global climate change (Ferré, 1988; Ihde, 1993). Efforts to integrate philosophical discussions of technology with substantive ethical concerns are of more recent vintage (Kransberg, 1980; Mitcham and Mackey, 1983 [1972]; Wajcman, 1991). By the early 1990s there was a rush towards techno-ethical discussion as part of the 'applied' turn in philosophy. In recent years, reflection has shifted to the social and economic consequences of 'computer-mediated communications' (CMC); study of underlying assumptions and foundational questions regarding technology and

knowledge (epistemology), reality (ontology or metaphysics), and values (ethics) has gained increasing momentum (Ess, 1996). Technologists, policy makers, business managers, and military strategists are asking whether or not the IT revolution requires a corresponding revolution in ethical thinking and doing. The questions and challenges are often so new that they wonder if traditional natural law, deontological, utilitarian, teleological, or rights-based ethical traditions are capable of responding to the tumultuous technological transformations of the information age.

The human rights analysis developed in this book builds upon, but goes beyond, these earlier approaches. We argue that if we are to achieve a needed balance between individual rights and societal interests, then informational rights will require far greater specification (Trudel et al., 1997), even as communal values of trust, social solidarity, and mutuality are increasingly vital to the promotion and protection of human dignity. For human rights are moral as well as legal, and it is their morality that underlies and justifies their legality.

The analytical human rights framework outlined in the next chapter shows how and why we must overcome the false opposition between human rights and community at a time when globally networked communications have provided new technological possibilities, but paradoxically have also led to exclusion, disconnection, and communicative ruptures between human beings. Human rights have as their objects the necessary goods of individuals to which they are entitled and that require duties on the part of others. Community protects and fulfils rights, especially for individuals who do not effectively have them, on the basis of mutuality and the social solidarity of individuals who recognize and fulfil common needs. Human rights require community for their implementation, while community requires human rights as the basis of its morally justified economic, political, and social operations and enactments. However imperfect and inevitably time bound ethical traditions may be, a proper understanding of the correlative nature of human rights and responsibilities is vital for ethical reflection in the information age.

Technology cannot provide an ethical 'operating system' for the deeper problems that plague communicative reason among individuals in our present historical situation. If anything, technology aids in the reduction of the other into an object or means. Nor does technology provide a response to the problem of balancing individual and communal goods, private and public interests. At the limits of technical

design and moral norms, the challenges of the information age open on to the need for a wider rationality or reasonableness and raise profound questions about the possibilities of human trust, mutuality, and social solidarity. We believe that the stakes and meaning of the information age revolution become clear only when analysed within the historico-technical situation of modernity and from a philosophical anthropology and human rights framework in which both the community of rights and human mutuality are viewed as compelling ethical ideals of the information age.

Structure of the Book

The reader will note the highly ambitious scope of the book. We propose to cover a vast range of literatures and a variety of complex technical and policy issues in order to explore the ethical dimensions of Canadian information highway policy; e-commerce strategy; the impact of IT on work, privacy, and security rights; and the ethics of information warfare use and deterrence. The research is necessarily far reaching, given the difficult policy issues at stake, the use of two major philosophical frameworks that define our analytic approach, and the aims of contributing to the ethics of information policy and social-political ethics. We seek to avoid 'departmentalized' thinking at a time when it is inevitable yet highly disconcerting.

In chapter 1 we set forth the human rights framework that guides the ethical evaluation of information highway policy and e-commerce strategy. We clarify our philosophical anthropology, the characteristics of modernity, and the world-historical impact of technology, and we identify our action-based human rights framework.

In chapter 2 we survey the main phases of Canadian information highway policy and e-commerce strategy. Non-Canadian readers will recognize similar debates and concerns that have emerged in their own national infrastructure policy debates. The methodological and ethical reflection highlights and analyses substantive policy issues while delimiting the ethical concerns addressed in subsequent chapters.

In chapter 3 we begin with an analytical discussion of productive agency, work, human capital, and property rights that expands the previous philosophical framework. We define the informational economy and identify globalization's challenge to social and economic rights, the failure of human development strategies, and the problem of pervasive poverty. We argue that there are empirical and ethical problems

with the so-called end of work thesis related to unemployment data and differing interpretations of the productivity paradox. The ethical problem is related to the meaning of productive agency, work for human dignity and income leading to property rights, and the importance of promoting and protecting economic rights to development and employment in the neo-liberal marketplace.

Like the debates surrounding the impact of IT on work in the informational economy, privacy and security policy debates turn back on substantive ethical and empirical questions. In chapter 4 the reason that the new situation of privacy and security policy is shaped by technological, economic, and political domains is revealed. We first survey international privacy and security policy developments before turning to the Canadian situation and recent concerns with private sector information protection and cryptography policy. The substantive policy issues are highlighted and should be read in conjunction with the ethical-philosophical analysis of chapter 5, in which we draw an ethical line between negative and positive surveillance and security practices. In chapter 5 we survey current technology practices as well as legal, social scientific, and philosophical conceptions of privacy with a view to their possibilities and limitations in our present situation. In our ethical analysis of information highway policy, e-commerce strategy, and privacy and security policy, we use norms of basic, non-substractive, and additive well-being; the criterion of degrees of needfulness for action; and the principle of human rights. We offer a thick theory of ethical justification whose substantive derivation of norms bears directly on the ethical 'balance' between individual rights and societal interests.

How far should surveillance and security measures be allowed to go in order to investigate and prosecute informational terrorism, violence, and crimes against domestic and international commercial, financial, and government systems? Do existing privacy and security policies achieve the sought-after 'balance' between individual rights and the public interest? These questions pose some of the most difficult challenges for policy makers, governments, and concerned citizens, because they are directly related to the rise of 'information warfare' technologies and practices. In chapter 6 we define various conceptions and practices of 'information warfare' (IW) and link IW practices to international human rights law and the indirect application of the principle of human rights. As an extension of the principle of human rights, we look to classical norms of the justifiable war tradition and ask: Can

there be a 'just' information war? At the limits of moral norms, we ask: Is a 'perpetual peace' possible in the information age? In accordance with the consensual procedures of the democratic state and the principle of human rights, we argue that citizens need more accurate knowledge of the empirical threats to national security and public safety in order to make informed judgments about legislation that seeks to restrict privacy rights through global surveillance practices.

Is information warfare deterrence both rational and reasonable? In chapter 7 we argue that a policy of strategic IW deterrence could be both rational and reasonable only if it were able to establish and stabilize alternatives that do not involve the threat of non-combatant murder or violate the principle of human rights by imposing substantial risks of harm without consent. Our challenge is to move beyond political realism, idealism, and even a necessary pragmatism, to a mutuality of human rights and a moral reasonableness that makes both trust and security possible. The problem of information warfare deterrence brings us to the limits of politics and technology for solving the problem of war. The information age revolution presents us first and foremost with the challenge of rational selfhood. The 'solution' to the problem of deterrence is a needed human transformation towards a wider rationality where mutuality and human communication are realized in a global community of rights. We fail to understand the meaning and significance of the information age revolution if we do not grasp its implications for a commensurate revolution in our respect for human rights, responsibilities, and mutuality in communication and action.

CHAPTER ONE

The Philosophical Framework

In this chapter we set forth the philosophical framework with which we will approach our ethical evaluation of Canadian information highway policy, e-commerce strategy, and privacy and security challenges. Because philosophical analysis must begin with reflection on the present historical 'situation,' and because the information age has evolved within the context of modernity, we first identify some key social and technological characteristics of modernity and the world-historical impact of technology. Then we delineate an action-based human rights framework that is neither exhaustive nor exclusive, but provides readers with the ethical horizon within which the information highway policy concerns of the subsequent chapters are explored.

The Information Age in the Context of Modernity

The information age revolution marks a new situation, with significant impacts on space, time, the state, identity and culture, and the informational economy. Information technology developments have created our informational mode of development and will shape the situation of future generations. In surveying a situation we must take into consideration 'historical knowledge, empirical data, and the potentialities of individuals in their historicity, relationality, and beliefs' (Jaspers, 1951 [1933], 24). A 'situation,' in the technical sense in which we are using the word, is a sense-related reality, both psychological and physical, a concrete reality that means advantage or detriment, opportunity or obstacle to human existence. Biologists, economists, and historians study situations in respective contexts of the animal environment, supply and demand economics, or the linear emergence of a new historical

age. As human beings we are always in situations, and we help to create new situations by the actions that we perform or do not perform. Every new technical creation confronts us with new situations. Every new situation, in turn, raises the question of what we will make of our situation, how we will act in it, in what sense we will master or succumb to it.

Our present historical and technological situation may be defined by the concept of 'modernity.' Modernity refers to the institutions and modes of behaviour first established in post-feudal Europe, especially the rise of modern science and technology in the seventeenth century. Industrialism, capitalism, global surveillance, and expert control of the means of violence essentially define modernity.

> 'Modernity' can be understood as roughly equivalent to the industrialized world, so long as it be recognized that industrialism is not its only institutional dimension. I take *industrialism* to refer to the social relations implied in the widespread use of material power and machinery in production processes. As such, it is one institutional axis of modernity. A second dimension is *capitalism,* where this term means a system of commodity production involving both competitive product markets and the commodification of labour power. Each of these can be distinguished analytically from the *institutions of surveillance,* the basis of the massive increase in organizational power associated with the emergence of modern social life. Surveillance refers to the supervisory control of subject populations, whether this control takes the form of 'visible' supervision in Foucault's sense, or the use of information to coordinate social activities. This dimension can in turn be separated from control of the means of violence in the context of the *'industrialization of war.'* Modernity ushers in an era of 'total war,' in which the potential destructive power of weaponry, signaled above all by the existence of nuclear armaments, becomes immense. (Giddens, 1991, 15; emphasis added)

The notions that modernity entails human beings' instrumental relation to nature or that the technologization of culture has tended to exclude questions of morality now are common. Germane to our historical situation is the dynamic character of modernity as marked increasingly by the separation of time and space by means of computer-mediated communications, the 'disembedding' of social institutions, and the thoroughgoing individual and institutional 'reflexivity' of our epoch. Pre-modern settings connected time and space through

the situatedness of place. Not so today. Our world has a universal dating system, global time zones, and networked social organizations that are coordinated without reference to the particularities of place. The separation of time from space makes historicity more global, and the year 2000 became a marker for the whole of humanity. The disembedding of social institutions has lifted social relations from their local contexts. 'Symbolic tokens' and 'expert systems' are two types of disembedding mechanisms. A symbolic token like money brackets time (by means of credit) and space, because monetary value allows transactions between individuals who never meet physically. Expert systems bracket time and space by the use of technical knowledge that has universal validity independent of its end-users. We fail to understand the meaning and pervasive influence of expert systems if we reduce them to artificial intelligence. Expert systems penetrate all aspects of our lives – from the food we eat, to the medicines we take, to the buildings we inhabit, to the transportation systems we use. They extend to social relations and the intimacies of the self mediated through doctors, counsellors, and therapists and thus are no longer merely the preserve of scientists, technicians, and engineers. The use of e-commerce and the Internet to conduct on-line market transactions represent disembedding phenomena. E-cash is a new symbolic token mediated through fibre-optic infrastructures and expert servers that will become new means for the interpenetration of human development and social systems, including global information systems and networks.

Discussions of expert systems often fail to admit that they depend on forms of mutuality and trust. Trust is not the same as confidence or the 'weak inductive knowledge' that informs formal monetary transactions (Simmel, 1978, 179). Confidence is a necessary, yet insufficient, element of trust, because authentic trust presumes a certain leap of commitment, a quality of faith in the other. Trust is related to *absence* in time and space, as well as to ignorance. We generally feel no need to trust someone who is constantly in view and whose activities can be directly monitored. Low-trust positions, for example, are low paying, monotonous, or unpleasant jobs in which the motivation to perform the work conscientiously is weak. High-trust posts, in contrast, are those carried out largely outside the presence of management or supervisory staff. Similarly, there is no requirement of trust when a technical system is more or less completely known to a particular individual. Trust frames the limited knowledge that most of us possess about the technological systems that routinely affect our lives. Trust underlies

our day-to-day activities, and we would find it difficult to function in the world without it, for example, each time we take off or land in an airplane. Trusting entails 'a generalized attitude of mind that underlies [consciously taken] decisions, something which has its roots in the connection between trust and personality development ... the faith which trust implies ... tends to resist such calculative decision-making' (Giddens, 1991, 18, 19).

The faith that trust implies encompasses the mere calculative decision making of the intellect. Our attitudes of trust in relation to specific situations, individuals, or systems are grounded in the psychological security of individuals and groups. The conditions of modernity now inevitably unfold between trust and security, risk and danger. To be sure, disembedding mechanisms provide certain levels of security in our daily lives, such as providing electrical power for heating during the winter, but they simultaneously create new risks and environmental dangers. This is why some philosophers of technology would remind us that the solution to our problems is 'not less technology, but more technology' (Agassi, 1985, 259).

The sciences play a key role in the 'reflexivity' of modernity by undermining the certainty of knowledge, even in the core domains of natural science. The integral relation between modernity and Cartesian doubt – that is, that data are always open to chronic revision in the light of new information or knowledge – is disturbing to philosophers and existentially troubling to ordinary citizens. Reflexively organized life planning– where risk is filtered through contact with expert knowledge – is a central feature of the structuring of self-identity.

Reflexively planned existence is a world-historical phenomenon. The technological revolutions of modernity have radically affected both westerners and non-westerners alike, ushering in an era of technologically based communication. An important question is whether or not technologically mediated communication will grow into a global communion of the human spirit, a loving struggle for communication, or whether new information and communication technologies will instead provide the means for mutual rejection and hatred. Technology fuelled the perverse totalitarian manipulation manifest in Hitler's *Führerprinzip*. Modernity's marvellous technological inventions have given birth to difference, exclusion, and marginalization long before the rise of informationalism. The 'Final Solution' [*Endlösung*] to the Jewish question, however banal the evil (Arendt, 1963), was possible only because of modern technological developments in engineer-

ing and architecture. The Nazis also used early computers and recording devices for surveillance (Flaherty, 1999).

We acknowledge the positive technological transformations of modernity while simultaneously drawing attention to the ambiguous impacts that technology has on self, society, and meaning. Philosophers, especially Kant, have always distinguished between theoretical and practical reasoning. The distinction between *Verstand* (intellectual thinking) and *Vernunft* (rational thinking) helps us to grasp the epistemological contours of modernity and the rise of the information age. *Intellectual thought*, or instrumental rationality, is the mode of the technological inventor and maker. Its precepts can be carried out and can multiply the technological making by infinite repetition. One consequence is that it results in a world in which a few minds devise the technics or technological operating system. They create, as it were, a second world in which the masses then assume an operative function on some aspect of the technological system. *Rational thought*, on the other hand, does not provide for the carrying-out of mass directives. It requires that each individual to do his or her own thinking. Reason believes that truth is found not by a machine reproducible at will, but by decision, resolve, and action whose self-willed performance by each person is what creates a common spirit (Jaspers, 1958, 1961). When intellectual thought dominates the economic, political, and social realms, humanity assumes an operative function in the state and society. Human will or volition becomes conditioned by means-end relationships, human beings become objectified, and the intellect usurps its proper role for human reflection.

Reason, as distinct from the intellect, grounds human communication in freedom. Freedom in communication unfolds in a dialectic between solitude and union. If we lose ourselves in others, we lose healthy independence. Conversely, if we isolate ourselves and the computer becomes an extension of the self in merely a virtual mode, communication grows empty. Solitude is the preparatory and anticipatory consciousness for manifesting communication between persons. Digital communication, even in interactive form, is no guarantee of authentic human communication, which is an arduous and continual process in which we must abandon mere self-preservation and self-concern and bounce back from angers and injured pride.

To be sure, modernity has been marked by conflict and struggle. Human beings struggle to enforce their interests and claims against others in situations of everyday life. Human rights recognize the inevi-

table fact of conflict and struggle in actions to achieve material ends, social status, or prestige and power in every group and society. In struggle, an agent's success is often necessarily accompanied by the suppression of the demands of others. In this situation, the ethical goal is to turn the violent and coercive struggle for existence into a 'loving struggle,' a non-violent, no-coercive form of struggle, whose dominant norms are mutuality and solidarity. Limit situations cannot be overcome by objective and rational solutions, but require a radical change or 'conversion' in our attitude and way of thinking (Walters, 1988). This new mode of rational or reasonable thinking goes beyond the intellect, even as networked modes of communication will play an increasingly significant role in human self-realization and the construction of the social, political, economic, and cultural order.

Technology's impact on modern communication, selfhood, and identity precedes the development of the Internet, but there is much that makes our present historical situation different from the earlier, second-wave industrialism of the post-war period. During the Second Industrial Revolution work was labour intensive and a determinant of mass life. Work's raison d'être was to supply the basic needs of the masses in an industrial mode of production. Technological universalization threatened human freedom with functionalization and the degradation of individuals into instrumental objects serving industrial or capital expansion. A certain dread resulted from the exponential dependence upon technology for the necessities of life and from the corresponding threat of technological breakdown. The 'man in the machine' had to work relentlessly merely to stay alive. Today 'man' increasingly *is* the machine, a cyborg in whom the boundary between animal and human is more thoroughly breached than ever (Haraway, 1991).

If the loss of joy in work was a fundamental problem during the period of middle modernity, it is no less a problem today. Finding and maintaining well-paid work in the informational economy are increasingly difficult for low-skilled, blue-collar workers. We also face the problem of overwork.[1] Second-wave mass labour bound individuals in community, but this effect was fleeting because of the functionalization of the worker. Are the virtual communities and alliances of our situation any less fleeting? Is the self becoming a community of two, that is, the self and the computer, with the latter as a 'second self' projected into cyberspace by means of Internet chat rooms and e-mail communication (Turkle, 1984)? Empirical data suggest that violent computer games

have a powerful impact on young people. Acting out virtual-realm fantasies has led to tragic loss of life among students and an increasing interest in hate propaganda and neo-Nazi ideology. Where life becomes meaningless because of the absolutization of a technological life-order, either radical human change entailing human freedom and well-being or pathological behaviour remain dominant possibilities.

More than ever before in human history, science and technology hold out new possibilities for human development and freedom, even as technological developments should be placed under ideals of rationality and ethics, a healthy sense of human humility and finitude, and the limits of cost-benefit analysis and risk assessment. Our existential framework espouses neither a Luddite manifesto nor millennial pessimism. Indeed, the technological ordering of life through symbolic tokens, expert systems, and networked structures is an inevitable feature of late modernity and does not entail belief in technological determinism. Instead, we affirm the complexity of societal structures and the reality that we cannot get outside Max Weber's 'iron cage,' now become silicon web, a globally wired world of light and fibre optics. The ethical and social dimensions of the IT revolution follow the law on the relationship between technology and society proposed by Kranzberg: 'Technology is neither good nor bad, nor is it neutral' (Kransberg, 1985, 50). Technology is a force that penetrates the core of life and mind precisely because human consciousness-as-such functions in terms of means-ends relationships and mediates the self's orientation to the world within the subject-object split. The existential point is that every thing we produce in the course of new information and biotechnological development is a realization of human potential, freedom, and rationality. Applications of IT in the realm of social, political, and economic action are matters of human freedom and self-realization, rather than blind fate or technological determinism.

Human Rights in an Information Age

One of modernity's most significant achievements has been the founding of the United Nations and the rise of the international human rights movement. Even those who adamantly oppose rights rhetoric must admit that human rights structure the space, national and international, within which human beings attempt to construct an ethical order of universal and global scope. In the early post–Second World War era, the opposition between culture and human rights was far less strident than

it is today. This is not surprising, given the transformation of liberal democracy by informational politics. Liberal democracy based on collective solidarity has given way to neo-liberal critiques of the welfare state. The appeal is to communitarian values and responsibilities, over and against individual rights claims. Community 'volunteerism' and 'charity' are proposed as substitutes for the social safety net in the waning days of social contract policies. The funding of non-profit organizations through the provinces' addiction to gambling revenues feels like cultural regress, however, at a time when new models of informational entrepreneurialism hold out hopes for the individual to participate in the new economy. Despite serious theoretical and philosophical debates concerning the nature, ethical justification, and universality of human rights, concrete violations of human beings – through genocide, torture, disappearances, state policies of starvation, slavery, racism, mass rape, domestic violence against women, social discrimination, and economic deprivation – still cry out for care of and solidarity with victims of oppression. Our historical situation has changed, but the information age has not changed the human condition.

The historical developments that have led to the expression 'human rights' since the end of the Second World War and the founding of the United Nations in 1945 are as fascinating as they are complicated.[2] Scholars generally classify the contents of human rights in accordance with their evolution in modern international law. During the drafting of the UN Charter in 1945, the question of individual versus groups rights polarized many members. Should economic, social, and cultural interests be accorded the status of rights on par with the traditional liberal values of free speech, religion, press, and association? The drafters decided to draw up two separate covenants, one dealing with political and civil rights and the other treating economic, social, and cultural rights. With regard to implementing machinery, states could ratify either or both conventions with no obligation other than a periodic report. The two main international human rights covenants – the United Nations International Covenant on Civil and Political Rights (ICCPR) and the United Nations International Covenant on Economic, Social and Cultural Rights (ICESCR) – were eventually opened for signature in 1966 and came into force in 1976. Together with the Universal Declaration of Human Rights (UDHR) and the Optional Protocol to the ICCPR, these instruments constitute the so-called International Bill of Rights, which encompasses an expanding range of personal, legal, civil, political, subsistence, economic, social, and cultural rights. In

addition, various treaties and declarations elaborate on single-issue concerns such as genocide, the political rights of women, racial discrimination, and torture. Human rights scholars generally view these rights as interdependent, and states often speak of the norms of the UDHR and the covenants as binding, despite the fact that states often refuse to allow strong international enforcement and even monitoring of their performance. In none of the United Nations instruments is there any mention of the rank ordering of rights, except for those rights that are stipulated 'non-derogable,' such as the freedom from arbitrary or unlawful deprivation of life, freedom from torture and inhuman or degrading treatment and punishment, freedom from slavery, and freedom from imprisonment for debt.

It is commonplace to speak of three generations of human rights. First-generation human rights, as embodied in the ICCPR, stress civil and political rights over and against the encroachment of the state on individuals. Thus, human rights were initially conceived more in negative ('freedoms from') than positive terms ('rights to'). States undertake to respect and ensure rights to life and personal integrity, due process of law and a humane penal system, freedom to travel within as well as outside one's country, freedom of expression, religion, and conscience, cultural and linguistic rights for minority groups, the right to participate in government and free elections, the right to marry and found a family, the right to equality and freedom from discrimination. Second-generation human rights, embodied in the ICESCR, emphasize economic, social, and cultural rights. Under this covenant, states are to take steps 'to the maximum of available resources,' 'with a view to achieving progressively the full realization' of designated rights (article 2,1). They include the following rights: to work; to enjoy just and favourable conditions of work; to join trade unions; to social security; to protection for the family, mothers, and children; to be free from hunger; to have an adequate standard of living, including food, clothing, and housing, and the continuous improvement of living conditions; to the highest attainable standards of physical and mental health; to education; and to partake in cultural life. Third-generation human rights involve 'solidarity' among developing states as a group and among states in general. They are said to be collective rather than individual and include 'peoples' rights' to development, the right to a healthy environment, the right to peace, the right to the sharing of a common heritage, and humanitarian assistance, for example, articles 22, 23, and 24 of the African Charter on Human and Peoples' Rights (cited in

Welch and Meltzer, 1984). Despite the gap that separates the theory and practice of international human rights, global human rights remain a vital 'standard of achievement for all peoples and all nations.'

While human rights are viewed by some individuals as a mixture of western cultural imperialism, rampant moralism, and political selectivity, it must be admitted that the concepts of 'natural right,' the 'Rights of Man,' and 'human rights' are essentially western concepts, which does not invalidate claims to their universal appropriation – or their analogues in other cultures and societies – in order to support human dignity, equality, and social justice. For most individuals, human rights are not primarily a juridical matter, but are related to the dignity of individuals and the respect and protection necessary for vulnerable individuals. Much of the history of the human rights movement in this century may be understood as claims by the have-nots against the haves, and it remains to be seen whether, and to what extent, human rights discourse might develop into a new generation of informational rights. While the full social and economic impacts of the information age are debated, we know that markets, economic growth, the nature of work, and privacy protections are undergoing profound transformation. What remains constant are basic philosophical questions about the nature and ethical justification of human rights that transcend our historical situation.

The essential element in the human rights framework that we set forth below resides in the primacy of human action, and the conditions of freedom and well-being that ground human rights and condition the realization of human communication and mutuality. Action may be defined in this context as behaviour undertaken voluntarily in order to achieve a freely chosen goal; action is voluntary and intentional behaviour (Gewirth, 1978, 26–7). Human rights are a species of moral rights held equally by all persons simply because they are human. Human rights are entirely or mainly kinds of claim-rights, and a claim-right of one person entails a co-relative duty of some other person or persons to act or to refrain from acting in ways required for the first person's having that to which he has a right. The ultimate purpose of the rights is to secure for each person a certain fundamental moral status tied to agency, which is both the metaphysical and the moral basis of human dignity.

The human rights framework that follows is indebted to the 'ethical rationalism' of social-political philosopher Alan Gewirth, whose remarkable achievements in modern ethical theory and social, eco-

nomic, and political philosophy are highly underrated (Gewirth, 1978, 1982, 1996). Some philosophers reject any rational justification or epistemological ground for the existence of human rights,[3] while others posit the priority of the virtues over rights in contemporary ethical theory. MacIntyre (1984, 69), for example, maintains that belief in rights is tantamount to a belief 'in witches and in unicorns,'[4] and that the virtues should be given primacy in any contemporary philosophical ethic. There do exist criticisms of Gewirth's so-called ethical foundationalism and his argument to the Principle of Generic Consistency (Bambrough, 1984; Regis, 1984). These criticisms, however, stem mostly from a misunderstanding of the method and logical operations of his central argument to the principle of human rights or the Principle of Generic Consistency. Deryck Beyleveld (1991) has mounted a compelling response to critics of Gewirth's ethical rationalism that remains, in our view as well, largely unchallenged (cf. Boylan, 1999).

Structure and Ethical Justification of a Claim-Right

While philosophers have done much to clarify the concept of a right and its correlative duties following the work of legal thinkers like Wesley Hohfeld (Hohfeld, 1966 [1919]), they have not always addressed the difficult question of ethical justification. Intuitionists like Robert Nozick appeal to certain unalienable rights as self-evident 'side-constraints' (Nozick, 1974, 28–35). Institutionalists like H.L.A. Hart maintain that rights arise from voluntary transactions grounded in the formal or informal rules of institutions and promising (Hart, 1955). Interest-based theories of rights, divine-command theories (Maritain, 1951), and John Rawls's argument that individuals would choose certain basic rights in the original position behind a 'veil of ignorance' of their particular qualities or position within civil society (Rawls, 1971), all stand in sharp contrast to the human rights framework we adopt. A claim-right entails a correlative duty on the part of another individual or individuals to act or to refrain from acting in ways required for the right holder's having that to which he or she has a right. The full structure of a claim-right is given by the formula: *A has a right to X against B by virtue of Y.* Thus, there are five main elements to a claim-right, and every theory of human rights must address each one of these elements.

1. The *Subject* (A) of the right, that is, the person who has or holds it.
2. The *Nature* of the right. Human rights are normatively necessary,

personally oriented moral requirements. Human rights are primarily moral rights that become a legal or political idea only because of their supreme moral importance.
3. The *Object* (X) of the right, that is, what it is a right to.
4. The *Respondent* (B) of the right, that is, the person or persons who have the correlative duty to fulfil the right.
5. The *Justifying Basis* or *Ground* (Y) of the right (Gewirth, 1982, 2).

The Principle of Generic Consistency

The justificatory ground of human rights is a moral principle that establishes that all humans are equally entitled to have the necessary conditions of freedom and well-being in order to fulfil the general needs of human agency. The Principle of Generic Consistency (PGC) states: 'Act in accord with the generic rights of your recipients as well as of yourself. Generic rights are rights to the universal features of action – freedom and well-being – which constitute its necessary conditions' (Gewirth, 1982, 2–3; 1996, 19). Freedom and well-being are generic rights because they are rights to the necessary conditions not merely of one particular action as against another, but of all successful action in general. Many uphold human rights on the grounds that because human beings have dignity, they therefore have rights. The appeal to human dignity to ground a human right is not wrong, but it is circular in that there is a tautology in the expressions 'A has human rights' and 'A has inherent dignity.' Jacques Maritain's (1951) rights theory equates the dignity of the human person with rights in precisely this way. If these two expressions are equivalent in meaning, then the attribution of dignity adds nothing substantial to the attribution of rights. If a person is doubtful about the attribution of dignity, he or she will be equally doubtful about the attribution of human rights to individuals. As such, the argument for rights based on an inherent human dignity does not satisfy the requirement of non-circularity. This is not to say that human dignity is not important to our understanding of human rights, but to confirm only that dignity is also inextricably linked to action. Because *action* is the common subject matter of all morality and practice, every agent regards his or her purposes 'as good according to whatever criteria (not necessarily moral ones) are involved in his acting to fulfil them ... as rational, [one] regards as necessary goods the proximate general necessary conditions of his acting to achieve his purposes. For without these conditions he either would

not be able to act for any purposes or goods at all or at least would not be able to act with any chance of succeeding in his purposes. These necessary conditions of his action and successful action are freedom and well-being, where freedom consists in controlling one's behaviour by one's unforced choice while having knowledge of relevant circumstances, and well being consists in having the other general abilities and conditions required for agency' (Gewirth, 1982, 47).

A *dialectically necessary method* is required to argue the case for the Principle of Generic Consistency. The method is dialectical because it deduces conclusions from statements made or accepted by a 'prospective purposive agent' (PPA) about how he or she views things. PPAs are those who act voluntarily for purposes that they have freely chosen, as well as those who have the capacity to do so, which they have some disposition to exercise. The method is *necessary* in that statements made or accepted by every PPA logically derive from the generic features of purposive action. The method is different than an assertoric method, and the necessary feature of the method is different from a contingent ethical method:

> it is one thing to say assertorically that X is good; it is another thing to say dialectically that X is good from the standpoint of some person, or that some person thinks or says 'X is good.' Where the assertoric statement is about X, the dialectical statement is about some person's judgement or statement about X. But whereas the dialectical method is relative to individuals in this way, the dialectically necessary method propounds the contents of this relativity as necessary ones, since the statements it presents reflect judgements all agents necessarily make on the basis of what is necessarily involved in their actions ... The basis of this necessity is found in one or another aspect of the generic features of action and hence in the rational analysis of the concept of action. Thus, although the dialectically necessary method proceeds from within the standpoint of the agent, it also undertakes to ascertain what is necessarily involved in this standpoint. The statements the method attributes to the agent are set forth as necessary ones in that they reflect what is conceptually necessary to being an agent who voluntarily or freely acts for purposes he wants to attain. (Gewirth, 1978, 44)

The dialectically necessary method seeks to achieve categoricalness for moral judgments. Every agent, by the fact that he or she engages in purposive acts, is logically committed to the acceptance of certain eval-

uative and deontic judgments, and the PGC's requirement to *act in accord with the generic rights of your recipients as well as of yourself.* This revised neo-Kantian categorical imperative, now reinterpreted by Gewirth along the lines of action theory, requires that each agent respect his or her recipients' necessary conditions of action. The framework is concerned with the problem of moral emotivism and the interminable claims and counterclaims that arise in moral discourse. Gewirth seeks to bring moral 'dissensus' to a halt by recourse to facts and propositions that a PPA cannot reject because they are tied to the normative structure of action: 'First, every agent implicitly makes evaluative judgments about the goodness of his purposes and hence about the necessary goodness of the freedom and well-being that are necessary conditions of his acting to achieve his purposes. Second, because of this necessary goodness, every agent implicitly makes a deontic judgment in which he claims that he has rights to freedom and well-being. Third, every agent must claim these rights for the sufficient reason that he is a prospective agent who has purposes he wants to fulfill, so that he logically must accept the generalization that all prospective purposive agents have rights to freedom and well-being' (Gewirth, 1978, 48).

Now the aim of Gewirth's steps is to show that the agent's pursuit of purposive action commits an individual to accept several normative judgments on pain of self-contradiction, and that purposive action depends on its having a certain normative structure. The crucial step in the argument is the logical connection between necessary goods and rights. The argument undertakes to establish two main theses, which must be established if self-interested individuals are to accept the idea of human rights. The first is that every actual or prospective agent must logically hold or accept that he or she has certain rights to the necessary conditions of action. The second is that the agent logically must also accept that all other agents have these generic rights equally with his or her own rights. The move from the affirmation of freedom and well-being as necessary goods of action to the affirmation that these goods entail that human beings actually have *rights* to freedom and well-being is important. The transition from necessary goods to rights is dialectically necessary – that is, when we adopt the agent's own perspective and advocate or will that each of us as a prospective or actual agent must have freedom and well-being in order to act at all. It is this *act of the will* that transforms the necessary goods of freedom and well-being into prudential prescriptions having normative necessity:

> When this internal, conative view is taken, the logical gaps indicated above between judgements about necessary goods and ascriptions of rights are closed. The agent is now envisaged as saying, 'My freedom and well-being are necessary goods.' From this there does logically follow his further judgement, 'I have rights to freedom and well-being.' For the assertion about necessary goods is now not a mere factual means-end statement; on the contrary, because it is made by the agent himself from within his own conative standpoint in purposive agency, it carries his advocacy or endorsement. In effect, he is saying, 'I must have freedom and well-being in order to pursue by my actions any of the purposes I want and intend to pursue.' Thus his statement is prescriptive. (Gewirth 1982, 49)

Each person *qua* rational agent must claim these goods as necessary for attainment of his or her own ends. Each actual or prospective rational agent must take this step towards normative necessity, linguistically affirmed, because any agent who denies that he or she has rights to freedom and well-being contradicts himself or herself with respect to the need for freedom and well-being as necessary conditions for pursuit of purposive action.

Up to this point, Gewirth's argument to the PGC establishes the individual agent's *prudential* claim to be allowed to act to achieve his or her own ends without interference. Gewirth needs a further argument to show that each agent must admit that all other human beings have generic rights in order to reach the conclusion that freedom and well-being are not only prudential rights, but also *moral* and universal human rights. He reaches this conclusion by the logical generalization that 'if some predicate P belongs to some subject S because S has the quality Q (where the "because" is that of sufficient reason or condition), then it logically follows that every subject that has Q has P.' If P as the predicate 'has generic rights to freedom and well-being,' S is 'human beings,' and Q is the quality of 'being a prospective purposive agent,' then the generalization principle logically entails that all human beings *qua* prospective purposive agents have generic rights to freedom and well-being (Gewirth 1982, 52). Because all human beings are purposive agents, however widely agency is defined, the argument provides a rational basis for belief in equal and universal human rights to freedom and well-being. In turn, generic rights to freedom and well-being serve to ground universal duties: that every person ought to refrain from interfering with the freedom and well-being of all other

individuals, and that, under certain circumstances, every person ought *to assist* other individuals to have freedom and well-being when they cannot have them by their own efforts. Prospective moral agents must accept the PGC both for the formal reason that if any agent denies or violates the principle, then the agent contradicts oneself, and for the material reason that the PGC's contents necessarily impose themselves as correlative duties on every agent who pursues purposive action. There are two final stages in Gewirth's argument. The first concerns the specific *contents* of rights and how they are *related* to each other, while the second concerns the *political effectuation* and *legal enforcement* of rights. Both sets of concerns are related to Gewirth's important distinction between direct and indirect applications of the principle of human rights (Gewirth, 1982, 60–2).

Direct and Indirect Applications of the PGC

In the direct applications of the PGC, its requirements are imposed on the actions of individual agents. Actions are morally right and the agents fulfil their moral duties when they act in accordance with the generic rights of their recipients as well as of themselves. In the indirect applications, on the other hand, the PGC's requirements are imposed in the first instance on social rules and institutions. Such rules and institutions are morally right, and persons acting in accordance with them fulfil their moral duties when the rules and institutions express or serve to protect or foster the equal freedom and well-being of the persons subject to them. Thus, by the indirect applications, recipients may be even coerced or harmed, but this does not violate their generic rights to freedom and well-being, because the rules and institutions that require such correction or harm themselves are justified by the PGC. The indirect applications of the PGC are of two kinds. The *procedural* applications derive from the PGC's freedom component and provide that social rules and institutions are morally right insofar as the persons subject to them have freely consented to accept them or have certain consensual procedures freely available to them. The *instrumental* applications derive from the PGC's well-being component and provide that social rules and institutions are morally right insofar as they protect and support the well-being of all persons equally.

Each of these indirect applications entails two further distinctions. The procedural applications may be either *optional* or *necessary*. They are optional insofar as persons consent to form or to participate in

entirely voluntary associations. The procedural applications are necessary insofar as individual consent operates as a general decision-making procedure. In this context, consent entails using civil liberties to provide the authoritative basis, through elections and other consensual methods, of specific laws or governmental officials.

The PGC's instrumental applications may be either *static* or *dynamic*. The static applications, embodied in the so-called 'minimal state' with its criminal law, serve to protect persons from occurrent violations of their rights to basic goods and other important goods – including the rights to life, physical integrity, and reputation – and to punish such violations. The PGC sets standards or limits as to how this protection is to operate, so that only persons who have violated these rights of others are to be punished: All persons must be equal before the law, trials must be fair, *habeas corpus* must be guaranteed, and human punishment must not be cruel, vindictive, or inhuman. The dynamic applications, embodied in the supportive welfare state, or what Gewirth calls the 'community of rights,' serve to provide longer-range protections of basic and other rights where these cannot be obtained by persons through their own individual efforts. The dynamic-instrumental justification of social rules recognizes that persons are dispositionally unequal in their actual ability to attain and protect their generic rights, especially their rights to basic well-being, and provides for social rules that serve to remove this inequality. These supportive rules have several kinds of content that provide for supplying basic goods, such as food and housing, to those persons who cannot obtain them by their own efforts. They try to rectify inequalities of additive well-being by improving the capabilities for productive work of persons who are deficient in this respect. They provide for various public goods that, while helping all the members of the society, serve to increase the opportunities for productive employment, in addition to regulating certain conditions of well-being by removing dangerous or degrading conditions of work and housing.

Basic, Non-substractive, and Additive Goods

To understand the specific objects of rights and duties and how they are related to each other, we must understand Gewirth's hierarchical orderings of the generic right to well-being. 'Basic' well-being consists in having the essential preconditions of action and includes basic rights to life, physical integrity, and mental equilibrium. 'Non-

substractive' well-being consists in having the abilities and conditions necessary to maintain one's general level of purpose-fulfilment and capacities for action. For example, a person's non-substractive rights are violated when he or she 'is adversely affected in abilities to plan for the future, to have knowledge of facts relevant to projected actions, to utilize resources to fulfill wants, and so forth' (Gewirth 1982, 56). 'Additive' well-being consists in having the conditions and abilities necessary for actually augmenting or increasing one's purposes and capacity for action. Additive well-being entails rights to education, self-esteem, and opportunities for acquiring an income and wealth. A person's additive rights are violated 'when a person's development of the self-regarding virtues of courage, temperance, and prudence is hindered by actions that ... contribute to misinformation, ignorance, and superstition' (Gewirth 1982, 56).[5] As we will argue further, below, covert surveillance practices and the disinformation characteristic of information warfare, as well as privacy violations stemming from informational omissions, all are examples of potential harms in relation to these goods and the generic right to well-being.

The Criterion of Degrees of Needfulness for Action

From the PGC derives an important criterion for the resolution of the conflict of rights, that is, the *'criterion of degrees of needfulness for action'* (Gewirth, 1996, 45–54). According to the criterion, when two rights conflict, that right takes precedence whose object is more necessary for action. Thus, rights not to be stolen from or lied to are overridden by the rights not to starve or be murdered, if the latter rights can be fulfilled only by infringing on the former. Many of the problems concerning the specification and adjudication of cyberspace rights and responsibilities may be illuminated by this criterion. Rights of physical access and/or access to content and services on the information highway may be viewed as 'additive' goods – if not 'non-substractive' goods – because such access is necessary for increasing the agent's capacity for action and ability to make a living in the informational economy. As such, the right of access to information is a logical extension of the generic goods and rights of freedom and well-being as necessary conditions of human action. This criterion does not resolve all existing or future problems of specifying norms for information policy, but both the criterion and an action-based human rights framework in general take us much further than existing ethical approaches.

The PGC and the Universal Declaration of Human Rights

Gewirth construes his argument to the Principle of Generic Consistency[6] as a rational reconstruction of the Universal Declaration of Human Rights because his generic rights coincide extensionally with social, economic, and cultural rights, as well as political and civil rights. However, there are two important differences. First, the objects of the PGC's rights apply not merely to social institutional arrangements, but also, in the direct applications of the PGC, to individual interpersonal transactions such as rights not to be lied to or not to have promises broken. Because the PGC aims to have all individuals possess the abilities and conditions required for action, and generally successful action, the generic rights apply to the individual as well as to the social sphere. There is a second key difference. The United Nations' rights are addressed almost exclusively to governments as the 'respondents' of human rights. The PGC's rights, in contrast, are addressed primarily to each individual to the extent that they have the relevant abilities to comply with the duties of the PGC, as well as governments acting as representatives of their citizens. Human rights are universal, because all the subjects and respondents of rights are human beings, though this feature does not mean that all of the PGC's human rights are, or even ought to be, legally enforceable.

With respect to the political effectuation and legal enforcement of rights, as noted above, four general kinds of social rules and institutions conform to the PGC. 'Voluntary associations' and 'the democratic state' – through the latter's use of consensual procedures – are the locus for applications of the right to freedom. The 'minimal state,' which embodies the criminal law, and the supportive welfare state, or 'community of rights,' which provides basic goods such as food and shelter to those who cannot obtain them by their own efforts, as well as education and other additive goods, are indirect applications of the right to well-being. A main line of ethical specification that we will pursue further in chapter 5 is the role that privacy and security rights play in promoting and protecting basic, non-substractive, and additive goods.

Negative and Positive Rights

Substantive philosophical debate surrounds the nature and ethical justification of human rights, especially the distinction between negative

and positive rights (Winston, 1989). The distinction turns on the duties of the respondents of rights. In the case of negative rights, respondents, whether individuals or the state, have duties to refrain from interference. They need not actually do anything. In the case of positive rights, respondents have duties to provide active assistance, such as the provision of funding with which to fulfil the requirements of a right to education; economic assistance; and other aid for individuals who cannot obtain basic and other action-related goods such as food, housing, income, and health care by their own efforts.

Numerous objections have been raised to the notion of positive rights, including the idea that there cannot be positive rights because they are inconsistent with the human right to freedom. Limitations on the freedom of the rich through taxation policies are justified, however, on the basis of the rationally grounded obligation to assist the needy. Critiques of social welfare policies often merely assume that there must be a permanent class of welfare dependants, whether domestic or international, and that charity is the most appropriate response. The history of social assistance in the province of Quebec and elsewhere reveals the limitations of this view. Another criticism is that positive rights are impracticable because of the overload of duties they entail. To be sure, rights must take into account the empirical conditions of their possible effectuation, which is why the correlative duties entailed by positive rights belong in the first instance to governments. Again, it is argued that positive rights do not meet the test of universality, including the view that Third World countries are too poor to provide the objects of rights such as education, medical care, and even food (Sidorsky, 1979). It is certainly the case that an individual cannot be both a rescuer and the rescued, be both starving and have the duty to relieve starvation. The issue, however, is whether or not all rational individuals have a right, as a matter of ethical principle, to be treated in an appropriate way when they have the need; and whether individuals have the duty to act in accordance with a positive right when the circumstances arise that require such action and when they have the ability to so act. The question of whether rights are universally exercised (which they are not) must be kept separate from whether they are universally held by all individuals (which they are).

Conceptual clarification of the distinction between negative and positive rights is important, because the human 'right to development' consists in obtaining the abilities needed for earning income so that individuals might become relatively autonomous or self-sufficient

with regard to well-being in the informational economy (chapter 3). The right to employment is a further specification of rights to basic and additive well-being (Nickel, 1978/9). A positive right and duty regarding employment can be traced back at least to the work of Thomas Paine, who upheld employment 'at all times for the casual poor in the cities of London and Westminster' (Paine, 1969 [1791/2], 280). In the twentieth century Franklin Roosevelt's economic bill of rights upheld 'the right to a useful and remunerative job in the industries or shops or farms or mines of the nation' (cited in Harvey, 1989, 127). Article 23 of the UDHR states that '(1) Everyone has the right to work, to free choice of employment, to just and favourable conditions of work and to protection against unemployment. (2) Everyone, without any discrimination, has the right to equal pay for equal work. (3) Everyone has the right to just and favourable remuneration ensuring for himself and his family an existence worthy of human dignity, and supplemented, if necessary, by other means of social protection. (4) Everyone has the right to form and to join trade unions for the protection of his interests' (cited in Brownlie, 1981, 25). While the right to employment is hardly discussed in our present historical situation, it is hard to deny the importance of work to human dignity and existence, whether in an agrarian, industrial, or informational mode of development.

The Right to Productive Agency

Positive rights begin with a person's right to productive agency. Productive agency is 'the agent's ability to achieve the outcome she desires or intends, and a productive agent is one who does thus achieve it' (Gewirth, 1996, 132). Productiveness is used here synonymously with additiveness and well-being. By additive well-being, an individual increases his or her capacity for purposive agency and general development of purpose-fulfilment. For most of us this implies, as a necessary if not sufficient condition, that we have or are able to acquire wealth or income sufficient for protecting a certain level of freedom and well-being. Productive agency is imperative for the development of skills that can lead to employment and the flourishing of economic and political democracy in western, liberal states. It is also a vital condition for developing virtues of courage, fortitude, perseverance, personal responsibility, prudence, and justice. The right takes on special urgency in a historical situation where improved productivity increases competitiveness, and modes of economic development refer to elements crucial

for fostering productivity in the production process. In the informational mode of development, the source of productivity lies in the technology of knowledge generation, information processing, and symbol communication with the action of knowledge upon knowledge being the main source of productivity. The shift from industrialism to informationalism does not render the right to productive agency obsolete, but instead redefines it in an informational mode of being.

A key ethical question, therefore, is the condition of possibility for exercising individual productive agency and the equality of human rights in the information age. At a minimum, 'mutuality' with respect to freedom and well-being involves equal protection for individuals' procedural and substantive abilities of agency. The equal protection of procedural abilities bears on issues such as whether or not individuals can control their own lives and behaviour without being dominated by other individuals and whether or not they have effective use of civil liberties. The equal protection of substantive abilities bears on issues such as whether or not individuals have an adequate supply of basic goods and whether they can develop their productive agency so as to secure livelihoods for themselves and their families.

Moreover, in the informational age, demand for developing productivity continues increasingly to transform educational development into IT training and reskilling. From kindergarten to university, the Internet is overlaid on an educational domain that has been awash in change for several decades. Non-profit educational institutions increasingly give way to commercial vendors. Relatively autonomous instructional and learning processes cater more directly to labour markets and corporate practices such as the growing utilization of casualized labour, productivity enhancement measures, and product development based on profit and loss potentials. Policy reforms towards school-to-work programs, lifelong learning, and partnerships are partially symptoms of educational vocationalization. For this reason, questions about the nature of information, to what end information ought to be directed, and the relation of information to human rights that we raised in the introduction are as vital to our present situation as they are urgent.

The Community of Rights, Mutuality, and Social Solidarity

Positive rights provide the underlying grounds for the 'community of rights' needed to protect human dignity amid the radical transformations of the information age:[7] 'The community of rights is a society

whose government actively seeks to help fulfill the needs of its members, especially those who are most vulnerable, for the freedom and well-being that are the necessary goods of human agency, when individuals cannot attain this fulfillment by their own efforts' (Gewirth, 1996, 5). Human rights and community have a relation of mutual support. Community protects and fulfils human rights on the basis of mutuality and the social solidarity of individuals who recognize and fulfil common needs. Human rights require community for their implementation, while community requires human rights as the basis of its morally justified economic, political, and social operations and enactments. Community entails an institutionalized social bond that unites individuals by virtue of their society's fulfilment of important needs of agency and individuals' mutual contributions thereto.

The community of rights is used synonymously with a renewed vision of the social democratic state towards which a normative political, social, and economic ethics would aspire. It embodies the 'minimal state' and is democratic through its use of consensual procedures that attempt to embody generic rights to freedom and well-being. The community of rights is also a 'supportive state' grounded in mutuality and solidarity. If the community of rights was difficult to attain in the post–Second World War period, which was marked by the rise of the democratic welfare state, then it may be even more difficult to attain in the new informational economy, where states have far less control in redistributing social goods and services. The information age may prove, paradoxically, to make it increasingly difficult for individuals to realize participatory social citizenship.

According to McChesney, Castells, and Fukuyama, mutuality and social solidarity are fading amid deregulation, the downsizing of the public service, the loss of public space to the private sector, and the privatization, informational commodification, and increasing surveillance of public space. The need for mutuality on the part of all members of society constitutes the ethical foundation of the community of rights. A rational agent's recognition and support of other individuals' positive rights does not have reciprocity or a *quid pro quo* framework as its philosophical ground. The ground is mutuality and a necessary matter of individuals' common humanity as purposive agents. The individual recognizes that other individuals are similar in being purposive agents having needs of agency and rationally accepts that others have the same positive rights that he/she personally claims. It is the mutuality of human rights that conciliates rights and community.

> Mutuality entails equality, but not conversely. Both equality and mutuality are symmetrical relations. But whereas equality may be confined to static, noninteractive relations between persons, mutuality is a dynamic, interactive relation. A and B may have equal amounts of some X without interacting with one another. But in a mutual relation, A gives some valued X to B and B gives some other kind of valued X to A. This relation is exemplified in, but is not confined to, some forms of economic exchange. Thus A and B are equal as participating in this interactive relation, and, so far as practicable, the respective amounts of X are also equal. It is this mutuality that figures in the principle of human rights where, in principle, all humans are both the subjects and the respondents of rights, in that each human respects and protects each other human's interests in freedom and well-being ... qualifications about practicality and governments must be kept in mind, but they do not remove the mutualist principle with its import for the community of rights. (Gewirth, 1996, 75)

If rights are the contents of justice, then equality and mutuality provide the formal conceptual framework that determines how those contents are to be distributed. The PGC as the principle of human rights is a principle of both material and comparative justice. In the tradition of giving each person his or her due, the PGC is a principle of material justice. In accordance with comparative justice, the PGC requires that all individuals be treated similarly by virtue of being prospective purposive agents, that is, we must treat like cases alike. A *prima facie* egalitarian universality is not a part of the concept of a right as such, however, because many societies have provided recognition and legal enforcement of rights, but they are distributed only among a small group of individuals. Even when legal rights have been universally distributed, often they have not been held equally. Although constitutions proclaim that 'all men are created equal,' we know that some individuals are, in fact, more equal than others. So whatever other rights persons may have, all have a right to a fundamental equality of positive consideration for their dignity.

The mutuality entailed by human rights also serves to ground individuals' self-respect. In the recognition that I am both a subject and a respondent of human rights, I may see that I fulfil my obligation to help others to secure their rights to the necessary conditions of their actions, and that they also hold the correlative rights and responsibilities entailed. The ethical requirement that governments promote and protect human rights, and thereby enable all humans to have the nec-

essary goods of action, is also a consequence of the mutuality of human rights. Governmental provision is vital to what constitutes a morally justified state as a community of rights.

Our philosophical human rights framework acknowledges the primacy of human agency, a rational community ideal and the mutuality of rights and duties it entails, and a vision of human communication grounded in freedom, well-being, and social solidarity. The framework is realistic about the nature of human conflict within the state and the role of inevitable struggle as a limit situation of the human condition. We cannot avoid conflict between states, within society, with other individuals, and even within the self. Conflicts may be a source of defeat or a limitation of our potentiality, but they may also lead to great depths of living and the birth of more far-reaching unities that spring precisely from the tensions that engender them. In this respect human life is a two-edged sword. We react to concrete situations, facts, and people. In our reactions we are also active and creative in the ways in which we confront the situation. It is not entirely correct to view action and reaction as opposed, just as it is impossible to imagine the possibility of human creativity that is divorced from some object-less activity. While some individuals today view human rights discourse as always reactive or ideologically motivated to serve merely individual or special-group interests, we have seen that this 'adversarial conception' of the relation of human rights and community is wrong both theoretically and practically. It is wrong theoretically, because human rights and community have a relation of mutual support, and wrong practically, because the conflicts generated by the information age may well lead to creative, cross-cultural communication.

The general purpose of this work and the nature of our human rights framework should now be clear. On the supposition that philosophical reflection must begin with the present historical situation, we have identified the unfolding of the information age within the historical context of modernity, the global impact of technology on persons and cultures, and the challenges the technological revolution raises for traditional questions about the nature of the human being, the impact of technology upon the self, modes of rationality, and the limits of cognition in the light of human historicity and finitude. Every new technical creation confronts us with new situations and raises the questions: what we will make of our situation, how we will act in it, in what sense we will master or succumb to it, and how we will mutually respect the

rights and responsibilities of persons in their needs for basic freedom and well-being as the necessary conditions of purposive action.

The positive technological transformations of modernity and the information age have also left us with basic philosophical questions of the meaning of our age and the social impact of technological developments on self, society, and culture. Reflexively planned existence is an inevitable feature of modernity, but the roles of trust, mutuality, and solidarity are often given short treatment. The epistemological contours of modernity have been driven and shaped by 'intellectual' thought or instrumental rationality. Is there space for that other kind of thinking, rational thinking, that does not reduce human will to means-ends relationships or reduce the human person to a function of the technological order or an object for potential commodification? Science and technology hold out new possibilities for human development and freedom, but technological developments should be placed under ideals of rationality and ethics, a healthy sense of human humility and finitude, and the limits of cost-benefit analysis and risk assessment.

The crucial aspect of our human rights framework resides in the primacy of human action and the conditions of freedom and well-being that both justify human rights and condition the possibilities for enhanced communication between persons. Can a human rights framework provide a richer philosophical justification for the debates surrounding Canadian information highway policy and the impact of IT on work and employment, privacy and security concerns, and emerging information warfare practices? We argue that it can do so, even as numerous commentators agree that we need more ethical reflection on the information technology and biotechnological practices that will continue to unfold in the twenty-first century and thereby directly affect productive agency and the rights and dignity of persons. We know that the privacy policy solutions of the past are not entirely adequate to present and future surveillance challenges. The statutory codification of fair information principles, their application to organizations that process personal data, and oversight and enforcement by independent data protection agencies are necessary, yet insufficient, developments for the implementation of privacy protection today and in the future. Greater ethical specification of the principle of human rights, further clarification and application of basic, non-substractive, and additive goods to new information technologies, and the application of the criterion of degrees of needfulness for action are

urgently needed. An application of the principle of human rights to the ethical challenges of Canadian information highway policy and e-commerce strategy, to which we now turn, will take us a long way towards the much needed 'balance' between individual rights and social interests and responsibilities in the information age.

CHAPTER TWO

Information Highway Policy and E-Commerce Strategy

In this chapter we present an exposition and analysis of Information Highway Advisory Council (IHAC) policy and e-commerce strategy. Information highway policy did not appear out of the blue, but it must be situated within the broader historical emergence and sociological development of Canadian communication sectors, technology, and policy. The history of Canadian telegraph, telephone, and broadcasting industries and restructuring has been explored by others.[1] The scientific foundations, key players, and legal dimensions of early information highway policy are examined by Johnston et al. (1995),[2] but they fail to treat the second- and third-phase policies and provide no ethical analysis. We begin by identifying the relevance of the public policy product cycle to information policy. In turn, our historical exposition brings into focus the key policy issues that surface across all three policy periods. A methodological conclusion confirms our choice of focus on the three substantive policy issues that follow, while the ethical analysis engages several other policy issues not directly dealt with in the remainder of the book.

The Public Policy Product Cycle

The development of a body of knowledge reflects shifting emphases and changing foci within a field over time. Just as there is a product cycle in the development of tangible goods, there is also a knowledge product cycle that spans a variety of policy issues ranging from the economy to defence, energy and the environment, and health care and science policy. The development of information highway policy is no exception. Wilson (1997) defines four main phases of the public policy

product cycle that provide a useful heuristic for understanding the emergence of information and e-commerce developments during the 1990s.

The *first phase* is a technical phase in which complex technical issues move from public bureaucracies to the public realm and onto the agenda of senior policy analysts. In the United States, for example, the 1973 energy crisis, environmental pollution of the Love Canal, and nuclear power policy after Three Mile Island politicized complex technical issues and garnered greater public attention.

In the *second phase*, social theorists and journalists take up emerging issues with their differing purposes, agendas, and audiences. Analyses at the second stage are often utopian, apocalyptic, or hyperbolic, and they focus on the positive attributes of some technologies for advancing democracy or revolutionizing the world. Information guru George Gilder, for example, could confidently assert that information technologies 'will blow apart all the monopolies, hierarchies, pyramids, and power grids of established industrial society ... [and] undermine all totalitarian regimes. Police states cannot endure under the advance of the computer because it increases the power of the people far faster than the powers of surveillance. All hierarchies will tend to become "heterarchies" – systems in which each individual rules his own domain. In contrast to a hierarchy ruled from the top, a heterarchy is a society of equals under the law' (cited in Drake, 1995, 10). Gilder makes utopian predictions concerning 'the most deprived ghetto child in the most blighted project' gaining educational opportunities that 'exceed those of today's suburban preppie' (Gilder, 1994). Michael Vlahos's (1998) 'Infosphere' thesis is only slightly less utopian. Complex and chaotic shifts surrounding IT developments involve the migration of identity and a revolution of place: 'Migration is human passage, the move from one place of identity and belonging to another ... Revolution is the ratification of the place that change makes ... achieved through social political theatre in which a new elite takes on the authority of leadership ... Revolutionary theater is necessary to resolve the complex conflicts unleashed by migration'(Vlahos, 1998, 497–8). Infosphere is his symbol for the fusion of communications networks, databases, and sources of information into a vast, intertwined and heterogeneous tapestry of e-interchange. Infosphere is a 'new city' that gathers together people and knowledge, a totality, an 'all-encompassing' reality. We can overcome resistance to the change sweeping across the digital city only if we meet the fear of chaos with cultural creativity. Infosphere creates fear of

losing the place we grew up in, our sense of self, ties to a job and work, and the continuity of everyday connectedness to community or nation. Somehow, some day, Infosphere will restore lost jobs, our sense of identity and history, old and new forms of art, and even romance – presumably once domination by the cyber porn marketeers withers away.

The *third phase* of the policy cycle is marked by non-technological concerns brought to the policy table by a wider group of social scientists. Institutional, political, and distributional issues are raised and debated. Analysts acknowledge that IT diffusion rates will be shaped by existing political and economic institutional incentives and regulatory environments. Government ownership and control of the IT industry gives way to private sector control (Frank and Cook, 1996). Social scientists and humanities scholars begin to analyse the dark side of the policy revolution for the poor, while information haves and have-nots get put on national and international agendas (Arunachlam, 1998).

In the *fourth phase*, dialogue and debate are extended to scholars who are primarily university based, who take up wider social concerns. They test traditional concepts and hypotheses and make interdisciplinary connections. In the process, a certain normative social science analysis takes place and adds to an expanding literature. A gulf is established between the almost exclusively technical approaches of the first phase and the broader academic approaches of the fourth phase.

The policy cycle serves as a methodological heuristic for contextualizing Canadian communication and information highway policy. Critical analyses of global information migration and numerous national information infrastructure initiatives are moving somewhere along its trajectory. We judge that I-way policy has moved through the first three phases, and if the Owl of Minerva takes flight only at dusk, then the fourth policy phase is now dawning.

Historical and Sociological Specifications of Canadian Communications Policy

During the late 1980s and early 1990s governments around the world recognized the fundamental changes under way in the IT field. 'Convergence' challenged governments to recognize a Global Information Infrastructure (GII). National policy initiatives that followed in the wake of the GII were marked by an extraordinarily broad IT scope, as well as unprecedented engagement with the private sector in the provision of resources. The Canadian information infrastructure debate

was launched within weeks of President Clinton's 1993 announcement of the U.S. national information infrastructure (NII), which attempted to marry non-market public policy objectives and market forces (Raboy, 1997). An NII refers to 'the computerized networks, intelligent terminals, and accompanying applications and services people use to access, create, disseminate, and utilize digital information' (Drake, 1995, 5). Academics will recall using the Internet for research and e-mail long before its commercialization and commodification. Since the late 1980s most government NII policies were driven by business interests and demands that formulated a policy vision with implementation strategies such as regulatory frameworks, tax incentives, privatization, and research funding (Kahin and Wilson, 1997).

The historical emergence and development of Canadian information policy spans a large array of issues, such as access, broadcasting policy, censorship and intellectual freedom, communications policy, content/cultural policy, education and training policy, government information policy, information industry policy, national information policy, the policy process itself, and workplace information policy (Nilsen, 1997). In its early years, the Canadian telegraph industry (dominated by the Canadian Pacific (CP) Telegraph Company) and the daily press were integrated, because newspapers depended on telegraph companies for both transmission services and news content. In 1910 the Canadian Railway Commission ruled that CP Telegraph's arbitrary price increases were discriminatory, and the separation of content and carriage was begun on the basis of a regulatory ruling, not technological developments per se. For many years the Canadian National Telegraph Company (a Crown corporation) and the CP Telegraph Company held a duopoly in Canada. In 1932 they established the nationally interconnected Trans Canada Telephone System (known today as Stentor Telecom Policy, Inc.), which in 1980 culminated in a partnership, CNCP Telecommunications.

The historical origins of the telephone industry date back to 1879 and telegraph companies such as Dominion Telegraph, Montreal Telegraph, and Western Union. Canadian telephony fell under U.S. control very early, when in 1880 U.S. Bell appointed the Bell Telephone Company of Canada to work its exclusive patents. Bell lost its patents on grounds of importation and refusal to sell telephone instruments (since it leased them), but it retained rights 'to construct telephone lines along any and all public rights of way, even in the absence of municipal or provincial authorization' (Babe, 1995, 189). Independent telephone

companies required consent from appropriate levels of government in order to construct their systems. Although there was strong growth of independents (676 companies) in the province of Ontario between 1906 and 1915 (Grindlay, 1975), Bell eventually halted, then reversed, their growth by means of long-distance interconnection and pricing and local 'rate rebalancing' policies. In 1979 CNCP Telecommunications gained access to Bell's local switched network for certain data and private-line voice services as a result of the Canadian Radio-televison and Telecommunications Commission Telecom Decision CRTC 79-11 (CRTC, 1979). In 1992 the CRTC broadened the parameters of the 1979 decision, permitting the sharing and reselling of long-distance voice service and lines, which gave rise to numerous long-distance resellers and value added carriers. In 1994 the CRTC's famous 'Review of Regulatory Framework' increased flexibility for the telecommunications companies, removing barriers to entry by cable companies and restriction to local markets. 'Open access' and 'interoperability' principles among networks, that is, 'Information Highway' principles, were promoted (CRTC, 1994, 16–17).

Communications scholar Robert Babe (1979) clarifies three distinct phases that structure the broadcasting industry. The first phase (1920–32) was marked by unregulated market forces. The second phase began in 1932, when the federal government responded to the 1929 Aird Royal Commission on Radio Broadcasting by creating the Canadian Radio Broadcasting Commission (CRBC). The CRBC was subsequently superseded by the Canadian Broadcasting Corporation (CBC) in 1936. The Broadcasting Act, adopted in 1932 and revised in 1991, states that all broadcasting is to be 'a public service essential to the maintenance and enhancement of national identity and cultural sovereignty' (article 3). Comprising public, private, and community elements, Canadian broadcasting must be owned and operated by Canadians (with foreign ownership restricted to 20 per cent); make use of Canadian resources; and serve the needs, interests, and circumstances of Canadians, including equal rights, linguistic duality, multiculturalism, and Aboriginal peoples. According to the 1993 Telecommunications Act, telecommunications perform 'an essential role in the maintenance of Canada's identity and sovereignty' (article 7), including safeguarding, enriching, and strengthening the social and economic fabric of Canada and its regions; providing accessible services; enhancing the efficiency and national and international competitiveness of Canadian telecommunications; promoting ownership and control of Canadian carriers and transmission

facilities by Canadians (foreign ownership is capped at 33⅓ per cent); fostering increasing reliance on market forces while ensuring regulation if required; responding to the socio-economic needs of users; and protecting privacy.

National development and industrial development have been the key policy poles since 1969. The backbone of cultural policy was the broadcasting system, designed to ensure a strong Canadian presence on radio and television. Industrial policy sought to develop communication infrastructure through the use of satellites. In 1969 the Department of Communications set up a task force known as the Telecommission to study national telecommunications policy. Their 1971 report, *Instant World*, was the official harbinger of the Information Revolution in Canada: 'Technology has fundamentally transformed the human condition twice before [reference being to the Agricultural and Industrial Revolutions] ... How the third technological revolution will shape our ends is still far from clear but its nature and substance are already becoming familiar ... Ours is ... a society built upon and shaped by technology' (Canada, Department of Communications, 1971, 24–5; cited in Babe, 1995, 183).

The third broadcasting phase was characterized by the decline of public broadcasting in 1958 after the government established the Board of Broadcast Governors (BBG), which would be responsible for broadcasting regulation. The government authorized the creation of a second television network (CTV) made up of private stations, which diminished the role of the public sector. In 1968 the CRTC replaced the BBG. The CRTC's mandate was to administer the shift from public to private sector broadcasting and to oversee the 'convergence' of cable, satellite, and information highway networks. Three conclusions may be drawn:

> 'First, media of communication in Canada have seldom been controlled within the country ... the Canadian broadcasting industry is still largely dominated by the US entertainment industry. Second, the historical record belies the doctrine of a *technological imperative* in Canadian communications ... publishing, telegraphs/telephones, and broadcasting – had common roots and diverged only on account of agreements dividing markets and government policy ... industry structurings were part and parcel of *the struggle for power* by contending interests ... the convergence, or to be more precise, reconvergence, taking place today is not technologically-induced either, but stems rather from corporate and/or governmental

> *power-plays*. Third, communications technologies are highly flexible ... Those in control of technologies can do with them largely what they wish. Once goals have been formulated, technologies can be deployed to pursue certain ends.' (Babe, 1995, 195; emphasis added)

In Babe's view, the federal Department of Communications, Industry Canada, and private industry sector Stentor equally mythologize technology by promulgating a 'technological imperative' and 'technological determinism.' The technological imperative states that technological developments are inevitable and that human choices are severely constrained. 'Technological determinism contends that all important human phenomena – cultures, distribution of power, belief systems, industry structures – are produced by Technology' (Babe, 1995, 181). When combined with the doctrine of technological imperative, the myth of technological determinism sees technology as developing independently of human free will and choice. The policy implications of these dual doctrines of techno-dependency entail a faith in technology as an active phenomenon, while human regulators and legislators are merely passive recipients of inevitable technological progress. Technology comes to have a life of its own. The best that humans can do is appropriate technics and adapt to the inevitable onslaught of technological developments. Jacques Ellul, whom Babe cites approvingly, ironically describes this deterministic world view as an insidious 'ethics of adaptation': 'Since technique is a fact, we should adapt ourselves to it. Consequently, anything that hinders technique ought to be eliminated, and thus adaptation itself becomes a moral criterion' (Ellul, 1980, 243).

The negative consequence of such mythologization is to divert attention to technology and away from the corporations and governments that exercise control over the distribution of economic, political, cultural, and communicatory power and policy. In order to overturn the doctrine of technological imperative and to demythologize the myth of technological determinism, we should never forget that technologies are also means for attaining, exercising, and aggrandizing power. 'Once elites responsible for their introduction and deployment are identified, then a dialectic of political dominance and political dependence substitutes for myth. Awareness of "the soiling trace of origin or choice" politicizes and de-mythologizes technology, permitting groups disadvantaged by "technological evolution" (for instance, labour displaced by capital, customers and suppliers disadvantaged by "natural

monopolies," nations subjected to foreign cultural hegemony, producers and users of public services marginalized by producers and users of private commodities) to become more strident and confident in their opposition' (Babe, 1995, 184).

Industry Canada and the Information Highway Advisory Council

The role of Industry Canada (IC) is crucial to an understanding of the origins of the recent information highway (I-way). Industry Canada is mandated to foster 'the development of Canadian business, by promoting a fair and efficient Canadian marketplace and by protecting, assisting and supporting consumer interests' (Ferguson, 1994, 219). On 18 January 1994, in the Speech from the Throne, the Government of Canada announced the development of its information highway strategy. In March 1994 IC Minister John Manley created an Information Highway Advisory Council (IHAC) to assist the federal government in developing and implementing a strategy for the Canadian information highway. The twenty-nine-member council, with twenty-six ex officio members, was chaired by David Johnston, former principal and Vice-chancellor of McGill University and professor of law at McGill's Centre for Medicine, Ethics and Law. Johnston applauded the IHAC committee members for reflecting a wide range of knowledge and expertise, including diverse perspectives on linguistic, cultural, and regional issues. Critics, including communications scholars and spokespersons from national public interest groups, maintained that the council was dominated by the primary stakeholders in the broadcasting, cable, and telecom industries, and that issues concerning equity, democratic participation, social justice, and employment were almost entirely dismissed. At this stage, 'information highway' included the means of information conveyance (or carriage) and content (Angus and McKie, 1994) and denoted the advanced information and communications infrastructure that would become a '"network of networks," linking Canadian homes, business, governments and institutions to a wide range of interactive services from entertainment, education, cultural products and social services to data banks, computers, electronic commerce, banking and business services' (IC, 1994a, 1). The 'network of networks' refers to the converging of cable and satellite television; digital and traditional airwave radio; broadband, narrowband, and cellular telephone; local area networks (LANs); wide area networks (WANs); and databases.

IHAC initiatives expressed an optimistic view of the I-way as essential for Canada's economic success. The three key policy objectives – 'creating jobs through innovation and investment in Canada, reinforcing Canadian sovereignty and cultural identity, and ensuring universal access at reasonable cost' (IC, 1994a, 1995b) – roughly corresponded to the parallel yet overlapping interests of industry, the state, and civil society, respectively. Four principles guided the development and implementation of the Canadian I-way as an 'interconnected and interoperable' network of networks, 'collaborative public and private sector development' marked by 'competition in facilities, products and services, and 'privacy protection and network security' (IC, 1994a, 2). A fifth principle, 'lifelong learning,' was added later. IHAC defined fifteen policy issues, ranging from competition and job creation to Canadian content and culture; human and social impacts (including access, illegal and offensive content, privacy, security, and employment and workplace issues); IT learning and training (IC, 1994c); research and development; and applications and market development. At times, IHAC policy captured a communicative vision of the I-way: '[It is] not so much about information as it is about *communication in both its narrowest and broadest senses* ... not a cold and barren highway with exits and entrances that carry traffic, but a series of culturally rich and dynamic intersecting communities, large and small, north and south, east and west, populated by creative thinking people who reach out and enrich one another ... *a personalized village square* where people eliminate the barriers of time and distance, and interact in a kaleidoscope of different ways' (IC, 1994a, 3; emphasis added). The metaphor did not ignore the role of individuals and communities, but it does so with an economic hitch.

IHAC Policy Phase I: 1993–95

In September 1995 IHAC released *Connection, Community, Content: The Challenge of the Information Highway* (IC, 1995b). Success on the I-way depends on establishing a competitive framework that will unleash 'creativity, innovation and growth,' exploiting the economic and cultural potential of IT, and preserving values as a society (IC, 1995b). Because it is impossible to do justice to the issues and the over 300 policy recommendations made during the first-phase deliberations, we will make a judicious selection, prioritizing the human and social dimensions of policy. Under the policy rubric of 'competitiveness and

job creation,' the goal is to set a regulatory and policy framework that encourages investment, competition, growth, and jobs and where the marketplace determines 'winners' and 'losers.' Because financing is mainly a private sector responsibility, individuals and firms who provide venture capital and take on the financial risks should reap the market's rewards. Foreign investment policies should be reviewed to keep pace with the decline of national ownership of globally dispersed operations. Outdated and unnecessary regulatory barriers should be removed.

In May 1995 the Canadian Radio-television and Telecommunications Commission issued its so-called Convergence Report, *Competition and Culture on Canada's Information Highway* (CRTC, 1995). IHAC shared the CRTC's view that competition in facilities and services is crucial to the creation of wealth and ideas, but it added a sense of urgency about moving ahead with competition. The CRTC acknowledged that market forces alone would not guarantee Canadian voices and ideas on the I-way, extend economic benefits to all regions of the country, or satisfy all public interest demands. The CRTC's key policy shift (Telecom Decision CRTC 94-19) promoted competition between cable and telephone companies, reciprocal access and interoperability in all telecommunications markets in Canada, and support for distribution technologies providing video-dial-tone 'switched' communications and direct-to-home (DTH) satellite service. The Telecom Decision used the metaphor of a 'public lane' to capture the concept of affordable public access to government and health care information, library and database information, community networks, and e-mail facilities and services designed for use by both Aboriginals and persons with disabilities. Direct and indirect subsidies and cooperation are required to realize universal and affordable service on the public lane. Canadians ought to become creators of content and tools that reflect society's linguistic duality, because our small domestic market and proximity to the United States could erode identity and sovereignty. The terms 'competition' and 'culture' used in the report's title illustrate well the tension that exists between business- and consumer-oriented interests and culturally sensitive, public-interest-based concerns.

The Human Dimension: Access and Social Impacts

Access is a critical dimension of the policy debate, involving both physical access (carriage) and access to content and services. Without

physical access, access to content is irrelevant, but without content there is little point to physical access. In January 1995 Industry Canada published *Access, Affordability and Universal Service on the Canadian Information Highway* (IC, 1995a). The national access strategy was based on four policy principles of (1) universal, affordable and equitable access, (2) consumer choice and diversity of information, (3) competence and citizens' participation, and (4) open and interactive networks.

IHAC's working group on 'Access and Social Impacts' received input from various groups, such as the Coalition for Public Information (CPI) and the Canadian Library Association (CLA). CPI was formed in 1993 to ensure that the I-way would serve the public interest. CPI endorsed, among other goals, allocation of public and private resources for infrastructure development; access to broadband and switched services; non-profit participation in governance; use of non-proprietary standards; flat-rate billing; and ease of use, on the grounds that Canadians have 'the right to fully participate' in Canadian society and democracy and therefore have 'the right of universal access' and participation (CPI, 1994). The CLA held similar positions, couching policy proposals exclusively in the language of rights to literacy: universal, equitable, and affordable access; the right to communicate; the right to public space on the telecommunications networks; and the right to privacy. Access – whether as a condition of possibility for the promotion and protection of human dignity and rights (Walters, 1997a) or the maintenance of democratic values and 'social citizenship' (Shade, 1998a,b; Clement and Shade, 1996) – was a key concern.[3]

IHAC makes recommendations concerning hate propaganda, obscenity, child pornography, harassment, defamation and libel, offensive content, and privacy and security. It advocates 'fine tuning' of bilateral and multilateral arrangements at the level of international law. The public has a role to play by using adaptive filter technology, and information providers are encouraged to develop and adopt voluntary codes that reflect community standards and guidelines for complaint handling and conflict resolution. A balance must be struck between ensuring individual freedom of expression and imposing state controls to deter harm, particularly to children. On privacy and security, IHAC warned against the development of comprehensive profiles of individuals or companies or what Clarke (1988) calls 'dataveillance,' referring to the collection and selling of information across borders without the expressed consent of the individuals or groups

from whom it is collected. National legislation is needed to establish fair information practices for the private sector and the use of public key encryption and smart cards to allow personal control of information. Access control, information integrity, authentication, and non-repudiation are to be managed through the Government of Canada Public Key Infrastructure, but *'individuals* must remain at the forefront of the information revolution. Their *interests and rights, especially in matters of security and privacy, must be protected'* (IC, 1995b, 86; emphasis added).

Economic Roadkill on the Information Highway?

Two divergent approaches emerged with respect to the role and responsibility of the government and private sectors regarding employment and work issues, revealing a classic clash between full employment as a central policy goal of the state versus a laissez-faire market-driven approach (IC, 1995b, esp. 215–27). IHAC maintained that the state ought to be a 'facilitator' rather than a central actor in the informational economy. The minority report prepared by the Canadian Labour Congress vice-president, Jean-Claude Parrot, rejected the IHAC assumptions that the private sector should build and operate the I-way or that competition should be its driving force. Free trade, deregulation, privatization, and cuts to social programs and public services are symptoms of the subordination of governments to markets. Full employment ought to be the central policy goal, along with government and employer-sponsored training programs, work sharing, phased-in retirement, and facilitation of worker mobility.

IHAC followed up with a National Forum on the Information Highway and Workplace Issues on 21–22 February 1997 (IC, 1997a). Forum delegates discussed the impact of the I-way on the workplace, new approaches to work, and worker protection. Business and labour contributed to a discussion on non-standard forms of work, that is, part-time work, contingent or contract work, 'telework,' hours of work and the distribution of work time, self-employment, polarization of income and opportunities, education, training, and skills development. Predictably, business and labour perspectives were still at odds.

According to the *business view,* either technological change can be exploited for its opportunities and adjusted to in order to mitigate costs, or technology can be resisted while policy tries to protect old paradigms. 'Non-standard' work is any type of work that deviates

from a full-time, permanent job with nine-to-five hours. This is an entirely negative definition at a time when new work standards are coming on line. Part-time work, contingent/contract work, and telework are not necessarily bad. Alternative work arrangements may help workers to retrain, may provide opportunities for gaining new work experience, or may give individuals the ability to choose the most optimal place and time to work. There is no increasing polarization of incomes or shrinking of the middle class, and IT 'enables' individuals by increasing their skills and earnings. The appropriate response to our historical situation, therefore, is to increase access to training in order to close the gap between information haves and have nots, rather than creating state-managed work programs.

The *labour view* presents a view of technology that assumes a weak link between economic growth and job creation. In policy debates over whether to prioritize job creation or job security, job creation invariably wins out. High unemployment and fierce global competition are radically different from the technological changes experienced from the 1950s to the 1970s. New technologies are not limited to one industry or form of commerce, but affect all labour-related activities and the demand for and supply of labour. The excesses of market forces need to be constrained in order to deal with the negative short-term impact of technological change by means of collective bargaining and legislative reform. Legislated minimum standards are necessary to check the downward pressure of market forces that seek merely to improve the 'bottom line.' Part-time work is a reality that is inherently neither superior nor inferior. The problem is that there are a significant number of individuals who are involuntarily underemployed for whom part-time work is not a 'lifestyle.' They fear that they will not be able to put bread on the table and meet family needs. In addition, part-time workers do not have access to equal pay and employment benefits, such as health care and pension plans, and they often work extremely variable hours.

Learning and Training, Research and Development

IHAC policy maintains that individuals will no longer have a single career, but should expect to have three, four, or even five different careers. The Internet is the enabling vehicle that moves individuals from career to career, from learning institution to learning institution. 'In the next decade, 50% of new jobs will require at least 16 years of education' (IC, 1995b, 58). The working group on Research and Development –

composed of public and private sector communications and IT organizations, industrialists, and educators – addressed standards and applications, science and technology priorities, applications in building a health information infrastructure, privacy and health information, education, electronic libraries, and electronic publishing of scholarly information. The tone of the group's position is foreboding: 'Canada faces both opportunity and threat in the evolving global Information Highway. Canadians must now build aggressively on their strengths in the pre-competitive and competitive carriage and content industries ... If we fail to move with alacrity, our global competitors will move in, taking away potential jobs from Canadians. The choice to seize promptly this opportunity is ours, and what we do now is critical to future generations' (IC, 1995b, 69). The key condition for R&D applications development is 'commercial success.' Tax incentives, not grants, ought to have a greater policy role, since tax breaks drive commerce.

Health Care and Education

Health care accounts for 30 per cent of provincial government expenditures. Cost reductions and shifts in basic health care attitudes are fuelling policy reforms. Geographic distribution of Canada's population will be a major determinant of health care quality in the future. In 1995, 25 per cent of Canadians lived in rural communities of fewer than 10,000 people, but 'only 20% of family physicians and 4% of specialists practice in rural communities. Approximately 5% of Canadians live more than 25 kilometres away from the nearest hospital and 2% live more than 25 kilometres from the nearest physician' (IC, 1995b, 78). Canadian-trained physicians are heading to the United States to practise medicine. IHAC notes the urgent need for a 'balance' between the need to protect individual medical privacy, on the one hand, and the need for epidemiological research to enhance and benefit public health, on the other hand. There is no discussion, however, of where and how to draw the line between individual rights and a health care 'common good.'

Despite massive investments in education and training, 'serious problems' plague the education system. We need to save money, while we improve learning in primary, secondary, and post-secondary institutions. The government ought to provide incentives for scholarly electronic publishing, and research granting bodies should adopt policies to encourage electronic dissemination of research.

IHAC Policy Phase II: 1996–98

The Phase II policy mandate began in June 1996. Its aims were to advance previous policy and to report on Canada's actual progress in the transition to a knowledge-based society (IC, 1997b). The creation, manipulation, and sharing of information and knowledge is the essential 'human imperative':

> No longer will distance pose an obstacle to economic development, social intercourse, learning, voluntary action, adequate health care, business success or full participation in society and Canada's national cultural dialogue. Knowledge will become increasingly available to everyone, allowing us all to make wiser decisions in all aspects of our lives – from business to government to health care to education to work to our everyday existence. Everyone will be not only a consumer of knowledge and content, but also a creator. Canada's national cultural dialogue and political discussion will take on a liveliness and depth that will strengthen national, regional and local communities. (IC, 1997b, 2)

We must set aside now an analysis of the suppositions in these promises. Suffice it to say that policy makers recognize a 'seamless interdependence' between the economic, social, and cultural dimensions of the I-way that did not exist in earlier policy formulations. If Phase I policy focused on access and *physical infrastructure*,[4] Phase II emphasizes IT *use* to meet individual and collective goals. This shifting emphasis at least partially reflects IHAC's response to critics of its earlier technological imperative: 'We have always recognized that technology is not an end in itself, but only a means to realize traditional Canadian goals and values' (IC, 1997b, 7). Phase II is far more circumspect about the negative impact of IT on unemployment and makes explicit reference to the human rights challenges of information policy.

'Technology-Neutrality,' Privacy, and Security

Networks, telecommunications, broadcasting, and computer communications had become increasingly integrated by 1996. Telephone companies entered the broadcast distribution market in January 1998 as a result of IHAC's earlier recommendation that the government pursue the principle of 'technology-neutrality' – that is, market forces should

determine the technology that is appropriate for the provision of particular services, while government and the CRTC should provide frameworks for fair and sustainable competition. At the time of Phase II policy formulation, Canada had a higher cable penetration than the United States, Japan, Sweden, and the United Kingdom, and cable TV was available to 95 per cent of Canadian homes (but the subscriber rate actually was 78 per cent). At 98.7 per cent, we had more telephone access than any other G7 nation,[5] a remarkable figure considering that more than half of the world population has never made a telephone call (Poirier, 1997/8). On the negative side of the IT ledger, Canadian expenditure on R&D represented a smaller portion of GDP than many other industrialized countries, and per capita IT capital investment ranked in the middle of the G7 nations. Through Industry Canada support for private sector investment in R&D and private and public sector collaboration in CANARIE (the Canadian Network for the Advancement of Research, Industry and Education), the world's first national optical Internet – CA*net 3 – became active in October 1998. With its capacity to carry multi-media traffic using wave-division mutiplexing technology, CA*net 3 enabled health, education, research, and commercial applications that were technologically impossible on the earlier voice-communication-only CA*net 2 system.

Ethical and legal concerns about privacy, security, and the amount of illegal, offensive, and inappropriate content carried on the Internet continued to be a dominant issue (IC, 1997b). Industry Canada had earlier warned against the development of comprehensive profiles of individuals or companies that can be sold or integrated across borders without the express consent of the individuals or groups from whom it is collected (IC, 1994a,b, 1995b). In Phase II a decidedly *economic* approach to privacy was taken (IC, 1998b). Invoking the CSA code, Industry Canada and the Justice Department sought a new law that would strike 'the right balance between the business need to gather, store, and use personal information and the consumer need to be informed about how that information will be used ... and protected' (IC, 1998b, 25). New legislation needed to address how responsibility for private sector protection was to be shared among the provincial, territorial, and federal governments.

Research Partnerships

The federal government's March 1996 Science and Technology Strategy advocated that government labs should work in close partnership with

industry. The goal was to form R&D consortia at pre-competitive stages of research, such as the National Research Council's formation of the Solid-State Optoelectronics Consortium, whose partners include the Communications Research Centre (CRC), Nortel, TRLabs, and other organizations, resulting in the deployment of photonics technologies in experimental broadband network applications. Phase II policy reiterates the importance of research partnerships at a time when the Internet had become the key 'enabling technology' and modus vivendi of access: 'Many regard today's Internet as a model for the Information Highway of the future and as a realization of the vision of the Information Highway articulated by the Advisory Council in its earlier work' (IC, 1997b, 23).

The information highway had become the Internet by 1997. There were legitimate empirical reasons for equating the two. Since Phase I, at-home use of the Internet had more than doubled to 13.3 million households, with even more users at work or in educational institutions. Internet penetration was high, but still not as high as it was in Finland, whose rate was double that of the United States. Canada had some of the lowest Internet costs because of monthly telephone service rates and attractive service provider costs. Development and maintenance of infrastructure trunk lines and bandwidth remained a challenge, but policy concerns were shifting to global agreements on standards. There was no public discussion of the challenges that open TCP/IP protocols (Transmission Control Protocol / Internet Protocol) pose for the law enforcement and security establishment. Instead, the emphasis was on national and global networks and industry's role in bolstering trust in e-commerce.

IHAC Policy Phase III: The Canadian Electronic Commerce Strategy

Information policy entered a new phase on 22 September 1998, when the prime minister announced Canada's Electronic Commerce Strategy (CECS), with the goal of making Canada a world leader in the development and use of e-commerce.[6] E-commerce includes 'any kind of transaction that is made using digital technology, including open networks (the Internet), closed networks such as electronic data interchange (EDI), and debit and credit cards' (CECS, 1998,1). The strategy entails four action priorities: (1) building trust via security/encryption, protection of personal information, and consumer protection; (2) clarifying marketplace rules surrounding the legal and commercial frame-

works, financial issues and taxation, and intellectual property protection; (3) strengthening the information infrastructure by increasing network access and support for open networking standards; and (4) realizing opportunities through the development of digital skills and awareness, with governments acting as model users. Our exposition will briefly highlight elements of the strategy, noting continuities and discontinuities from the earlier two phases.

The Phase I and II debate about the impact of IT on work and employment now gives way to support for e-commerce as the primary business platform that cuts across business-to-business, business-to-consumer, and government use. Building business and consumer *trust* is the key priority. E-transactions must be secure and private, supported by complete and accurate information, with redress available. It is the responsibility of the private sector to build trust now that industrialist measures, such as storing data in paper-based files or internal computers, are inadequate for informationalism's main mode of development and domains. *Intranets* distribute information and speed data between offices and behind company firewalls, often spanning multiple locations via the Internet. When businesses make their intranet available to business partners, such as suppliers, distributors, and other authorized users, an intranet becomes an *extranet.* Business-to-business applications drive growth, accounting for about 80 per cent of all Internet e-commerce. Consumer use of the Internet is still in its infancy, with only 16 per cent of users in Canada and the United States making purchases in 1997 (Margherio et al., 1998). On-line consumers will grow to 100 million (adults, United States only) by 2001, with global e-commerce growing from c. 22–33.5 million in 1998 to c. 350–435 billion by 2002 (CECS, 1998).

Security issues during industrialism were related to law enforcement, but in the informational mode of development they are primarily related to protecting on-line transactions. Both the need for a common verification framework for the identity of parties and global jurisdictional issues remain unsettled. The strategy seeks secure e-transactions through the use of cryptographic technologies (CTs) and 'certification authorities' (CAs), which bind parties to their respective digital signatures and provide identity authentication. CTs also provide for the integrity and confidentiality of communications, ensuring that neither party can deny participation (so-called non-repudiation). Cryptography is beneficial for e-commerce, privacy protection, and crime prevention, but CTs are being used to hide criminal activity and

to threaten public safety and national security. Investigations, prosecutions, and the enforcement of laws and regulations could be hampered without lawful access to evidence pertaining to illegal activity. Canada has not restricted individuals or businesses from importing or using strong cryptography, and end-users have been free to determine what kinds of authentication and encryption products and services they need. Canada, along with thirty-two nations that are signatories of the Wassenaar Arrangement, does control the export of cryptography.[7] Government policy will not implement licensing regimes for CAs or trusted third parties, but calls instead for industry-led accreditation of CAs as a means of promoting sound business practices and building consumer trust.

Without clear 'marketplace rules,' the growth of e-commerce will stall. The legal and commercial frameworks that currently exist are uncertain, such as evidence rules and over 300 federal statutes that require documents to be 'in writing' or equivalent words. Both the trustworthiness of electronic signatures and uncertainty concerning the liability of Internet Service Providers (ISPs) and other Internet intermediaries, may impede e-commerce. Far-reaching issues about taxation, tariffs, and financial services and markets can be adequately dealt with only internationally. Like the principle of 'technology neutrality,' the strategy supports 'tax neutrality': 'Taxpayers should not be subject to different taxes simply because they provide services either on or off the Internet' (CECS, 1998, 29). The protection of intellectual property (IP) in music, computer programs, video, multimedia works, and databases must be 'balanced' with the needs of users. Canada signed two new World Intellectual Property Organization (WIPO)[8] treaties in 1997, which give right holders – including authors, performers and record producers – exclusive right to make their works, performances, and recordings available through interactive media. IP trademark rights and duties and domain names continue to pose structural problems, because the Internet is international, while trademarks law is national. Generic top-level domain names (e.g., .com, .org, and .net) have been determined by a U.S. private company under government contract, and top-level country codes (e.g., .ca, .uk) are under domestic jurisdiction (Manishin, 1998).

Telecom investment and the CA*net 3 have led Canada to a leading-edge infrastructure, yet 'most Canadians do not yet have a computer at home' (CECS, 1998, 33). Access policy ought to be focussed on community access sites through schools and public libraries. For e-commerce

to be globally adopted, the interoperability of networks and universal communication require internationally agreed-upon codes, user interfaces (e.g., icons, dialogue design principles), basic functions (e.g., trading protocols, payment methods, security mechanisms, identification and authentication, and auditing and record keeping), and agreed-upon definition and encoding of data and other objects (e.g., IT enablement of existing standards, message semantics).

E-commerce dominates our historical situation and is the almost exclusive means of the informational economy. The government's e-commerce strategists assume that IT is making a 'significant contribution' to strengthening the social infrastructure through improvements in education and health care, but admit that IT effects on the distribution of income and opportunities are debatable. The emergence of information haves and have-nots must be a pressing policy concern to governments seeking to broaden access to opportunities through the development of digital 'skills and awareness.' Acting as a model user, the government can build trust and demonstrate the advantages and disadvantages of e-commerce, thereby diffusing opportunity to all Canadians.

Methodological and Ethical Analysis

Developments during the three policy phases surveyed above betray the public policy product cycle and corroborate the impact of capitalist restructuring on cultures, institutions, and organizations. All three policy phases reflect the spirit of the informational economy. Three fundamental national (and global) policy issues surface time and again: (1) the impact of IT on work and employment, (2) privacy, and (3) security and encryption or 'information warfare' policies, all of which provide the rationale for the structural contents and concerns of subsequent chapters. Before turning to an analysis of the question concerning the impact of IT on work, we bring our philosophical framework to bear on some of the other ethical issues raised by the foregoing exposition of Canadian information highway policy.

First, with respect to the public policy cycle, Gilder's optimistic bias concerning the power of people over big brotherism needs an empirical reality test. Orwell's famous metaphor is still necessary, but insufficient, since invasions of privacy are often carried out by private sector 'little brothers' rather than the traditional model of the totalitarian state or government surveillance industry. Utopian visions have given way

to privacy concerns over the subject's 'digital persona' as an aspect of identity projected in cyberspace (Clarke, 1994). Michael Vlahos rightly asks how we are to emerge from our techno-historical situation and feel a larger sense of community and identity, but he offers no vision of community in the transformation of global identities. He appears to believe we are only a few years away from a digital *civitas eterna*, with the Infosphere as soteriological goal, a digital reign of God. A digital Tower of Babel may provide the needed cognitive correction to his vision of Infosphere as communicative totality. For the affluent, mobile, and educated, the future on the Infosphere may look bright, but for the unskilled, the underclass, and those already living on the margins, it looks like an informational avatar of the Dark Ages. Utopian visions often labour under the reductionist dominance of what Jaspers calls 'Spirit,' seeing technological and cultural phenomena in terms of unities or parts of a meaningful whole. Infosphere is not a Hegelian embodiment of 'Absolute Spirit,' but only one important technological aspect of a global network society.

Second, IHAC's endorsement of *public access* to community computers in libraries, government offices, and schools is an ethical good. SchoolNet, the Community Access Project, and Computers for Schools all represent efforts by the government in cooperation with community interest groups and the private sector to ensure that the business and social benefits of the I-way will be available to all Canadians (Williamson, 1995). Such policies fulfil norms of mutuality and social soldidarity and potentially aid productive agency and a more vibrant community and state. It is debatable, however, whether or not access points installed and sustained by government provide *sufficient access* for citizens, and whether or not they will be financially sustainable in the long term. Public libraries have been confronted with static or declining budgets, while public use of them is on the increase. The idea that computing cheapness and the plummeting price of hardware will make costs decline towards near-zero with a fully accessible and democratic cyber culture achievable in the not-too-distant future is probably more utopian than real. The global Internet culture does not function within a context of pseudo-classlessness; the locus of class and power relations may have slipped into a more diffuse, individuated mode, but it is by no means class neutral (Lockard, 1997). If Bell Canada were to change its local carriage rates from a flat rate to a time-based rate, for example, the impact on access for persons with disabilities would be devastating. Assistance device technologies for the hear-

ing and vision impaired are miraculous technologies, but without adequate connection and just pricing structures such persons will be additionally disadvantaged. Increasing numbers of persons with disabilities find themselves without work in the informational economy.

Public interest groups have advocated 'local, electronic public space' as a shared learning environment in response to the exclusive, market-based vision of I-way policy.[9] Their role is to ensure open access to a not-for-profit public space that facilitates self-expression, education, learning, and social and cultural participation. The importance of shared electronic public space derives not from the technology, but from the ability of community members to interact and participate in the production of public information content, from access to the exchange and use of information, from broad-based education and learning, and from literacy and skills training (SCEPSP, 1997). The term 'local' is rather flexible and may mean a single community; a number of communities; locations across several hundreds of kilometres, such as rural and remote situations, and even a 'province-wide system,' like an Atlantic province. Community networks serve social functions that are not in competition with commercial Internet service providers (ISPs), achieving an equitable balance among economic and democratic concerns. Such community networks instantiate a 'community of rights' in an informational environment and accord with the principle of human rights.

A sceptic might argue that individuals do not have positive rights to public access community networks. If individuals can help themselves, then there is no obligation on the part of others to pay for their participation. How are such public space networks to be implemented and maintained? Who will pay for their effectuation? Who will be the *respondents* of rights to public space community networks?[10]

These are exceedingly important questions. It is hard to imagine the viability of public space community networks without a significant commitment on the part of the state to ensure funding and ongoing operations. The state, as a community of rights, must be the effectuating agency of access rights, and the state in question must also be democratic. Moreover, individuals do have an incentive to acquire a level of productive agency that actually enables them to act more successfully in pursuit of their purposes. If persons cannot afford access, the ability to maintain purpose-fulfilment and capacities for action (i.e., non-substractive well-being) are severely hindered. At ethical issue in community networks is a vision of *mutuality* that is sensitive to indi-

viduals who cannot secure access to the exchange and use of information, to general education and learning, and to literacy and skills training by their own means. Participation and interaction in community networks represent an ideal that is not dependent solely on market forces, and thereby mirrors the idea of a community of rights as a solidaristic system dedicated to working for the equal economic and social rights of all individuals living within a given community, whether local or national.

Again, however, the sceptic might ask: Is the virtual community envisioned by public networks a real community, or is a 'virtual community' really an oxymoron? In this view, forms of 'real life' community are under attack by the very techno-cultural forces that have made Internet culture possible. We should be highly suspicious of terms like virtual community, because real community entails physically committed, embodied relations of commonality between individuals and objects. Virtual communities, however, are no less real because they are mediated through cyberspace. 'Virtual communities are social aggregations that emerge from the Net when enough people carry on those public discussions long enough, with sufficient human feeling, to form webs of personal relations in cyberspace' (Rheingold, 1993, 5). We believe that the community of rights will not remain completely virtual, because human rights and responsibilities must be recognized and enforced in theory and practice. The state remains a concrete manifestation of political and economic democracy, and an informational community of rights still requires moving between digital and face-to-face interactions. The best virtual community is an extension of the community of rights in which communication is not asynchronous, as is the case on an electronic mailing list. What is most important, however, is the holding-in-common of qualities, properties, identities, or ideas grounded in social solidarity and mutuality, manifest in both the virtual and non-virtual realm. Let us recall that the etymological root of the word *virtual* is 'virtue,' thus bringing together notions of power and ethics. The deepest roots of virtuality reach back into a philosophical and religious world view where power and moral goodness are united in virtue. The characteristic of the virtual is that it is able to produce effects, or to produce itself as an effect, even in the absence of the 'real effect.' The connotation of the word *virtue* in ordinary usage obscures the distinction between real effects of power and/or goodness and effects that are as good as real (Wilbur, 1997). The informational community of rights would restore these concurrent meanings.

Third, throughout the main information highway policy phases, the Internet has been largely a libertarian milieu, where participants prefer self-regulation and self-help to government intervention. Canadians appear to be increasingly weary of near-absolute appeals to individual freedom over and against the state, as epitomized, for example, by John Perry Barlow's 'Declaration of the Independence of Cyberspace' (1996). Barlow dismisses the role of government and other mediating institutions in shaping information technologies. The earlier 'Bill of Rights and Responsibilities for the Electronic Community of Learners' (cited in Walters, 1995a, 415–18) is a more balanced approach than Barlow's, our/your, dichotomizing harangue against government, because the bill maintains a correlative view of the rights and responsibilities of individuals and institutions within the electronic community and in relation to the larger educational community and society.

Despite the 26 June 1997 U.S. Supreme Court decision in *Reno v. American Civil Liberties Union et al.* – which struck down the 1996 Communications Decency Act's regulation of sexual material online – the Internet is not a 'regulation-free zone.' Obscene material, as defined by U.S. Supreme Court jurisprudence, is still prohibited, as is child pornography. While there have been no attempts to criminalize on-line communications in Canada, constitutional law scholars have argued that it is illegal to spread hate propaganda, child pornography, and obscene material on the Internet (Mendes, 1997a; Sopinka, 1994, 1997). The situation is constantly changing. In January 1999 Justice Duncan Shaw of the British Columbia Supreme Court struck down section 163.1(4) of the Criminal Code, which makes it illegal to possess child pornography. The judge ruled that the law is a 'profound invasion' of freedom of expression and right to privacy guaranteed by the Charter of Rights and Freedoms. The ruling led, in turn, to the dismissal of child-pornography possession charges against another individual. The case triggered a groundswell of fury from lawyers, politicians, and citizens, and the Canadian Judicial Council received at least fifty complaints. Over half of the government's backbench MPs urged Prime Minister Jean Chrétien to take immediate legal or parliamentary action to override the ruling. The debate over whether or not the court's decision creates a 'free market for the work of pedophiles' will be debated well into the future (Naumetz, 1999). The fundamental issue concerns individual rights claims and some conception of communal interests and the public good. U.S. and Canadian Supreme Courts have applied 'an ethic of the law and justice of proportionality' to on-line communications. Mendes

notes that both ethics and the law must 'balance' the goods and evils of free expression on the Internet with societal interests in such a way that the interests of neither the individual nor society are overwhelmed or sacrificed at the expense of those of the other (Mendes, 1997a).

Are ISPs liable for defamatory, obscene, or hate literature posted on their bulletin boards? This policy question has not been directly addressed in Canada, but in the two well-known American court cases – *Cubby v. CompuServe* and *Stratton Oakmont Inc. v. Prodigy Services Co.* – the court ruled in two different ways. CompuServe got off the legal hook because the court ruled that it was a 'distributor,' like news vendors, bookstores, and libraries. CompuServe was not liable, because the company did not know about the defamatory material. In contrast, the court ruled against Prodigy on the grounds that it acted like a 'publisher.' Prodigy publicized itself as controlling content, and it used a software screening program to monitor content. The irony of these rulings is obvious: if ISPs intend in good faith scrupulously to regulate content – a Herculean task even for the best screening technologies – they may be held legally liable as a publisher. If they do absolutely nothing and are merely passive 'distributors,' they may avoid legal liability for defamatory material but at the same time run a moral risk to their corporate image and social responsibility. U.S. case law appears to represent a case of legally damned if you do, and morally damned if you do not. Under Canadian law, it appears that an ISP cannot escape liability by the simple expedient of being classified as a library, bookstore, or news vendor. Depending on the case, 'the courts may be willing to impose some sort of screening responsibility as an element of the [ISPs'] "proper operation of the business"' (Sopinka, 1997, A19).[11]

Fourth, we have seen that the principle of 'lifelong learning' is central to I-way policy. Does the principle serve, perhaps unwittingly, the interests of corporate downsizing or educational commercialization? Aristotle (1924, I, 2: 982b, 11–21; 983a, 12–20) made *thauma*, or 'wonder,' the source of all thinking and education, and the ethical mean avoids either excess or deficiency in cognition or emotion. If lifelong learning is defined strictly in terms of technological instrumentality, we miss the ethical mark with harmful effects on human dignity, rights and responsibilities, and culture. If public education becomes a pay-as-you-go smorgasbord, and a technocratic-competitive vision of education emphasizes economic goals (Taylor, 1997) with little regard for their costs and consequences to the individual, society, and the environment, we will lose the ethical mean.

Fifth, research partnerships between the private and public sectors and between industry and universities may represent an ethical good by serving social and economic values. How far should such partnerships go? We know that scientific data may be potentially skewed when driven by deep economic pockets and corporate power. The question turns on the nature of research, the idea of the university as a place and space dedicated to the quest for truth (Walters, 1996), and clarification of the *internal goods* and *external goods* of research practice.[12] The ethics of scientific research has received a new lease on life in the light of conflict of interest cases, problems with double-dipping, and abuses in public sector procurement processes. It is not moralistic to sound a warning against ideological uses of science and technology that merely mask personal or private sector economic interests. Whistle-blowers have had their lives threatened, have been ostracized from high paying positions, and have even been demoted to running company car pools for speaking out against such abuses. Scientific knowledge itself is a type of technology – a knowledge technology – that ought to serve human goals and values. Only an existential will to truth can check the abuse of scientific research that masks disvalue for value in the name of law and order, national security, or the common good, and self-deception is a real and ongoing possibility.

Sixth, information policy promotes the advantages of telework for workers, business, and society. We must distinguish, however, between telecommuting and telework. *Telecommuting* is a phenomenon that involves skilled professional workers and often does entail less travel, less stress, and more access to the labour market for individuals with disabilities and women with children. *Telework*, by contrast, tends to be low-status, low-paid work, with few of the protections enjoyed by on-the-job workers, including proper equipment, regular breaks, health and safety protection, and visibility. In most business discussions telework is erroneously presented as if it were telecommuting work (Wheelwright, 1997). We should not assume that everyone will be doing telecommuting or telework in the future or that either type of work will necessarily be beneficial. Empirical evidence suggests that the ways in which work is decentralized vary enormously from country to country and region to region and depend upon the prevailing organizational culture, government regulation of the labour market, population density, family structure, income levels, and the availability of IT infrastructure (Huws, 1999).[13]

Finally, despite the policy struggles between business and labour,

there does exist common ground with respect to roles for education, training, and skills development. The great challenge for both business and labour is to turn the debate into a communicative, loving struggle. Amid concerns with the material basis of existence, the economy should serve human beings, not vice versa. This fact begs the question of how best to serve human dignity through IT development and whether IT is, in fact, a jobs killer. The question turns back on empirical data and ethical analysis of the informational economy which we will now examine.

CHAPTER THREE

The Informational Economy, Work, and Productive Agency

We virtual workers are everyone's future. We wander from job to job, and now it's hard for anyone to stay put anymore. Our job commitments are contractual, contingent, impermanent, and this model of insecure life is spreading outward from us ... We live in a contest of the fittest, where the most knowledgeable and the most skillful win and the rest are discarded; and this is the working life that waits for everybody. Everyone agrees: be a knowledge worker or be left behind. Technical people, consultants, contract programmers: we are going first. We fly down and down, closer and closer to the virtualized life, and where we go the world is following.

(Ullman, 1997, 146)

Is this the world of virtual work that information highway planners would have us enter? Has the global informational economy and new division of labour left us unconcerned with individual victims of mass unemployment resulting from technological displacement, negative trade impacts, fiscal, monetary, and other economic policies? Or is the issue of technology displacement and unemployment moot in the absence of fully acceptable global and national economic data or massive civil unrest? How ought we ethically to assess the policy debate that characterizes all three phases of information policy concerning the impacts of the informational economy on work and human development?

In response to these questions, we begin this chapter with an analytical discussion of productive agency, work, human capital, and property rights. Next, we define the informational economy and identify globalization's challenge to social and economic rights, the failure of

human development strategies, and the problem of pervasive poverty. While there is a role for information and communications technologies (ICTs) in sustainable development, the research that maps and measures the benefits of ICTs for human development is ambiguous. We then turn to the question of whether or not IT is a 'jobs killer' in the North American situation. We argue that there are empirical and ethical problems with the so-called end-of-work thesis. The empirical problems are related to unemployment data and differing interpretations of the so-called productivity paradox. The ethical problems are related to the meaning of productive agency, work, the earning of income leading to property rights, and the importance of promoting and protecting economic rights to development and employment in the neo-liberal marketplace.

Productive Agency, Work, and Human Capital

Productive agency is the agent's ability to achieve the outcome he desires or intends, and a productive agent is one who thus achieves. Productiveness is synonymous with additiveness and well-being. By additive well-being, individuals increase their capacity for purposive action and general purpose-fulfilment. To be a productive agent is to develop and maintain additive well-being in one's actions, or to achieve one's purposes, and productive agency is the continuing proximate capacity or disposition for actually being a productive agent. For most of us, such development requires, as a necessary if not sufficient condition, that we have the ability to acquire income or wealth sufficient for protecting freedom and well-being. In an economic sense, then, productive agency consists in the capacity for economic acquisition.

Work is 'the expenditure of effort for some end or purpose preconceived and aimed at by the worker' (Gewirth, 1996, 134). The concept of productive agency has three components that serve to define a general concept of work or labour. First, not only is what is produced by work one's own purpose-fulfilment, but it must be embodied in products, services, or objects external to the agent in a form that is recognized by others. Second, the products of work must be valued by others; that is, they must be 'use-values' for other individuals. Third, the use-values of work must also be 'exchange-values,' that is, effectively demanded by others who are willing to pay for them. By working to produce exchange-values, productive agents obtain income that allows them to be productive agents in the more general sense of

achieving outcomes that they intend or desire, including various additiveness. Additive well-being presupposes basic well-being, and income serves the material bases and purposes of existence of having food, clothing, shelter, and fulfilling other basic needs. This relation of work to the earning of income makes employment so important, whether one is self-employed or employed by others. Moreover, the importance of exchange-values reminds us of the social context of work. If there is no demand for an individual's products, then the work one does is ineffective from the perspective of economic productive agency. This fact limits what can be accomplished by the right to productive agency, including the extent to which what one earns by one's work can be attributed solely to oneself, and has direct bearing on the right to employment and full employment policy.

There is a close connection between agency and work. Unlike action in a strict sense, a worker may not have control over his or her behaviour and may be forced to do work. Moreover, action per se may not result in an external product as such, as is the case when an individual 'works out' in a gym in order to stay healthy. Individuals who have productive agency as an enduring disposition or capacity usually have corresponding traits of character, such as courage (including fortitude, perseverance, and personal responsibility), temperance (controlling appetites and inclinations judiciously), prudence (calculating efficient means to achieving ends, and in choosing ends most worthy of pursuit in the light of their overall capacities and deepest aspirations), and justice (where the productive agent acts in accordance with the generic rights of his recipients as well as those of him/herself). Individuals have positive rights to the development of their productive agency when they cannot do so by their own efforts (e.g., persons with disabilities), as do workers whose skills are needed to protect other persons' basic and additive rights to health, food, shelter, and other goods. Positive rights belong to workers not only for their own sake, but also because they are mutually instrumental to promoting and protecting other persons within the community of rights. The positive rights provided by welfare states help persons to develop their 'human capital,' which, in turn, helps to promote greater autonomy and reduce economic inequality within society.

Human capital is a form of productive agency. Human capital entails various skills and abilities that have economic value because they may be used in income-yielding activities. These skills and abilities are, in a real sense, a means of production. They are 'produced' insofar as they

have resulted from an individual's investment in education, health, and other conditions of successful agency. In this way, human capital is identical with productive agency. What distinguishes this definition of human capital from traditional economic definitions is that its distinctive features derive from their ground in the principle of human rights. Human capital is in the possession of the individual agent, is oriented towards his or her benefit, and involves the idea of self-improvement, development of personal virtues, and a sense of personal responsibility. Through human capital development, the individual is enabled to contribute to fulfilling other persons' needs and wants, thereby maintaining mutuality and participating in the community of rights.

Developmental economists have generally criticized this view of human capital, presupposing a utilitarian interpretation of human capital in terms of economic growth rather than individual rights. However, when human beings are reduced to means of production or the material (Dasein) elements of the labour process purchased by the capitalist, as Marx understood (1978 [1859]), the individual becomes a mere *means* to economic growth. Labour becomes a part of capital, and the goal of human capital is to serve 'efficiency' for a maximum rate of return (as in the case of educational funding and publishing grants that are viewed only for their monetary output potential). This tends to denigrate forms of education that are considered 'soft' or merely cultural. In turn, existing social and economic inequalities are reinforced. Note, however, that this utilitarian view of human capital is aggregative, not distributive. In contrast, when human capital is seen in terms of individual rights, each person is the owner of his or her own capital that is not used for maximizing return or the expansion of capital. This agency-based view of human capital does not deny the role of monetary exchange values and their important relation to individual human capital. Nor does it deny that governments should be concerned to invest in human capital for the sake of economic growth. But the economy serves human beings, not vice versa. Economic growth is valuable because of the contribution it makes to the dignity and well-being of individuals, especially those who cannot maintain their basic well-being by their own efforts. In this way the state functions as a community of rights, because it helps persons to attain autonomy and the abilities of productive agency that they would otherwise be unable to attain. A key value of human capital is that it provides individuals with capabilities for self-help, including developing an effective sense of personal responsibility. To be sure, economic growth can also help to

move social structures in more egalitarian directions. Because 'struggle' is a 'limit situation' of the human condition, however, it will normally do so 'only if strenuous efforts are made by governments and organized groups, including especially the workers and those who suffer from economic deprivation' (Gewirth, 1996, 141).

We interpret human capital as promoting each individual's development of abilities and productive agency. From the ethical standpoint of the principle of human rights, the application of human abilities is rewarded in an economic sense: producers contribute to the fulfilment of other persons' needs and wants. So this view of productive agency also recognizes the economic import of earning an income by making an input and thereby benefiting others as well as oneself. The economic view of productive agency still raises a host of questions concerning what is produced, for whom, for what end, the relation between production and income, price, and so forth. These questions are normally discussed in terms of the distinction between 'productive' and 'unproductive' labour. Labour that is productive has implicitly been defined in terms of three normative assumptions concerning: '(a) What is genuinely valuable, at least within some given economic system; (b) what contributes to the making or providing of what is thus valuable; and (c) what alone is therefore deserving of income as reward' (Gewirth, 1996, 142). Conversely, to call something or someone 'unproductive' is disparaging. What ought to be emphasized about these three assumptions at the core of classical economics is that productive labour is very narrowly defined. Labour productivity consists in profits for capitalists, not in its broader effects or benefits for other persons. Similarly, its view of work is not on how work is experienced by the worker, but rather on its 'output' and relation to persons who presumably receive benefits from it. For Smith, Mill, and even Marx, what constitutes productive labour is added value for capitalists and material vendible objects, and the primary recipient of the product is the employer or capitalist entrepreneur. The importance of work to human dignity, social cohesion, community building, and broader mutuality is set aside.

Since all modes of the productive are kinds of action, the primary and inescapable context for differentiating 'productive' from 'unproductive' labour is the freedom and well-being that are the necessary goods of action and the objects of human rights. This view ties the distinction between the 'productive' and 'unproductive' to the principle of human rights and to the requirement of the equal and mutual pro-

tection of all persons' needs of agency. What is productive, at base, is that which contributes to the protection and development of the necessary goods of agency. The human well-being that is an object of productive labour includes basic, non-substractive, and additive well-being. Productive labour entails a wide range of work activities that correlate with goods such as food, clothing, and shelter production; goods that serve life, health, and safety; and goods that foster humanistic and scientific culture and opportunities for earning an income adequate for all three levels of well-being. The criterion of degrees of needfulness for action justifies certain monetary transactions but does not go so far as complete equality. Even utilitarians do not uphold complete economic equality based on the diminishing marginal utility of money through the need for work incentives. If wealth is equalized, then the incentive to work and work hard is removed. Therefore, economic redistribution must stop short of complete equality (Bentham, 1928). The principle of human rights acknowledges this incentive factor, but it emphasizes that the rational autonomy that is the aim of human rights requires that each person be a self-developing agent, in contrast to being a dependent, passive recipient of the agency of others. When positive economic rights are involved, the point is not to increase dependence, but rather to provide support that enables persons to control their own lives and effectively pursue and sustain their own purposes without being oppressed or subject to domination and harms from others. For this reason, the criterion of degrees of needfulness for action justifies only those monetary transfers that enable persons to acquire and exercise abilities of productive agency on their own behalf.

On the basis of the foregoing understanding of productive agency, the 'unproductive' emerges as that work or activity that does not contribute to the fulfilment of the three levels of agency needs. Indeed, much of the classical economic critique is that much of what is produced and paid for in the capitalist economy does not fulfil any real needs. Consumerism is artificially stimulated by advertisers, and global currency traders are not producing anything, but instead are manipulating markets in order to line their pockets without adding any real goods to the economy. Once the primary context of the necessary goods of action are fulfilled, however, we may then shift to a broader economic view of the productive as tied to desires and preferences whose satisfaction is demanded by a market economy. In this view, musical performers, artists, unpaid housewives or house-

husbands, and clergy make essential contributions to human productive agency. While single welfare mothers fall under the positive welfare right to basic well-being, productive agency recognizes a wide variety of cultural work that contributes to additive well-being. For this reason, productivity must not be reduced only to the outputs of technology, nor should educational productivity be reduced to training for IT skills.

In international policy debates, human development is normally defined as economic growth, increases in per capita income, and the attainment of an adequate standard of living along the lines of economic 'productive' labour. We must acknowledge the non-material aspirations of individuals in developing countries (Benzanson and Sagasti, 1995) and the essential, philosophical sense of productive agency. We stress human-agency-based development and work as one, among others, of the conditions for productive agency in the informational economy. This view of productive agency, work, human capital, and property rights also accords with the belief that the individual and the worker are more than existence (Dasein). Although dependent upon the material conditions of life, human rationality, love, and existential communication are higher ends of human agency served by economic agency.

Two Justifications of Private Property

A major purpose of productive agency is to enable individuals to earn income for themselves and their families. Work provides income, which is a species of private property, and insofar as there exists a right to productive agency, there is also a right to private property, as represented by an individual's earned income. While the right to private property is primarily a moral claim-right, it also entails legal powers to possess, use, transmit, exchange, or alienate objects. Property consists not only in objects and other things, but also in relations between persons and things whereby individuals have rights with correlative duties placed on others. Property rights are negative rights insofar as other persons have duties to refrain from interfering with the owner's possessing, using, and handling the things that are owned without the owner's consent. This applies to houses and money, as well as to information. As we shall see, positive property rights help to ground both the United Nations' human right to employment and the International Labour Organization's view of full employment as 'feasible and highly

desirable' in a situation where trade and investment flows are globally integrated.

This link between productive agency and property rights begs the question as to which arrangement of property rights is most efficient for the informational economy, and it raises a host of questions about privacy and security rights. How may we best 'balance' the protection of intellectual property in music, computer programs, video, multimedia works, and databases with the needs of other users? Again, it is important to note the way in which the community of rights has positive duties to help persons who are most deprived to develop their abilities of productive agency in accordance with the principle of human rights. The acquisition of property is one outcome of the development of productive agency. This does not mean, however, that the state itself should provide property for all persons. On the contrary, it would seem that individuals must use their own productive abilities to attain income and property. Practical questions thus are raised about the proper connection between productive agency and private property. For example, an individual may work hard, but fail to succeed in earning enough income – that is, their agency does not result in use- and exchange-values. Moreover, income and wealth do not always derive from productive agency, since the de facto inequalities that exist in the informational economy cannot be explained solely in terms of inequalities in productive agency. Furthermore, should income derive solely from the exercise of productive agency, especially given basic human needs for food, water, clothing, and shelter? And, especially germane to the privacy and security issues of the next two chapters: How is the *privacy* of property rights related to the mutuality and social solidarity of persons in the community of rights?

These are difficult questions beyond the specific policy debate concerning the impact of IT on work and employment. The question concerning the justification of private property rights must briefly be addressed, however, because property rights affect both the normative question of which arrangement of property rights is most efficient for the informational economy (which is beyond this work's aim and purpose), as well as the policy debates surrounding norms of privacy and security policy (chapter 5).

Two independent justifications of private property rights may be given: a 'consequentialist' justification based on human need and an 'antecedentalist' justification based on contribution, both of which are derived from the principle of human rights. If the main purpose of the

right to productive agency is to enable individuals to earn income through their own work, then the element of purpose, on the one hand, and the element of work, on the other hand, give rise to the two different justifications. Both justifications emphasize different aspects of the principle of human rights, and they have different implications concerning the subjects and objects of property rights as well as the role of the community of rights as the respondent of these rights. The consequentialist justification bears directly on the consequences for persons as productive agents who have legal rights; it concerns the *final cause*, the end, or the purpose served by individuals' having property rights. The consequentialist justification is derived from well-being as the substantive generic feature of action and focuses on purposiveness and the consequences that result from an individual's actions. The antecedentalist justification bears directly on the antecedents or the prior conditions and work activities that determine the subjects and objects of property rights; it concerns the *efficient cause*. The antecedentalist justification is derived from the freedom that is the procedural generic feature of action and focuses on voluntariness of action and the generating process of work that leads to the acquisition of property rights (cf. Locke, 1965 [1690]). Both freedom and well-being, then, as the necessary conditions of human action, enter into the contents or objects of each justification, and neither justification alone is adequate without the other.

The consequentialist justification of property should be interpreted in an unconditional manner. It is morally required that each person's freedom and well-being is protected in accordance with the principle of human rights, so it is also morally required that individuals have private property rights. This raises the further question, however, of whether or not the final cause of protecting individuals' freedom and well-being is best achieved through a system of communal, though not necessarily communist, or through private property ownership. Philosophers have long noted that communal property rights entail a lack of freedom of individual control over external things that allows an individual to exclude others from taking or using his or her own things without consent. Moreover, the security that follows from holding one's own property might be jeopardized, work incentives lost, and care of the property objects minimized. Note that the community's control over roads, police and national security protection, and information and communications infrastructures is on a different level from that of the types of property ownership that contribute to individual

freedom and autonomy. The latter types of goods are not public goods, but rather the necessary goods of each individual as a prospective agent. Individuals still have obligations to share some of their property with the community because they are, in part, 'social products' to whose productive agency the community contributed in the first place.

Inequality and the Restriction of Property Rights

In the consequentialist justification, property rights promote the freedom of the property owner, but at the same time they restrict the freedom of all other persons who are legally excluded from taking or handling the property object without the owner's consent. The paradox of freedom – the more freedom there is, the less freedom there is – is at play here. The paradox states that if 'A is free to do X,' then any law that gives A the freedom to do X must make all other persons 'unfree to prevent A from doing X or to determine whether A will do X' (Gewirth, 1996, 174). This logical point is similar to the correlativity of human rights and duties. If A has a right to do X, then it logically follows that all other persons have the duty to refrain from interfering with A's doing X. The fact that property rights enhance the owner's freedom and simultaneously restrict the freedom of others reveals that property relations are inevitably asymmetrical relations of power that involve struggle. Struggle is a 'limit situation' of the human condition, but this fact does not nullify the more important question of whether the freedom of property owners should always take precedence over the freedom others. Should the well-being that property owners derive from their property be maintained without any regard for the well-being of others? No, because the mutuality of human rights requires both that persons contribute to one another's acquisition of abilities of productive agency and also that they share some of the resulting property with the wider society. Property rights, like human rights in general, while serving to protect each person's freedom and well-being, are not absolute. The thesis of 'world ownership' serves to modify the privacy of property rights. The thesis states that 'if A produces X with the help of resources Y, which he does not personally own but which is owned by H (where H comprises all humans or at least all the members of A's own society), then A is not the sole owner of X; instead, X is at least partly owned also by H' (Gewirth, 1996, 195). So the owner cannot make an absolute claim.

The holding of property rights thus bears on the general question of

economic equality. If consequences for property owners are relevant to the justification of property rights, then it follows that their consequences for other persons are also relevant to the justification of property rights when viewed from the principle of human rights. The consequentialist justification of property rights entails all persons' having equal rights to property, but it does not necessarily mean that they have rights to equal amounts of property. If the use to which some individuals put their property is 'harmful' to others, especially the human rights of other persons, the owner's property rights may be called into question as a result of the harmful consequences of such use, including inequalities in property holdings so wide that they allow some individuals to dominate and oppress others.[1]

The antecedentalist justification of property rights is based on the individual's work or labour. In this view, property rights belong to individuals who actually produce the goods, whether commodities or services, that are the objects of rights. The justification acknowledges that, in the individual's transition from basic productive agency to property production, individuals must earn income through their own work. Just as productive agency requires that individuals develop skills and abilities, so, too, the antecedentalist justification of property rights requires private property generated by these skills and abilities. The just economic distribution of goods may be an ethical ideal, but without the actual production of goods, there would be nothing to distribute justly. The antecedentalist justification of property understands this traditional economic doctrine and is concerned with the 'efficient cause' of property rights, the actual generating process that leads to the acquisition of such rights. The individual's labour or productive action is the factor that justifies one's having property rights in the things that they produce. One important aspect of this justification is the way in which labour itself is an application or exercise of human rights. Because an individual has, in fact, exercised generic rights of action through labour, he or she should have rights in what is produced by this labour.

This 'purposive-labour thesis' of property, as Gewirth calls it, is important, because it actually functions to connect the two justifications of property rights:

> The labor justification of property rights through the generic rights of agency has its deeper basis in the nature of purposive action itself. The reference to purpose serves to connect, at an elemental level, the efficient-cause justification of property rights with the final-cause justification.

> Since it is by A's own efforts that X is produced or made available in ways that do not harm any other persons, and since A's direct purpose in so producing is to have X as her own thing either as a use value or an exchange value, to say that A does not have a property right in X would be to say that A's purpose in so acting may rightly be frustrated. But this, when generalized, would be an attack on the whole purposiveness of human action and hence on human agency itself. For all human action is performed with a view to achieving the respective agents' purposes; and such action is morally permissible insofar as it does not violate the generic rights of other persons. It follows that persons have property rights in things they have produced for the purpose of having such rights. (Gewirth, 1996, 184)

The purposive-labour thesis does not determine that the workers' product will have any exchange value. In this case, the worker has a property right in the product, but it is one that does not effectively fulfil the final cause or purpose of property. The objection that because the world is owned in common, nobody can claim exclusive rights to it (i.e., the world ownership thesis) limits the purposive-labour thesis. The antecedentalist justification sustains the purposive-labour thesis, with the world ownership qualification, and thereby provides for property rights; but at the same time the consequentialist justification limits property rights in the interest of economic equality. Both justifications point to the justice of sharing wealth as provided by the community of rights. The reality of our situation in the informational economy is that the antecedentalist justification invariably leads to unequal property rights and raises numerous questions about how rich or how poor persons should be in relation to each other. The classic economic 'contribution principle' states that 'distribution should be determined by the contribution; or, in comparative terms, how much goods or rewards persons get relative to one another should be determined by, and be proportional to, how much, by their prior work, they have contributed to the total product' (Gewirth, 1996, 204–5).

The contribution principle raises the difficult economic problem of how best to correlate work with income, where workers refer to those who sell their labour power in order to live. It does not matter whether the 'means of production' of the workers are their own hammers, sewing machines, word processors, computers, or Web sites. When workers are distinguished from capitalists in terms of ownership of the means of production, however, what is at issue are the capitalists' impersonal and

extensive mechanical, electronic, and other instruments that are used in large-scale industrial, post-industrial, and informational production. Apart from the historical evidence of brigandage and the 'inverse ratio' between labour and reward,[2] we would do well to recall some empirical data about our present situation. The ratio of top executive to factory worker pay has exponentially increased over the 1990s. If the average production worker's pay had risen as rapidly as CEO pay, then 'a worker would be making $110,000 a year today, instead of the $29,000 a worker actually makes. Put another way, the minimum wage today would be $22.08 an hour, rather than the $5.15 it actually is.' The average CEO pay was $10.6 million in 1998, a fivefold increase from the $1.8 million of 1990. CEO pay rose 36 per cent compared with only 2.7 per cent for the average blue-collar worker.[3] Surely the vast inequalities of rewards between capitalists and workers cannot be justified by any comparative contribution principle. Instead, what is operative here is a system where 'the capitalist uses his preexisting economic power to extract a reward that is grossly disproportional to the value of his contribution' (Gewirth, 1996, 212). The overnight, millionaire success of some agents' .com Internet IPO is a case in point.

These two ethical justifications of property rights are sound, but only with the appropriate provisos regarding the social contribution of the community to the individual, the responsibility entailed by purposive-labour, the limits to property rights stemming from the world ownership thesis, and the harsh empirical realities of economic inequality in the informational economy. The main analytical point we wish to stress, especially in what follows, is the way in which persons, through developing their abilities of economic productive agency, are able to earn sufficient income for their well-being and thereby acquire property rights. This development requires both individual responsibilities and agency, as well as the positive support of the state. The state's mandated policies of free public education, welfare payments for transitional or 'lifelong learners,' persons with disabilities, and the protection of private property combined with progressive taxation in order to prevent the abuses of power and great wealth, are vital. In this way, the community of rights seeks to reduce economic inequalities, not in a passive, static fashion, but in a dynamic way that takes seriously the teleology of the subject and his or her agency and development. The ideal is to move the individual from 'productivist welfarism' (defined below) where necessary, through education, to employment and earned income, to rights in property, to communal contributions, and

beyond. The community is characterized by human mutuality and social solidarity whereby the rich contribute, in the first instance, to the productive agency and development of the poor. In turn, the poor are enabled to contribute, through their own work and responsibility, to the well-being of others. Policy goals should embody such provisions in the economic constitution of the state.

The Global Situation: The Informational Economy

In the past two decades a new economy has emerged on a worldwide scale. Manuel Castells refers to this economy as both informational and global:

> It is *informational* because the productivity and competitiveness of units or agents in this economy (be it firms, regions, or nations) fundamentally depend upon their capacity to generate, process, and apply efficiently knowledge-based information. It is *global* because the core activities of production, consumption, and circulation, as well as their components (capital, labor, raw materials, management, information, technology, markets) are organized on a global scale, either directly or through a network of linkages between economic agents. It is informational *and* global because, under the new historical conditions, productivity is generated through and competition is played out in a global network of interaction. And it has emerged in the last quarter of the twentieth century because the Information Technology Revolution provides the indispensable, material basis for such a new economy. (Castells, 1996, 66; emphasis in original)

Sources of productivity are increasingly dependent upon the application of science and technology and the quality of information and management in the processes of production, consumption, distribution and trade. Advanced economies increase their productivity not so much from capital and labour inputs, but rather from a more efficient combination of production factors. We have witnessed a shift from material production to information-processing activities, both in terms of proportion of the gross national product and of the population employed in such activities. For firms, the quality of information and the efficiency in acquiring and processing it constitute the key strategic factors in competitiveness and productivity. The organization of production and economic activity has profoundly shifted from mass production to flexible, customized production; and from vertically

integrated, large-scale organizations to vertical disintegration and horizontal networks between economic units. The informational economy is global. Capital, production, management, markets, labour, information, and technology are organized across boundaries. The basic source of wealth generation lies in the human ability to create new knowledge and apply it to human activities through technological and organizational procedures of information processing.

Although the informational economy is global in reach, its development has been uneven. The structural evolution of the economy during the past thirty years reveals cleavages between major economic trading blocs, the marking out of macroregions, growing cross-regional investment patterns, the locations of firms, and exports and imports. There are winners and losers in the degree of penetration of regions by capital, goods, and services from other regions. It is not surprising that North America, Japan, and the European economic area represent the 'centre' of capital, technology, and market potential with which the peripheral players must either connect or perish (Ohmae, 1985). The information economy has affected north-south relations to such an extent that we may now speak of *'the end of the Third World as a relatively homogeneous economic region'* (Castells, 1993, 27; emphasis in original; see also Harris, 1986). The hegemony of the United States, whose comparative advantage was based on large markets and economies of scale in manufacturing, has declined somewhat as Japan and Germany successfully compete. The economies of South Korea, Taiwan, Hong Kong, and Singapore have made great strides since the 1960s. By way of contrast, Latin America (the lost decade) and Africa (de-development) have suffered because of changes in the world economy. The debt burdens of Brazil, Mexico, Argentina, Nigeria, and Venezuela have left them behind the transformation occurring in Asia. The low-income, agricultural economies of Africa, Asia, and Latin America are even further behind in the development process than in the past.

Globalization's Challenge to Social and Economic Rights

Globalization[4] has brought human rights under fire from many quarters. Despite the inflation of rights rhetoric, it must be admitted that human rights still function as a de facto global moral philosophy. There is no other international framework as far reaching as the international human rights regimes. We possess a tradition around economic rights that began with the emergence of the International Labour Organization

(ILO) following the First World War and its consensus about basic workplace rights and duties. The ILO's focus on employer-employee relations has been transformed by globalization. The Universal Declaration of Human Rights (UDHR) reminds us of the centrality of economic and social rights, including 'the right to social security ... the right to work, to free choice of employment, to just and favourable conditions of work and to protection against unemployment ... the right to equal pay for equal work ... the right to just and favourable remuneration ensuring ... an existence worthy of human dignity ... the right to form and to join trade unions,' 'the right to a standard of living adequate for ... health and well-being ... including food, clothing, housing and medical care and necessary social services, and the right to security in the event of unemployment, sickness, disability, widowhood, old age' (UDHR, art. 22, 23, cited in Walters, 1995a, 412). Globalization has undermined traditional employee protections and rights in the workplace and contributed to new structural forms of unemployment. The effects of globalization on vulnerable groups cut across industrialized and developing economies. When workers lack job security or basic employment-related protections, when social-welfare recipients are confronted with cuts, when structural unemployment results in plant closures and a declining public sector, these trends can be challenged by drawing upon international human rights law (Lamarche, 1995). The universality of economic rights to basic human freedom and well-being must take into account the empirical conditions of their possible effectuation. Given the vastness of global, unfulfilled rights to basic well-being and the societal bases of these unfulfilled needs, the correlative duties belong, in the first instance, to governments that can command the relevant resources and hence affect or restrain the relevant political power structures. We are in a difficult situation, because the erosion of the social welfare state in industrialized countries is occurring at a time when governments are increasingly less able to control and redistribute income and revenues generated by the knowledge-based economy. Statist economics were a failure, but we must also admit that capitalist market economies also are plagued by deeply rooted social ills such as poverty, unemployment, crime, and homelessness.

The Failure of Development Strategies

The basic development strategies of the post–Second World War period have failed. The 'traditional international trade model,' whereby raw

materials and agricultural commodities were traded for manufacturing and know-how, was replete with unequal exchange and exploitation, and it collapsed in the 1960s. The 'import-substitution industrialization model' collapsed in the 1970s. The 'outward-oriented development strategy,' which took advantage of cost/price differentials and was focused either on exports from domestic manufacturing firms or, to a lesser extent, on exports from offshore manufacturing facilities of multinational corporations, failed in the 1980s.[5] A new international division of labour was set during this time. Some regions of some industrializing countries thrived on the model of low production costs at the low end of the manufacturing world assembly line (e.g., Bangkok, *maquiladoras*), but most other industrializing countries suffered severe crises of development. In terms of structure, cheap labour was not a sufficient comparative advantage. Automation could easily replace unskilled labour while improving quality. The winning formula required a higher technological component. Many countries lost out in the process of continual upgrading of the technological component of manufacturing products and processes in an effort to keep pace with international competition. The Pacific Asian Network Integration and Consulting Services made the technological transition and became competitive worldwide in the low to middle ranges of electronic products, winning market share in high-technology international trade.[6]

In contrast, the economies of sub-Saharan Africa and Latin America plummeted during the 1980s, falling from an annual gross domestic product growth of 4.2 per cent and 6.1 per cent to 2.4 per cent and 1.6 per cent in 1980–89 (i.e., negative growth in per capita terms). By 1991 the Direct Foreign Investment in all of sub-Saharan Africa was less than that in Chile, which has a population of only 12 million people! (Islam and Morrison, 1996).

The relation between the role of 'multinational corporations' (MNCs), development, and human rights is complex. William Meyer (1998) has empirically analysed the relation between human rights and the international political economy in Third World nations. The so-called engines of development school maintains that MNCs directly promote economic and social rights and indirectly support civil and political rights. Unemployment rights and social security depend on the level of economic development. MNCs create jobs by bringing in new capital and technology, and they also provide health care benefits. In contrast, supporters of the 'Hymer Thesis' argue that Third World MNCs create situations that lead to lower levels of human rights, espe-

cially violations of first-generation civil and political rights. Poor nations are exploited by wealthy countries, and it is the organizational structure of MNCs that causes inequality among nations. Meyer uses aggregate and cross-national data to describe the international political economy of human rights. He finds a statistically positive relationship between the presence of MNCs, gross national product, U.S. economic aid, foreign debt, and levels of civil and political rights in the Third World. Least-developed countries (LDCs) with higher levels of development, more economic aid, and heavier debt burdens tend to score higher in regard to civil/political rights rankings. MNCs, as reflected in direct foreign investment, also are positively associated with economic rights. Life expectancy, literacy, and infant survival rates tend to rise as MNC investment increases across LDCs. Increased GNP has a positive impact on socio-economic rights.

In most quantitative studies foreign aid is rarely conceptualized as a possible determinant of human rights in the Third World. Unlike previous authors, who assume rights to be the independent variable and economic and military aid the dependent variables, Meyers postulates aid as the determining (independent) variable and levels of human rights as the dependent (determined) variable. The arguments to be tested are first modelled, then operationalized (multivariate regression), and subsequent equations are estimated based on the best available data for the largest possible samples. There exists a *positive* relationship between U.S. economic aid and civil-political rights in the fifty or more LDCs studied. Increases in U.S. economic aid are likely to be associated with improvements in first-generation rights. Military aid, in contrast, is inversely related to levels of rights. Military assistance (defined as more than $1 million per year) has a negative impact on civil-political freedoms. The link between development (GNP) and human rights is generally significant and consistent over time. Statistically significant declines in mortality rates and illiteracy are associated with increased economic aid during the 1980s. With increased economic development there is an improvement in human rights. The militarization of an LDC political economy by means of foreign security aid serves to endanger health, education, and social welfare. These results are consistent with classical democratic theory and conform to the predictions of early post–Second World War theories of development. Neither the 'Hymer Thesis' nor the 'engines of development' thesis are false; instead, both are supported by evidence, but at different levels of analysis and in different contexts.

'Winners,' 'Losers,' and the Risk of Barbarism

The global 'situation' has changed. The Third World no longer exists as such, but it has been rendered meaningless 'by the ascendance of the newly industrialized countries (mainly in East Asia), by the development process of large continental economies on their way toward integration in the world economy (such as China and, to a lesser extent, India), and by the rise of a Fourth World, made up of marginalized economies in the [least developed] rural areas of three continents and in the sprawling shanty towns of African, Asian, and Latin American cities' (Castells, 1993, 37). Winners and losers are classed into four main groups defined by their ability to produce informational goods and services. The 'clear winners' are the rapidly growing, newly industrializing countries in Asia. The 'potential winners' are Mexico and Brazil. Next are India and China, which, because of potentially huge markets and highly skilled human capital, are integrating into the global economy. The 'clear losers' are Fourth World marginal rural economies and sprawling urban peripheries and 'information slums' (Carnoy et al., 1993 Lanvin, 1995).

The incapacity of a number of developing countries to adapt to the informational economy appears to be leading to radical reactions and the 'risk of barbarism' (Cardoso, 1993, 150 Sottas, 1990). Some countries have established new linkages with the global economy through the criminal economy by means of drug production and trafficking, illegal arms deals, smuggling, money laundering, and commerce in women and children or in human organs for transplant (Mussington et al.,1998). Another reaction entails widespread individual and collective violence. Frustration over disintegrating economies and societies is expressed in ancient ethnic struggles. A third reaction is the rise of the ideological and religious fundamentalism associated with terrorism (Hoffman, 1997), including advocacy of the non-universality of human rights. This reaction is the flip side of the exclusion that many individuals feel in our current global economic situation. Without a countervailing and deliberate reform of the current world development model, the informational economy of the twenty-first century will have to face not only starving children, but the proliferation of criminal mafias, dramatic inter-ethnic violence, and fundamentalist groundswells. If at some point it becomes economical to clothe, feed, and house the entire world population with an input of only a fraction of the world labour force, the distribution of earned income will still be

highly skewed. The challenge of socially acceptable wealth distribution mechanisms will likely be imperative if we are to avoid 'barbarism' (Blume, 1998).

Non-Virtual Poverty and Full Employment

The need for human development in the informational economy is inextricably linked to the problem of poverty. The existence of poverty is, at the least, a prima facie violation of human rights that negatively affects an individual's capacity for human development. To be sure, there was great success in reducing poverty in the twentieth century:

> Since 1960, in little more than a generation, child death rates in developing countries have been more than halved. Malnutrition rates have declined by almost a third. The proportion of children out of primary school has fallen from more than half to less than a quarter. And the share of rural families without access to safe water has fallen from nine-tenths to about a quarter ... China, and another 14 countries or states with populations that add up to more than 1.6 billion, have halved the proportion of their people living below the national income poverty line in less than 20 years. Ten more countries, with almost another billion people, have reduced the proportion of their people in income poverty by a quarter or more. Beyond mere advances in income, there has been great progress in all these countries in life expectancy and access to basic social services. (UNDP, 1997)

At the United Nations World Summit for Social Development in 1995 most countries committed themselves to the goal of eradicating severe poverty in the first decades of the twenty-first century. Yet one-quarter of the world's people still remain in severe poverty in a global economy of $25 trillion, with more than one-fifth of the world's people living in extreme poverty, on little more than U.S. $1.00 per day (UNDP, 1998). Poverty involves not only the poverty of income and basic services, but denial of choices and opportunities for living a tolerable life – in other words, the basic conditions leading to the potential for action and successful action in the sense of basic, non-substractive, and additive well-being. In both developing and industrial countries children, women, and the aged suffer more than others. The poverty of choices and opportunities is often more relevant than the poverty of income. This is why the deprivation of productive human agency

focuses on the causes of poverty and leads directly to strategies of education, empowerment, and full employment to enhance action opportunities for individuals.

For most global intergovernmental organizations and western governments, employment has not been a major policy issue. Rather, it has been a socio-economic concern secondary to economic growth. Polish Prime Minister Mazowiecki delineates the matter clearly: 'Full employment – at the price of waste and economic stagnation – is no longer the ideal situation for us. Unemployment is not ideal either, but it is a necessity that we have to learn to live with, just as the other market economies' (ILO, 1991, 12–13). The ILO's Declaration of Workers' Fundamental Rights defines these rights as the prohibition of forced labour and child labour, freedom of association, freedom to form trade unions and carry out collective bargaining, equality of pay between men and women for work of equal value; and the elimination of discrimination in employment (ILO, 1998). While the ILO clearly supports the feasibility and desirability of full employment, there is hardly any mention of a right to employment. Moreover, foremost among the policy requirements for reversing recent trends away from full employment is 'to reverse the trend decline in growth rates over the past two decades' while moderating wage inflation and improving the design and implementation of labour-market policies (ILO, 1996). A right to employment, which evolved from conceptions of national solidarity and welfare state obligations in the century before the Second World War, is noticeably absent from the literature, despite its inclusion in the UDHR; the International Covenant on Economic, Social, and Cultural Rights as well as the Council of Europe's European Social Charter; and despite support for full employment in OECD conventions and recommendations and the ILO's Committee on Employment in 1983–84 (ILO, 1984).

The informational economy requires a global response to unemployment that can build on a new spirit of global socio-economic solidarity and justice. The rights that need to be assured should, in principle, include 'equal employment opportunity, free association, and security against arbitrary and sudden termination of employment. These should be combined with a reinforced duty of all states to use all available policy instruments to prevent high levels of unemployment' (Siegel, 1994, 183). In the international human rights literature it is generally conceded that states have obligations in accordance with resources and capabilities. States should also not be able to trade mass

unemployment or its exacerbation for other political and economic interests. Intergovernmental organs and forums should be able to define responsibilities of national governments as well as their own obligations. Potential workers or the long-term unemployed cannot resort to lawsuits and expect to win them or to gain particular jobs or the right to any employment, but they should have recourse for complaints to international organizations when states ignore the interests of workers. Time and again, we hear or read that national, regional, and global agencies should be held fully accountable for their efforts to promote full employment and to avoid mass unemployment. Can information technology itself serve development goals, including full-employment policy concerns?

Harnessing Information and Communications Technologies for Productive Agency

Despite the rise of the Fourth World and roadkill on the global information highway, there are some hopeful signs of ICTs' being harnessed to development goals. Between 1995 and 1997, the United Nations Commission on Science and Technology for Development (UNCSTD) Working Group on IT and Development investigated the empirical evidence on the benefits and risks of ICTs in developing countries. It found that there are many instances where the use of ICTs is bringing widespread social and economic benefits, but it also found just as many instances where ICTs are making no difference or are actually having harmful effects. UNCSTD's overall assessment, however, suggests that governments and other stakeholders should build new capabilities for producing, accessing, and/or using ICTs, including new social capabilities and innovation systems necessary for sustainable development. 'Social capabilities,' we should add, refers to a society's stock of shared values and social virtues, such as honesty, mutuality, promise keeping, and commitment. Like physical capital (e.g., land, buildings, and machines) and human capital (e.g., the skills and knowledge that we carry), social capital helps to produce wealth and is of economic value.

The same difficulties in measuring productivity in the North American situation apply to ICTs in developing countries (Chataway and Cooke, 1995). One difficulty in measuring the productivity impact of ICTs concerns the nature of the beast – information – whose value varies dramatically depending upon the context. The liberalization of

competition in domestic markets has also tended to limit empirical evidence on the diffusion and use of ICTs in order to protect commercial interests. The implementation of ICTs in least-developed countries (LDCs) raises a host of problems related to the reliance on electricity; financing; problems of access and gender equity;[7] information content; and specialized participatory, facilitating, and control skills. 'If the satisfaction of fundamental human needs is the "driver" of the introduction of ICTs there is a greater chance of success than if the technology is permitted to "drive" applications. This means that social and economic development go hand-in-hand' (Mansell and Wehn, 1998, 117). In a world where nearly a billion people are illiterate and lack access to safe water, where 840 million go hungry or face food insecurity, and where nearly one-third of the inhabitants in LDCs are not expected to survive to age forty (UNDP, 1997), it seems reasonable to be guardedly optimistic about the use of ICTs for development. There is also the danger that ICTs might become simply another democratization tool 'for' the Third World (Graf, 1996).

The North American Situation

While people have been worrying about machines replacing human beings since the beginning of modern capitalism, few would deny that we live in a historical situation marked by downsizing and lean-and-mean global corporate strategies. Job security and corporate responsibility for employee welfare appear to be far down on the list of priorities. Pressures for globalization and international competitiveness made possible by new information technologies encourage the near worship of so-called flexibility. These pressures have given rise to 'locational tournaments,' where governments have recast their conception of competition in more mercantilist terms as the ability to attract investment from elsewhere (Mytelka, 1995). Recent recessions have enabled firms to drastically reduce workforces or move large-scale operations to countries with cheaper and less protected labour. So far these developments have not engendered substantial public criticism, even as weakened labour unions seem less able to contend with new pressures by managers to identify and cultivate a firm's core competencies.

New organizational forms have been brought about by the 'information-based organization' (Drucker, 1988). The so-called shamrock organization – with its three-leaf professional core of employees, temporary employees, and contractor-suppliers – has decreased the value of

many types of employees to corporate leaders (Williams, 1997). The shift from the command-and-control style, which has dominated large organizations, is not necessarily bad, since the development of work teams where the lines between boss and employee have become blurred may eventually lead to a 'management and accounting revolution' (Beck, 1992).

The issue that poses the greatest ethical concern for IHAC policy makers is the impact of IT upon jobs and economic growth. E-commerce involves 'conducting, managing and executing business transactions using computer and telecommunications networks. It can save time and be relatively inexpensive. It creates opportunities for companies to shorten procurement cycles, cut inventory costs, customize products and expand their market shares. Ultimately, electronic commerce will result in rapid, essentially paperless transactions, sharply reducing both the cost and geographic constraints associated with global trade' (IC, 1997b, 33). In information policy the view that e-commerce is Canada's top economic priority has never been compromised. In fact, IHAC believes that the creation of a legal and policy environment that promotes e-commerce on the Internet is the only way to ensure that the economic promise of information highway policy can be realized. Surveys of Canadian employers and workers show that they acknowledge the revolutionary economic changes occurring as a result of technology (OECD, 1996; Reid, 1996). In 1998 $13 billion in goods and services were purchased through the Internet, and the market is expected to grow to $73.7 billion by the year 2001 (CECS, 1998). About 75 per cent of Canadian businesses expect to buy and sell on the Net by then, and some estimate that business-to-business markets will swell to $327 billion by the year 2002 (Aly, 1997). Innovation, ideas, and information drive growth and now overshadow physical goods and services; but the behaviour of interacting markets in the production, distribution and consumption of information goods is far from clear in a world where, in seconds, day-traders enact far-reaching global currency trades that impact entire national economies. It was found that 88 per cent of Canadians support and encourage IT development, while 51 per cent supported the statement: 'I really worry that new technologies take away more jobs than they create' (EKOS, 1996). What is clear is that traditional economic theories about market behaviour do not seem to fit the informational economy and that 'low employment can weaken demand, decrease output and cause further declines in the demand for labour' (IC, 1997b, 81).

Competing Moral Visions: E-Commerce versus E-Commons

During all phases of information highway policy some commentators argued that IT would have negative impacts on employment, equity, leisure, and social cohesion (Forrester, 1996; Menzies, 1996). Indeed, two competing moral visions of the Internet have arisen: a vision of the I-way as a space for e-commerce versus the ideal of an electronic commons (Moll and Shade, 2001). The commerce or 'jobs-agenda' vision has led a variety of individuals, organizations, and special-interest groups to criticize the government policy as a market-driven, top-down approach – an information equivalent of trickle-down economics. In this view, the global commodification of information has negative implications for social control and power over community and cultural forms. 'Commodification' refers to the transformation of use-value into exchange-value, in which objects and ideas are stripped of their intrinsic, moral, aesthetic, and utility values and replaced by market values, or what an object or idea will return in economic trade (Babe, 1995; Mosco, 1989, 1995; Yerxa and Moll, 1995; Varian, 1995). This shift is leading to an ever-widening gap between the rich and the poor, between wealthy information 'haves' and poor information 'have-nots.' Critics of IHAC policy suggest that the e-commerce vision of the Internet is really about increased transnational corporate power, the blurring of national identities, the breakdown of human solidarity and community, and a neo-liberal policy agenda of privatization, deregulation, and user-pay, which are leading to the collapse of public space and education. This is an information world of in-your-face capitalism, where one loses a job one day, the ex-employer's stock prices rise the next day, and the telecommunications CEO – already boasting a seven-digit salary – gets a fat raise or stock options on the third day. Such developments are not mere fantasy; they have emerged in the context of corporate mergers and acquisitions and growing societal divisions and unemployment. Over 19 per cent of Canadians appear to have no ties or commitments to mainstream economic life, 22 per cent are living on government programs with no alternatives. In short, 41 per cent of Canadians no longer feel connected to mainstream society in the nascent information economy (EKOS, 1996). In this view, e-commerce is really 'e-con,' with corporate propaganda blurring Canadian national interests with business interests, collapsing the public interest into private interest, and whittling away public information access and democracy (Gutstein, 1999). The I-way is being used not to serve the goal of participation and social

justice in the electronic commons, but rather as a palliative for a vulnerable time of social and economic transition (Franklin, 1994; Turkel 1984, 1996). The electronic commons vision of the information highway wants to guard against the logic of technocratic and economic polarization. It holds out a view of electronic democracy that can be to the benefits of all citizens, male and female, in the electronic polis.

There is surely merit to the argument that companies and organizations that fail to adapt to e-commerce may be in danger of losing a competitive position or missing opportunities. We do well to avoid an either/or – either e-commerce or e-commons. But whether or not e-commerce among rapidly growing companies will help to create jobs, other than for those with high-technology skills, is a moot question. Drucker (1994) believes that only 30 per cent of future workers will be part of the so-called knowledge worker class. The productivity of the non-knowledge services worker will be the greatest social challenge of the digital world, but the nature of non-knowledge services work and how it will be compensated is not merely a social challenge. It also signals a profound change in the 'human condition.' What this social challenge means – 'what are the values, the commitments, the problems, of the new society – we do not know. But we do know that much will be different' (Drucker, 1994). While the industrial revolution was labour intensive, the present revolution is 'restructuring' workers at an ever-increasing rate. Statistics Canada reported that 38,000 full-time jobs were lost in February 1997, despite the fact that industry was operating at 85 per cent of capacity at the end of 1996 – hence the expression 'jobless growth' (Beauchesne, 1997).

The e-commerce debate poses a host of ethical questions. Because the Internet knows no international boundaries, how will governments tax digital products such as software, music, videos, and services rendered over the Internet from another country? Will this be an opportunity for governments to increase their tax revenues, or an opportunity for transnationals to find tax shelters? Won't businesses tend to set up their virtual shops where tax law is lenient and rates are lower? The international accounting firm KPMG has prepared one solution to the problem. Their idea is to have the European Commission set up virtual bonded warehouses holding computer-controlled inventory at strategically located sites around Europe. Goods would be tracked by one central bonded warehouse and could be audited by customs officials using the Internet (Powell, 1997). The fact that smaller players may be able to enter the market as a result of e-commerce does not change a

host of traditional business ethics issues concerning competition and fair play.[8]

The Conference Board of Canada entered the policy debate in 1997 with the publication of *Jobs in the Knowledge-Based Economy.* Lafleur and Lok (1997) conclude that the adoption of IT does not lead to an overall loss in employment. Firms that both purchase and use IT intensively have actually created more jobs in the long run than those that do not, even though IT's impact across industries and occupations is not uniform. High-IT-intensive industries (e.g., commercial services, electrical power and gas distribution, electrical products, construction) experienced significant employment growth during the period from 1986 to 1995, while in low-IT-intensive industries (forestry, mining, furniture and fixtures, textile products) employment fell. There are, however, a number of important factors that affect the impact of IT on employment. A great deal seems to depend on how much IT investment occurs, how quickly the technology is diffused, the extent to which labour productivity is increased, how wages and product prices respond, and the time-frame under consideration. Much also depends on the point in the economic cycle at which new IT is introduced, governments' policy reactions, the flexibility of labour markets, the skill mix of the workforce, domestic and international competition forces, and the specific regulatory environment in which a firm operates. In the long run, they conclude, price, income, and investment benefits compensate for short-term employment loss.

The Conference Board's macroeconomic forecasting model charts the flow of economic activity arising from new IT in terms of 'productivity impact' and 'investment impact.' With respect to productivity impact, the board admits that the extent to which productivity increases depends on whether IT replaces workers, the speed at which workers can do their jobs, the proportion of workers or workers' hours affected by IT, and the 'diffusion' rate – the rate at which the full potential of the new technology is realized. Diffusion rates, in turn, are affected by the training and education of the workforce and how well institutions adapt to change and innovation. The assumption here is that as productivity increases, there is initial employment loss. If cost savings are passed through to prices, however, then output increases and net employment gains result. On the other hand, if firms do not pass on the cost savings resulting from diffusion to consumers, then there is no real increase in output and the initial job losses result in net employment losses. With respect to investment impact, the authors

assert that investment creates jobs independently of the productivity effect. Availability of more investment dollars raises production in IT industries and has a positive impact on other industries through income and consumption.

The 'End of Work'?

The Canadian policy debate follows on the heels of the American debate launched by Jeremy Rifkin's controversial book, *The End of Work*. Rifkin argues that the 'apostles and evangelists' of the information age presuppose that the Third Industrial Revolution will succeed in creating more new job opportunities than it forecloses. The promised increases in productivity will be matched by elevated levels of consumer demand and the opening up of new global markets to absorb the flood of new goods and services that will become available. Rifkin does not deny IT productivity growth so much as challenge its implications for a right to participation and a government-guaranteed income: 'In the debate over how best to divide up the benefits of productivity advances, every country must ultimately grapple with an elementary question of economic justice. Put simply, *does every member of society, even the poorest among us, have a right to participate in and benefit from increases in productivity brought on by the information and communication technology revolutions?* If the answer is yes, then some form of compensation will have to be made to the increasing number of unemployed whose labor will no longer be needed in the new high-tech automated world of the twenty-first century' (Rifkin, 1995, 267 emphasis added).

We are set on a firm course to an automated future and a near-workerless era, if not in the service sector, then at least in the manufacturing sector. Globalization and automation will permanently idle hundreds of millions of workers. Unused human labour will be the overriding reality of the twenty-first century. If human talent, energy, and resourcefulness are not redirected to constructive ends, then civilization will sink into a state of destitution and lawlessness. The middle class finds itself buffeted on every side by technological change, reduced wages, and rising unemployment. Many more individuals are looking for quick solutions and dramatic rescue from the market forces and technological changes that are destroying former ways of life.

In Rifkin's view, the Third Industrial Revolution is spreading quickly to the Third World. Capital-intensive, highly automated pro-

duction has now been successfully transplanted. Because the wage component of the total production bill has shrunk in proportion to other costs, the cost advantage of cheap Third World labour has become less important. Advances in technological innovation have made the advantage of human labour over machines a thing of the past. Between 1960 and 1987 'less than a third of the increase in output in developing countries ... came from increased labor,' while 'more than two-thirds [came] from increases in capital investment' (Rifkin, 1995, 204). Whether the context is the *maquiladoras* or the Japanese-looking plants in Brazil, machines are replacing workers. The polarization of incomes for the elite knowledge workers and growing long-term unemployment for millions of others has led to labour unrest in Bangkok, China, India, and the United States. Rifkin's prognosis is not good: 'Between now and the year 2010, the developing world is expected to add more than 700 million men and women to its labor force – a working population that is larger than the entire labor force of the industrial world in 1990 ... Worldwide, more than a billion jobs will have to be created over the next ten years to provide an income for all the new job entrants in both developing and developed nations. With new information and telecommunication technologies, robotics, and automation fast eliminating jobs in every industry and sector, the likelihood of finding enough work for the hundreds of millions of new job entrants appear slim' (Rifkin, 1995, 206).

The problem, in short, is that new information technologies are bringing us 'near workerless production' at a time when the world's population is surging to an unprecedented level. The problem is exacerbated by the influx of immigrants into poor communities, who are competing for a smaller slice of the economic pie, thus giving rise to neo-Nazi youth gangs as well as neo-fascist movements in France, Italy, and Russia. Rifkin's practical solution is to build up the 'Third Sector' and renew communal life. Instead of a market economy based solely on economic productivity, which is amenable to the substitution of machines for human input, he advocates a new social contract and an economy centred on human relationships, feelings of intimacy, companionship, fraternal bonds, and stewardship. His alternative vision to the utilitarian ethics of the marketplace, with its materialistic cornucopia and resource depletion, includes a 'shadow wage' for volunteer work given to legally certified tax-exempt organizations and a government-provided 'social wage' as an alternative to welfare payments and benefits for the permanently unemployed. A social wage would build

trust and shared commitment to community-building tasks. It would be extended to management and professional workers whose labour is no longer valued or needed in the marketplace. He also proposes grants to non-profit organizations to help to recruit and train the poor for jobs in their organizations. In addition to public-works projects and corporate tax credits for hiring welfare recipients and huge subsidies in the form of direct payments and tax breaks, he wants a greater expansion of service programs for impoverished communities. The shadow and social wages could be paid for by replacing current welfare bureaucracies with direct payments to individuals performing community service work, discontinuing costly subsidies to corporations that no longer invest at home, cutting unnecessarily bloated defence programs, and, most important, by enacting a value added tax (VAT) on all non-essential goods and services, which would tax consumption rather than income. The VAT would also be targeted and levied on IT goods and services, the entertainment and recreation industries, and advertising, thus hitting the 'symbolic analyst' class the hardest and asking them to help those cast aside by the high-tech global economy.

Empirical Problems with the 'End of Work' Thesis

Although we are extremely sympathetic to Rifkin's heartfelt concern for human dignity and the renewal of human and social community ties, there are two main empirical problems with the 'end of work'[9] thesis, which are related to unemployment data and the productivity paradox.

First, unemployment now is a relative concept, which, at least under U.S. definitions, requires that one is looking for work. If you have given up looking for work, you do not count. From a historical perspective, unemployment today is very low, compared with standards of the past 30 years. In January 1998 the average U.S. unemployment rate was 4.7 per cent compared with 7.0 per cent over a 108-year average, and 5.6 per cent in the post–Second World War period. In fact, 64.2 per cent of the adult population was working. The so-called broad unemployment rate stood at 9.3 per cent. This rate includes those employed part time for economic reasons, such as individuals who want full-time work but can find only part-time work, and those 'marginally attached' or those who want to work but have hopelessly given up the search (Henwood, 1998). The U.S. Bureau of Labor Statistics lists thirty occupations with the greatest projected growth between

1994 and 2005.[10] Of the top thirty categories, only 7 per cent fall in the class of 'symbolic analysts' with a 13 per cent projected growth by 2005. Indeed, 'engineers, computer professionals, and associated technicians together now account for about 3% of total employment and under 7% projected growth' (Henwood, 1996, 2). These data stand in sharp contrast to those of scholars like Noble (1995, 1998), who see rising unemployment as proof of the thesis that all technological developments sooner or later manifest themselves in job losses and rising unemployment.

In Canada the picture appears more mixed. Osberg et al. (1995) have analysed the shrinking number of opportunities for blue-collar and white-collar workers in various sectors of the economy. In the Maritimes and Nova Scotia, the role of technology has altered jobs or reduced them altogether in the coal-mining industry. The nature of the production process has fundamentally changed, with productivity now depending primarily on coordination of jobs and cognitive and social skills, not on individual physical effort. The common denominator in the mining, fishing, construction, and farming industries is that all employ fewer workers today than they have in the past. Between 1989 and 1992, 338,000 jobs in manufacturing in Canada disappeared, a decline of 16 per cent in employment. The textile and forestry industries were particularly hard hit by the North American Free Trade Agreement. In sharp contrast to the textile and forestry industries, the aerospace industry has flourished because of high-quality technology and a more egalitarian team management. Although there are opportunities opening up in the service and information industries, these new jobs are not being created fast enough to replace the old ones. In the early days of the telecommunications and computer revolution, there was a faith and technological optimism about the role that telecommunications would play to encourage job diffusion from the city to the country. There has been minimal technology diffusion, however, even though IT has 'delayered' levels of management with more broadly diffuse supervisory roles (Osberg et al., 1995). Indeed, in the years between 1994 and 1996, Canada's unemployment rate was roughly even, at 10 per cent, 9.8 per cent, and 9.8 per cent, respectively (ILO, 1996). By 1998 unemployment had fallen to 8.3 per cent. In September 2000 Statistics Canada reported the seasonally adjusted labour participation rate at 65.9 per cent, the employment rate at 61.4 per cent, and the national unemployment rate, for both sexes age fifteen and older, at 6.8 per cent.[11]

Even the experience of developing countries does not support the 'end of work' thesis. To be sure, Third World unemployment grew in the second half of the 1980s in the midst of what most of the developed world experienced as a major economic expansion. In many favoured developed countries, the boom of the 1980s ended with unemployment at a higher level than it was at the end of the previous cyclical expansion. The recession of 1990–93 brought unemployment statistics to politically dangerous levels in countries like Britain, France, Spain, German, and Italy. The fifteenth edition of the Organization for Economic Co-operation and Development (OECD) publication *Employment Outlook*, notes that there are 36 million unemployed individuals in OECD countries. Over the 1990s there have actually been structural unemployment declines in Ireland, the Netherlands, New Zealand, and the United Kingdom, but unemployment increases in Finland, Germany, Spain, and other countries. Workers' perceptions of job insecurity have certainly risen sharply, but 'on average, jobs last just as long now as in the 1980s' (OECD, 1997b, 2). There would appear to be, then, no real long-term structural change in the relationship between economic growth and employment growth in the OECD countries.

This is not to suggest that global underemployment and unemployment are not serious problems: they are. The ILO called the global employment situation 'grim' in its *World Employment, 1996–97* report. 'Nearly one billion people around the world, approximately 30% of the entire global work force, are unemployed or underemployed in industrialized and developing countries alike' (ILO, 1996, 4). The ILO calls for renewed international commitment to *full employment* in order to reverse global unemployment and underemployment. Current levels of unemployment and 'jobless growth' make no economic sense and are neither economically nor socially sustainable. Yet the ILO sees no evidence that globalization, technological change, or even corporate downsizing are bringing about an 'end of work.' Indeed, Kari Tapiola affirms that 'the information technology revolution is a key element in globalization' and that 'nations, enterprises and individual workers who are able to acquire, transform and use information productively and imaginatively will benefit from the technological advances now set in motion' (ILO, 1997, 1,2). At the same time, *full employment* is both feasible and highly desirable and should not be abandoned at a time when trade and investment flows are being integrated into the world economy. The problem with developing countries is that workers 'are engaged in low-productivity work that is often physically onerous but

yields only meager earnings.' Although full employment is a long-term objective, it nonetheless 'provides a useful framework for the formulation of employment policy' (ILO, 1996, 3).

The Productivity Paradox

A second empirical problem with the 'end of work' thesis stems from the assertion that work is disappearing because of productivity gains, whereby machines are replacing labour. Industry Canada, the Conference Board, and Rifkin's work reveal that expert economic opinion is solidly divided on the question of the impact of IT on productivity. The apparent contradiction between the deceleration in measured productivity growth rates in most industrial countries since 1973 and the extraordinary growth of IT during the same period defines the so-called productivity paradox. As Solow (1987) asked, why can you 'see the computer age everywhere but in the productivity statistics'? The productivity paradox, in Rifkin's view, 'suddenly disappeared' in 1991 (Rifkin, 1995, 91).

Some American and Canadian analyses of productivity directly counter Rifkin's thesis. Drawing upon U.S. Bureau of Labor Statistics data, Doug Henwood has argued that there is no U.S. productivity miracle. Labour productivity in all private U.S. non-agricultural industry is growing under 1 per cent per year. While manufacturing productivity is growing more quickly, computers are not making human workers obsolete, nor does the bureau's capital productivity series support any empirical evidence of fundamental change. Despite the conceptual and practical difficulties surrounding the measurement of capital productivity, Henwood (1996, 3) states that the 'output per unit of real capital' is in a forty-year downtrend.

Sharpe notes that between 1992 and 1995 investment in office computers in the Canadian service sector rose 64.2 per cent in real terms, but total factor productivity advanced a meagre 1.2 per cent (Sharpe, 1998). Even more significant is the fact that service industries with the highest percentage of total investment seem to have experienced the worst total factor productivity growth. So what accounts for this paradoxical behaviour of productivity growth?

Sharpe advances three basic hypotheses to account for the apparent productivity paradox. The first hypothesis argues that 'the benefits of IT are already here,' but statistical agencies underestimate increases in real or inflation-adjusted output arising from computerization, especially in

the service sector. Variations on this hypothesis are that the benefits of IT cannot be captured in output statistics – for example, benefits resulting from greater customer service – and that slow demand growth acts as a negative influence on underlying productivity growth.

A second major explanation is the 'lag hypothesis,' which takes electricity as its main historical analogue. Just as it took forty years from the time the first dynamos were introduced for the diffusion of electricity to result in faster productivity growth, so, too, the productivity effects of IT take a long time because we humans take a long time to adapt organizational structures to gain the full benefits (Davenport, 1997; David, 1990). An MIT study by Brynjolfsson and Hitt (1993) published productivity data for more than 380 giant U.S. firms between 1987 and 1991. Their conclusion is that computers added a great deal to productivity, but also contributed to downsizing. The lag in productivity gains was a result of outdated organizational structures, or the wrong use of IT, but not with new information technologies per se. We must also place Industry Canada and the Canadian Conference Board report in the 'lag hypothesis' camp. The latter's macroeconomic forecasting model assumes a time frame from 1990 to 2015: '[Canadian IT] growth in productivity fell from 1.84 per cent in 1990 to 1.66 per cent in 1996. Under status quo conditions, it is forecast to continue to fall, reaching 1.26 per cent in 2005. With the introduction of new IT spending, however, productivity growth is expected to increase gradually over the forecast period, reaching 1.72 per cent in 2015' (Lafleur and Lok, 1997, 12). The Conference Board's model assumes an IT investment average of 6 per cent per year between the period 1997–2015 and under status quo conditions.

A third hypothesis stresses the 'exaggerated benefits' of IT. There is no productivity paradox, because one shouldn't expect it, given IT's total investment in the economy. A variation on this thesis is that in many economic areas, IT does not basically alter production and improve productivity. In fact, many computer applications, such as spreadsheets, graphics and presentation programs, e-mail, and Web sites, may create little value, and games are often a productivity sink. Similarly, it is also argued that the costs of IT are greatly underestimated. Hardware and software upgrading, technical support, employee training and retraining, and the substitution of expensive labour and machines for cheap labour actually reduce the net benefits of IT. The year-2000 conversion problem cost U.S. $600 billion to correct, and this a permanent feature of IT use (Jones, 1999).

Each of the above hypotheses may capture aspects of the productivity paradox. To be sure, based on quantifiable indicators of output like ATM transactions processed, IT has increased productivity. But when it does not fundamentally affect the nature of the production process, as may be the case in many managerial and professional activities, IT does not directly increase any quantifiable indicator of output. Sharpe concludes that the strongest case can be made for the mismeasurement and exaggerated benefits of the lagged benefit hypothesis. Thus, in his view, we need to give priority to the development of better output and performance measures and indicators for the service sector and provide tougher approval criteria for IT investment decisions in the private sector.

Despite the empirical problems with the 'end of work' thesis, we do not want to minimize the increasing harshness of economic life as a result of downsizing and technological change. Even if there is no general disappearance of work, it is difficult to dispute rising wage polarization, the decline of middle-income jobs, the loss of fringe benefits, overwork, job insecurity, rising stress levels, and much alienation in our present historical situation (Osberg and Sharpe, 1998).

The Ethical Objection to the 'End of Work' Thesis

The ethical objection to the 'end of work' thesis is tied to the concern for social and economic rights, including full employment policy. Is there really no need for work? Objections are often made that the protection of human dignity and well-being can be achieved without individuals' having to work. Let us assume for the sake of argument that the first and second hypotheses regarding the productivity paradox noted above are correct. In this view, immense IT productivity is real, or will be realized in the short – or middle – terms of the twenty-first century. The argument is that such productivity now makes it possible for modern technology to supply all individuals' basic needs without their having to work. Moreover, and assuming a 'natural' rate of unemployment,[12] full-employment policies are outdated modes of thinking in this view. The conclusion to be drawn from these putative IT developments has been called 'the no-work solution'[13] – in other words, 'income should be separated from work; individuals, including those capable of working, should be enabled to live at leisure while drawing an "unconditional basic income" set "at the highest sustainable level"' (Gewirth, 1996, 229). If we call 'loafing' the opposite of

working, then the ethical problem with the 'no-work solution' is that potential 'loafers,' living as parasites off the work of others without contributing anything, would violate the moral requirement of *mutuality* at the heart of a proper view of human rights and responsibilities. Basic income policy entails a legal right to receive at least subsistence. If a 'loafer' has a positive right to subsistence, however, then other individuals have a positive duty to provide the subsistence by working, including any loafers who are in a position to fulfil the subsistence needs of other individuals. The exemption from working proposed by the 'no-work solution' is contradictory, since 'loafers' are not exempt from the generalization to which they are logically committed in claiming their own right to receive subsistence.

Instead of a 'no-work solution' based on the erroneous assumption that IT will render work unnecessary, a more realistic and feasible response would be to reduce the hours of work and aim for a full-employment policy. We do not imply that Rifkin's pragmatic proposals for work in the voluntary sector perfectly fit the 'no-work solution.' His suggestion that government tax credits be issued for voluntary work with not-for-profit organizations is a creative proposal. A full-employment policy could provide private and public sector retraining of workers and shortened work weeks. In addition, one can envision tax credits to employers who hire previously jobless workers, as well as direct public sector employment for all those able and willing to work on various publicly funded projects. What is also needed is a cultural shift that embraces a view of work based on productive human agency. What we have in mind is not 'workfare,' which points in the right direction but incurs factual and moral problems, but what Gewirth calls 'productivist welfarism,' which focuses on distributing and fostering personal productive abilities and responsibility. Most theories of distributive justice involve dependence and passive welfarism, where individuals are dependent recipients of money or economic goods produced by others. In contrast, productivist welfarism revolves not so much on distributing products, but rather on helping individuals to develop their own capacities for producing goods or commodities, including their own effective sense of personal responsibility, so that they can dispense with help from others to secure their basic well-being. In this way, the right to productive agency is in keeping both with the spirit of Rifkin's concerns, as well as with the United Nations Development Program's notion of human development. Fulfilling the right to productive agency is crucial, given the growing

importance of information and knowledge skills for human development in the informational economy.

The Informational Economy and the Community of Rights

It has been suggested that the keys to unlocking the genetic code for long-term, functioning, sustainable democratic national institutions and international development are an 'elusive mystery' (Conley and Livermore, 1996). This may well be true, but ideas of mutuality, social solidarity, and trust associated with national and global community are important values worthy of support. Can these values realistically be attributed to relationships and institutions that can, and do already, exist in the new informational economy? The society of human rights justified by the Principle of Generic Consistency may serve as a guide for social and economic institutions that seek to instantiate these values in policy. The PGC's society of human rights can be a genuine community of rights, because it provides for equal and mutual assistance to secure human rights by equally protecting and promoting the freedom and well-being of all its members. This is a matter of institutional arrangements focused in national and international legally enforced policies that serve to secure legal rights and enforce international standards of privacy and security. Such arrangements mark a departure from individualistic views of human rights because of the positive obligations they require through taxation and other means that commit individuals to further the agency-related needs and interests of others besides themselves, especially those most deprived of basic goods. At the same time, the community of rights, through its indispensable contributions to members' education, health, safety, and various other social and economic goods that comprise the necessary conditions of action, helps individuals to attain personal responsibility. The informational community of rights represents an institutional harmony among its members insofar as they mutually share in the benefits of technology productivity gains. The harmony is also psychological insofar as the members are aware of the rightness of the arrangements as deriving from the rationally justified principle of human rights. Institutional efforts to remove poverty, work towards full employment, and harness ICTs for productive agency would not only go far in avoiding the risk of 'barbarism,' but would also help to close the gap between the information haves and have-nots.

CHAPTER FOUR

Privacy and Security Policy: The Historical Situation

Privacy and security issues posed the second major concern for Canadian information highway policy and e-commerce strategy, and they continue to pose vexing ethical challenges in our present situation. Privacy and security policy concerns turn back on basic ethical and empirical questions, even as our new situation for privacy protection is shaped by technological, economic, and political domains (Bennett and Grant, 1999). Most individuals care something about their personal privacy, but where they differ greatly is in the extent to which they are prepared 'to grant privacy priority over other human rights, values, and interests when a competitive environment exists' (Flaherty, 1999, 28). In this chapter we treat privacy and security policy developments at the international level before turning to the Canadian situation and, especially, recent concerns with private sector information protection and cryptography policy. The historical situation of past and present policy approaches also is established, while in chapter 5 an argument is made for privacy as a human right and social value whose ethical justification is best grounded in human freedom and well-being as the generic rights and necessary conditions of human action. The concrete specification of privacy and security policy norms are best derived from the generic rights to freedom and well-being and the principle of human rights, as we shall discover in the next chapter.

The Global Situation

The right to privacy is integrally linked to the development of international human rights legislation after the Second World War, the atrocities of the Hitler regime, as well as the inception of the United

Nations' Universal Declaration of Human Rights (UDHR) in 1948. In article 12 of the UDHR it is explicitly stated that 'No one shall be subjected to arbitrary interference with his privacy, family home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks' (cited in Walters, 1995a, 411). The rise of the informational economy during the past two decades has made international standards for personal data protection imperative. International businesses use data on customers, employees, suppliers, investors, and competitors that make it increasingly difficult for national solutions alone to provide privacy protection for citizens. The debate over transborder data flows began in the late 1970s and subsequently inspired two important international instruments, the Council of Europe's 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the 1981 OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. The former evolved through several drafts to become The EU *Directive on Data Protection*.

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD)

In 1984 Canada joined twenty-three other industrialized countries in adhering to the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. The guidelines are intended to protect personal information and to ensure the free flow of data between countries. The guidelines have been regarded as a code of fair information practices for the collection, use, disclosure, retention, and disposal of personal information. Sets of fair information practices vary, but they generally include principles such as collection limitation, quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability (Cleaver et al., 1992). In the OECD guidelines no distinction is made, however, between government and private institutions, but the majority of OECD countries today have enacted data protection legislation that extends to both the public and the private sectors. Canadian laws, with the exception of Quebec's Act Respecting the Protection of Personal Information in the Private Sector, have recently applied only to the actions of governments and government agencies. Although both federal and provincial data protection laws adopt the OECD principles for the collection, use, disclosure of, and access to information about an identifiable individual,

Canada's enforcement mechanisms and legislative scope are somewhat different than other countries. The United Kingdom uses a registration regime, while Germany has a data protection commissioner, and Japan does not yet have in place any private sector legislation. Canada uses its privacy commissioner as the principal mechanism for safeguarding personal information. As such, moral suasion or public embarrassment have been traditionally used to ensure compliance, rather than legislative provisions with real penal bite in a fashion not unlike international human rights regimes that have often acted as shaming mechanisms to enforce compliance with human rights standards.

The Council of Europe's Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (known as Convention 108) was opened for signature on 28 January 1981. The convention was designed to maintain a '*just balance* between the different rights and interests of individuals,' and in particular between 'the freedom to process information on the one hand and rights of privacy on the other' (Council of Europe, 1981; emphasis added). The 1981 convention was arguably as important as the OECD guidelines in supporting international privacy law harmonization. The convention's primary concern is with data protection, but it also attempts to reconcile privacy rights to data protection with the right to the free exchange of global data flow. The Council of Europe convention seeks to restrict the free flow of information across borders 'only to the extent strictly justified for the protection of other individual rights and freedoms, in particular the right to respect for individual privacy' (Council of Europe, 1981, 10–11). The common core of minimum data protection principles established by the Convention made it possible for signatories to agree to relinquish possible restrictions on data flow across borders. As one commentator notes, this possibility removed 'the threat posed to the free-flow principle by any kind of trade protectionism masquerading as a special concern for privacy' (Raab, 1999, 70).

In 1986 the federal government attempted to comply with the OECD guidelines by encouraging private sector companies to develop and implement voluntary privacy protection codes. At that time, the Canadian Bankers Association, the Canadian Life and Health Insurance Association, the Insurance Bureau of Canada, the Canadian Cable Television Standards Council, and the Canadian Direct Marketing Association implemented self-regulating, sectoral codes that provide guidance on how legal requirements are applicable to a given industry. Sectoral codes can instantiate ethical goods and values because they allow spe-

cific industries to explore their needs for information and make a commitment to privacy rights and norms by setting an example with their own practices. Compliance with and leadership in relation to sectoral codes build consumer trust and offer protection. Industries benefit because sectoral codes help to promote a workplace and industry ethos for good information management. Some of the early sectoral codes facilitated audits by providing a manual of information practices and, in turn, led to provincial privacy legislation in relation to consumer credit.

The Canadian Bankers Association (CBA) was a leader in the development of a voluntary approach to the protection of personal information. During the period 1995–96, the CBA brought its sectoral code into line with the Canadian Standards Association (CSA) Code. The Standards Council of Canada adopted the CSA code as a national standard in 1996. Not only does the CSA code manifest Canadian innovation of legislating both privacy and fair information practices in the same statute, but Canada was the first country in the world to adopt such a standard. As noted in Industry Canada's Task Force on Electronic Commerce, the CSA code 'demonstrates the continued commitment of participating parties to fair information practices, while providing an instrument that promises to be consumer-friendly, fair, effective and cost-efficient' (IC, 1998b, 9). The cooperation and patience among public sector industries such as transportation, telecommunications, information technology, insurance, health, and banking, as well as among consumer advocacy groups, unions, and other general-interest groups, makes the CSA code a truly remarkable achievement and one that Canadians ought to be proud of.

Many privacy scholars and activists maintain that the voluntary model is inadequate because privacy codes operate within a complicated and fluctuating set of political, organizational, cultural, technological, and economic incentives that vary between and within business sectors. Colin Bennett, who has spent many years studying the comparative analysis of privacy policies, correctly notes that the entirely 'voluntary approach always suffers from the perception that the individual's privacy rights are in the hands of those who have the most to gain from the processing of personal data' (1996, 481–2).

The European Union Directive on Data Protection

Going beyond the Council of Europe Convention and the OECD guidelines, the European Union required that member countries adopt

or adapt national data protection laws by 24 October 1998 in order to comply with the EU's Directive on Data Protection. The directive was adopted by the European Parliament and the Council of Ministers of the European Union on 24 October 1995 (EU, 1995). The provisions of the directive are similar to those of the Council of Europe Convention of 1981. Countries that were signatories of the convention already had a regulatory framework in place for data privacy. Within the EU, not only are the Member States implementing the directive differently, but the data registrar in each Member State will also implement any legislation according to his or her interpretation. The directive in itself is not law, but rather it sets out the minimum requirements for compliance by the national legislation of Member States. The key principles of the directive's legislation include the following.

Purpose limitation: Data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer.

Data quality: Data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant, and not excessive in relation to the purposes for which they are transferred or further processed.

Transparency: Individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country and other information insofar as it is necessary to ensure fairness.

Security: Technical and organizational security measures should be taken by the data controller that are appropriate to the risks presented by processing.

Rights of access: The data subject should have a right to obtain a copy of all the data relating to him or her that are processed and a right to the rectification of the data where they are shown to be inaccurate.

Restrictions on transfer: Further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient is also subject to the rules affording an adequate level of protection.

The restriction on transfer is one of the main differences between the EU Directive and the 1981 Council of Europe Convention. For the majority of the Member States, this is the first time that protection becomes available for paper-based as well as electronic data. Article 25, dealing with the transfer of data to third countries, prohibits member countries and businesses within those countries from transferring personal information to non-member countries like Canada if the country's laws do not adequately guarantee protection. Cross-border exchange of personal information, particularly between the United States and Europe, has posed difficult questions about the meaning and scope of the EU Directive. What must be understood by the 'adequate protection' required of non-European jurisdictions to be able to receive or transmit personal data from or to the EU's member countries? Will companies based in the United States, Latin America, Asia, China, the South Pacific, and Canada be able to satisfy the adequate protection criterion through contractual agreements with their European counterparts?

Other substantive issues have concerned access and enforcement. The directive requires that companies offer individuals access to information collected about them and recommends specific penalties if the procedures are not rigorously followed. Regulations providing access to data raise the delicate question of confidentiality. Do corporations have a right to keep their own data private? Compliance with the EU Directive will have a direct impact upon journalists, personnel managers, investment bankers, human resource managers, and auditors.

To assuage these concerns, the United States Department of Commerce and the European Commission proposed a 'Safe Harbor' plan to bring U.S. companies up to a minimum level of compliance with the EU Directive, and to ensure that data flows to the United States are not interrupted. On 27 July 2000 the European Commission issued its decision that the Safe Harbor Principles provide 'adequate protection' in accordance with article 25.6 of the EU Directive (EC, 2000). The main benefit of the Safe Harbor framework is that it provides predictability and continuity for U.S. and EU companies that send and receive personal information from Europe, and it is a simpler and cheaper means of complying with the adequacy requirements of the directive. U.S. organizations may voluntarily enter the Safe Harbor by annual self-certification to the Department of Commerce and note its published privacy policy statement that the organization adheres to the requirements. An EU organization may then ensure that it is sending informa-

tion to participating Safe Harbor U.S. organizations by consulting the Department of Commerce's public list of such organizations on its Web site.

Participating organizations must comply with the seven Safe Harbor principles, which include (1) a 'notice' stating the purpose for which the company collects and uses data. (2) 'Choice' or the option to choose whether or how their personal information will be disclosed to a third party; this principle stipulates an 'opt-out' policy, and, in the case of 'sensitive' information, an 'opt-in' policy. (3) 'Onward transfer' or transfers to third parties that are consistent with the principles of notice and choice. (4) 'Access' to data with the ability to correct, amend, or delete any personal information. (5) 'Security' measures taken by organizations creating, maintaining, using or disseminating personal data. (6) 'Data integrity' relevant to the purposes for which it is to be used. (7) 'Enforcement' and recourse mechanism for ensuring compliance; enforcement of the Safe Harbor will take place in accordance with U.S. law and carried out by the private sector and, where necessary, by government enforcement of federal and state unfair and deceptive statutes, thereby giving a participating organization's commitment to the Safe Harbor the force of law.

All along, Europeans have been very serious about U.S. compliance with the EU directive and Safe Harbor principles. For if the negotiations had failed, the European Commission could have decided to declare the United States off limits for European data. Such a ruling would seriously affect U.S.-based e-commerce companies and other data-rich sectors like the airline industry. By 1999 numerous European countries had formally adopted national laws to comply with the EU Directive, and many others had passed similar laws.

Privacy advocates in Canada have cheered the EU Directive, while many European and U.S. business firms have expressed misgivings. Contrary to initial expectations, the United States has not established a data protection or privacy commission or strengthened its privacy legislation. Instead, U.S. businesses have fiercely lobbied abroad to preserve their business interests. Their argument against the directive is based on the view that its requirements increase business costs and hamper global economic development: '[There are] *practical problems* with the directive, especially in the areas of banking, air travel, insurance, and direct marketing; *ambiguities in the directive*, which made it difficult to achieve the uniformity sought by the directive; *the business expense* associated with complying, which might lead some companies

to forsake critical business activities involving the use of personal data; and, perhaps most importantly, *the restrictions on the export of personal data*, which were viewed as a step backward in terms of globalization of business activity. More specifically, American companies were troubled by the requirements of "informed consent" and "adequate" or "equivalent" protection' (Regan, 1999, 210; emphasis in original).

The debated issue surrounding informed consent concerns the so-called opt-in or opt-out policy. Early drafts required that information collected for one purpose not be used for another purpose without informed consent, and individuals were required to 'opt in' to any new uses of their personal information. Many businesses prefer a more passive, opt-out requirement, whereby individuals are informed about secondary uses and then given the opportunity to object or opt out of having their personal information reused or exchanged. The European Direct Marketing Association (EDMA) spent over $50 million lobbying against the opt-in requirement of an early data protection draft. This led, in turn, to the establishment in 1992 of the European Federation of Direct Marketing (EFDIM), composed of seven national direct-marketing associations and the EDMA.

Businesses view the directive as requiring them to adopt a more active role in securing informed consent from customers. In a world where transactions and manipulations take place routinely and immediately, in their view it is both unrealistic and onerous to get permission from everyone in a database before financial or credit transactions can be processed. Thus, for British Airways, the American credit card industry (Equifax and Trans Union Credit), the U.S. International Trade Commission (ITC), the U.S. Council for International Business, and other information-intensive industries the 'adequate protection' clause caused anxiety. Political parties, and even seventy charities – which formed Charities and Non-profit Groups in Europe (CHANGE) – opposed the directive, fearing that it would reduce their mailing lists and hurt fund raising. In the final version of the directive, article 7 requires, with some exceptions, that member states shall provide that personal data may be processed only if 'the data subject has unambiguously given his consent.' In short, most businesses favour market-based and technological solutions and standards combined with voluntary self-regulation, rather than legal regulation, and many have adopted 'Codes of Fair Information Use.' It is unlikely that these codes will be evaluated in a critical way, because voluntary contractual arrangements do not have the force of law and are not entered into by

two sovereign nations. As a result, some European Commission members find such arrangements politically unacceptable, and privacy advocates and data protection commissioners will continue to seek legal redress in order to hold businesses accountable.

The Canadian Situation

Canadian privacy policy has a long history. After the Second World War provincial and territorial legislatures led the way in enacting human rights laws prohibiting discrimination by landlords and employers on grounds such as race, national origin, colour, religion, sex, and age. In 1960 basic rights and freedoms were introduced by Prime Minister John Diefenbaker in the Canadian Bill of Rights, but the bill was extremely limited because provincial governments failed to participate in its enactment (Bayefsky and Eberts, 1985). In 1977, the same year that the Office of the Privacy Commissioner was initially established, the federal government introduced the Canadian Human Rights Act, designed to prohibit discriminatory practices under federal jurisdiction. In 1978 the Canadian Human Rights Commission was created to administer and enforce it. Ten prohibited grounds of discrimination are named under the Act: Race, National or Ethnic Origin, Colour, Religion, Age, Sex (including pregnancy and childbirth), Marital Status, Family Status, Physical or Mental Disability (including dependence on alcohol or drugs), and Pardoned Conviction. Despite various provincial codes, there was nothing at the time to prevent the federal legislature from enacting discriminatory laws or violating fundamental rights and freedoms.

The Canadian Charter of Rights and Freedoms

In order to remedy this situation the Canadian Charter of Rights and Freedoms was entrenched as part of the constitution in the so-called Constitution Act, 1982. The act was passed as a resolution by the Canadian Parliament in December 1981 and is referred to as the Constitution Act, 1981. It was later passed by the British Parliament and became the Constitution Act, 1982. All Canadian jurisdictions except Quebec, which did not participate in the enactment of the constitution, in turn amended provincial laws to bring them into line with the charter. The introduction of the charter has not diminished the importance of provincial codes which still regulate private individuals, companies,

and government bodies, but it has clearly expanded the role of the courts. Because charter rights are not expressed clearly and distinctly, the courts have been left to determine their meaning. Canada has no explicit constitutional right to privacy, even though there have been numerous attempts to entrench the right to privacy in the constitution. In 1981 member of Parliament David Crombie proposed the inclusion of a constitutional right of privacy in the charter, but his amendment was defeated (HC, 1987, 91).

The courts have interpreted charter sections 7 and 8 as guarding against unreasonable privacy invasions. In section 7 it is stated that 'everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice.' Section 8, which is similar to the U.S. Fourth Amendment, states that 'everyone has the right to be secure against unreasonable search or seizure.' Privacy issues have also been recognized with respect to section 10, which provides that 'everyone has the right on arrest or detention (a) to be informed promptly of the reason therefore; (b) to retain and instruct counsel without delay and to be informed of that right; and (c) to have the validity of the detention determined by way of habeas corpus and to be released if the detention is not lawful.' Derived from the common-law presumption of 'innocent until proven guilty,' this section, especially (b) concerning the right to retain and instruct counsel, protects persons from disclosing information that could serve to incriminate them. The courts have extended the section so that the right to retain and instruct counsel may be exercised in private between an individual and his or her lawyer without being overheard. Thus, it is not acceptable for a police officer to take notes about a telephone conversation he or she overheard (*R. v. Donegani* (1983), 8 C.C.R. 24 (B.C.S.C.). The right to be tried within a reasonable time period, covered in section 11(b), has also been recognized as a relevant privacy issue. Privacy may emerge as an issue regarding the fundamental freedoms set forth in section 2, especially freedom of conscience and religion and freedom of thought, belief, opinion, and expression, including freedom of the press and other media of communication (Flaherty, 1991).

Charter rights and freedoms are not absolute. They must be qualified in order to protect the rights and freedoms of others. Isaiah Berlin remarks that 'in a lake stocked with minnows and minnow-eating pike, freedom for the pike means death to the minnows' (cited by Sopinka, 1994). The paradox of freedom is at play here. A's freedom to do X

entails the unfreedom of other persons to interfere with A's doing X. So freedom involves a certain amount of unfreedom. Section 1 of the charter guarantees rights and freedoms only to such 'reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.' More important, the charter applies only to the laws and activities of governments; it does not apply directly to the private sector.

Quebec's Constitutional Privacy Protection

Quebec is the only Canadian province that gives some explicit constitutional privacy protection. Article 5 of the 1975 Quebec Charter of Human Rights and Freedoms guarantees that 'every person has a right to respect for his private life. In 1987 Quebec amended its Civil Code to respect individual privacy, specifying that 'every person has a right to the respect of his reputation and privacy. No one may invade the privacy of another person except with the consent of the person or his heirs or unless it is permitted by law' (cited in Flaherty, 1991, 844). Since 1982 Quebec's Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information grants individuals a right of access to personal and non-personal information held by the local, municipal, provincial, and regional governments. This act also regulates the confidentiality, collection, correction, disclosure, retention, and use of personal information. Records are requested directly from the institution that has custody of the information. Since 1994 the Act Respecting the Protection of Personal Information in the Private Sector grants individuals a right of access to personal information held by private sector businesses operating in the province. The act regulates the confidentiality, collection, correction, disclosure, retention and use of these businesses' personal information holdings. Records are requested directly from the business which has custody of the information. The 1994 version of the Civil Code grants all Quebec residents similar rights, as well as civil protection against violations of their informational, territorial, and personal privacy.

The Quebec model has offered relief to individuals, but it falls short of curtailing the development of generalized surveillance in the private sector (Laperrière, 1999). Data subjects can easily slip through the law's loopholes, because the law protects personal information in varying degrees, depending upon whether or not the information is in the hands of a public body, a private enterprise, or an individual. The Quebec law does allow free exchange of data between public and private investiga-

tors, debt collectors, and marketers with a weak opt-out procedure. Personal data can be collected or exchanged for 'verification' purposes, without quality control and without a set time limit for destruction. Businesses have no legal obligation to identify themselves when collecting data, to inform data subjects of their rights, or to appoint a person in charge of implementation and complaints. As long as a firm can show 'legitimate' purposes – which are not defined – it can accumulate and exchange data on individuals with few limitations. Moreover, the responsibilities given to the Commission d'accès à l'information (CAI) – the regime responsible for monitoring and administering requests for access, correction, and compliance – have not been adequately funded. Audit investigation and on-site visits and surveys have suffered. The Quebec statute fails to institutionalize the participation of interested parties, such as industry, consumers, and governments responsible for determining the specification of privacy norms within their respective sectors, though the courts have readily recognized the privacy rights of corporations. We need new privacy laws that determine for each sector what data banks should be set up, what types of information ought to be subject to collection, and what rules of disclosure and norms of security should apply. Systems designs would require, from the outset, mandatory privacy-enhancing devices.

The Federal Privacy Act and Access to Information Act

The federal government enacted the Privacy Act in 1982 in order to extend the laws of Canada that protect privacy of individuals 'with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information' (PCC, 1991, 1). The act took effect on 1 July 1983 and replaced some limited personal information rights set out in part IV of the Canadian Human Rights Act. The act regulates the collection, use, disclosure, and disposal of 'personal information'[1] held by the government. The act does not address privacy in its broadest sense, nor does it apply to the federally regulated private sector, for example, telecommunications companies interconnected to public networks, broadcasters and cable companies, banks, insurance and trust companies, and interprovincial carriers such as trains, airlines, and pipeline companies. It sets out numerous principles of fair information practices and requires some 150 federal government institutions to collect only the personal information they need to operate programs directly from the

person concerned, if possible. Governments are required to tell persons how information will be used and then use it only for the purpose for which it was collected, or for a 'consistent' purpose. Information may be disclosed only as the act permits, and governments must take all 'reasonable steps' to ensure accuracy and completeness of the information. Persons have a right to access their personal information, to question the accuracy of the personal information on file, to request changes to their files, and to notify other users of the information in the objections (PCC, 1992).

Canada acknowledges the complementary nature of the concept of privacy and access to information by virtue of the fact that the federal Access to Information Act was enforced at the same time as the Privacy Act. This is why section 12 of the Privacy Act provides Canadian citizens and permanent residents a right of access to '(a) any personal information about the individual contained in a personal information bank; and (b) any other personal information about the individual under the control of a government institution with respect to which the individual is able to provide sufficiently specific information on the location of the information as to render it reasonably retrievable by the government institution' (PCC, 1991, 10). Information of a personal nature held in government data banks is treated as private, whereas information of a non-personal nature held by a public body is accessible. Yet the Privacy Act is something of a misnomer in that it actually deals only with *data protection*. Data protection is concerned with controlling the collection, use, and dissemination of personal information. All legislatures in Europe and North America have enacted protective laws that seek to control government activity by means of fair information practices. General claims for individual privacy protection or 'informational privacy' have been on the rise in relation to abortion, AIDS, drug testing, workplace surveillance, electronic surveillance of public washrooms, employment privacy rights, medical privacy, genetic privacy, privacy and the press, communications privacy, library records, caller identification telephone systems, sexual privacy, and residential privacy. With respect to health information, the act defines 'personal information' as relating to the education, medical, criminal or employment history of the individual. Under the statutes of the act, the head of a 'government institution' may refuse to disclose any personal information (as requested under subsection 12-1) that relates to 'the physical or mental health' of an individual who requests it in cases where such disclosure would be contrary to the individual's best interests.

The main problem with the Privacy Act is that it has no teeth. If anyone violates the act's data protection provisions, even if the violations are wilful or intended to prejudice the individual or individuals involved, there are absolutely no penalties contained within the body of the act. Private sector protection of personal information is entirely lacking, and for this reason policy makers early on understood the need to move Canada from its de facto voluntary approach to a legislative approach.

The Canadian Standards Association, Model Code for the Protection of Personal Information

Privacy experts agree that the CSA code is a great improvement over the OECD guidelines. Published in March 1996, the CSA code has four main goals: (1) to provide principles for the management of personal information; (2) to specify the minimum requirements for the adequate protection of personal information held by participating organizations; (3) to make the Canadian public aware of how personal information should be protected; and (4) to provide standards by which the international community can measure the protection of personal information in Canada (CSA, 1996). The code represents a consensus among key stakeholders from the private sector, consumer and other public interest organizations, as well as some government bodies, regarding the minimum requirements for the protection of personal information. It combines normativeness with flexibility, since it was designed to serve as a model for more specific industry codes. Industry maintains that the code is 'technologically neutral' because its principles go beyond specific industry applications and will not become outdated as technologies for the collection and storage of information change. This claim may be misleading, since any standard is shaped by historical and cultural conditions, so the real question is whether or not it is adequate to the ethical and policy needs of our present historical situation. Most privacy experts think that it is. For the code to become legislation, it required greater precision about when and how personal information may be collected, for what reasons, how long an organization may keep such information, what consent must be obtained for its collection and in what form, what fees can be charged for copies of records, what exceptional circumstances would apply, additional obligations, and whether some types of information ought to be excluded from the scope of the legislation. All these concerns have shaped Bill C-6. The

code embodies ten fair information principles that go beyond the OECD guidelines:

1. **Accountability:** An organization is responsible for personal information under its control, and shall designate an individual or individuals who are accountable for the organization's compliance with the Code's principles.
2. **Identifying Purposes:** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
3. **Consent:** The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.
4. **Limiting Collection:** The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. **Limiting Use, Disclosure and Retention:** Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as is necessary for the fulfilment of those purposes.
6. **Accuracy:** Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.
7. **Safeguards:** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
8. **Openness:** An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
9. **Individual Access:** Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information, and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. **Challenging Compliance:** An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance. (CSA, 1996, x)

Industry and Justice have been prescient in asking key questions

about the CSA code. First, can a voluntary instrument like the code be precise enough in setting out legal obligations, or would it require further elaboration? Privacy experts would note that when an organization becomes a signatory to the code and receives accreditation, then the CSA provisions become *mandatory,* rather than merely voluntary. This practice is one of the most important differences between the CSA code and other 'codes' of practice. Nonetheless, law will still have to specify the exceptional circumstances under which personal information may be disclosed to a third party *without* the consent of the individual. Obviously, such disclosures do not always fall under the principle of 'identifying purposes' for collection as stated by the organization. There are surely some rational grounds for justifying disclosure such as the protection of the health and safety of one or more individuals, emergency situations where it is impossible to obtain the individual's consent, the conduct of imperative medical research, or the conduct of lawful investigations and compliance with a court order. The code recognizes that consent can be either 'implied' or 'express.' *Express consent* is consent that is explicitly given in oral or written form. Express consent is unequivocal and requires no interference on the part of associations, businesses, charitable organizations, clubs, government bodies, institutions, professional practices, and unions involved. The code's assumption is that an organization should generally seek express consent when the information is considered to be sensitive. *Implied consent* arises where consent may 'reasonably be inferred' from the action or inaction of the individual and appears appropriate when the information is not highly sensitive. What may be reasonably inferred is open to legal interpretation and, of course, begs the further philosophical question of what is both reasonably inferred and considered to be 'highly sensitive.' Article 4.3.4 states, in part, that in determining the form of consent to use, organizations should take into account the sensitivity of the information. Medical records and income records are almost always considered to be sensitive, whereas the names and addresses of subscribers to a news magazine generally would not be considered sensitive information. On the other hand, the names and addresses of subscribers to special-interest magazines might be considered sensitive.

Second, are there any additional obligations not set out in the CSA code that should be included in legislation? Such obligations could include a duty to report any complaints received to a government body or a requirement to educate members of the public

about their rights, or, indeed, new obligations unforeseen in the original code.

Third, should some types of information be excluded from the scope of the legislation? For example, the Quebec Act does not apply to journalistic material collected, held, used, or communicated for the purpose of informing the public.

Industry and Justice maintain that the obligations and approach of the CSA code could be incorporated in law by setting out the basic principles in a statute, with more precise details included in regulations or some other instrument like sectoral codes. Regardless of how the necessary details would be incorporated into law, organizations that use personal information would be required to meet the obligations of the statute.

The House of Commons Report: Privacy – Where Do We Draw the Line?

While policy makers were scrambling to incorporate the CSA code into a legislative framework, the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities published *Privacy – Where Do We Draw the Line?* in 1997. The committee asks fundamental questions about how far the government should go in trading off the benefits of new technologies for a sense of personal privacy (HC, 1997). Privacy is affirmed as a fundamental human right and assertion of personal freedom, but not an absolute right. Privacy must constantly 'balance' competing rights and interests, but where should the line be drawn? An ethical framework is called for, to ground privacy policy and to help in the task of balancing individual and societal protections: 'If we approach privacy issues from a human rights perspective, the principles and solutions we arrive at will be rights-affirming, people-based, humanitarian ones ... if we adopt a market-based or economic approach, the solutions will reflect a different philosophy, one that puts profit margins and efficiency before people, and may not first and foremost serve the common good' (HC, 1997, 33).

The use of the term 'common good' is ambiguous. The common good might be invoked morally to override the rights of individuals, for example, when individual privacy must be balanced against the need to permit the collection, use, and disclosure of personal information as part of a public health response to AIDS (PCC, 1989). Common good may have a 'collective' meaning in reference to the community as a whole, as distinct from its individual members. This view of the com-

mon good of community has been used as a utilitarian justification for infringing the rights or basic goods of a few, if it would lead to maximization of overall good. South African apartheid, forms of religious, nationalist, and ethnic intolerance provide examples of this collective conception of a common good. The term common good may also be interpreted 'distributively' where it refers to some good or goods equally common to, equally shared by, or distributed among, all the members of a community. To this apparent distributive intent we would add that privacy rights protect the generic rights to freedom and well-being that all persons share as persons who pursue purposive goals and ends of action.

In its report the committee sets forth an ethical 'blueprint' of core privacy principles, such as physical privacy, privacy of personal information, freedom from surveillance, privacy of personal communications, and privacy of personal space. The legal justification for exceptions would be the concrete proof that the invasion is in the 'public interest' or that it is a 'reasonable' violation of individual liberty. The benefits achieved ought to outweigh any harm caused by the infringement. The report's list of obligations includes the duty to secure meaningful consent, to take all steps necessary to adequately respect others' privacy rights, to be accountable, to be transparent, to use and provide access to privacy-enhancing technologies, and to build privacy protection features into technological designs. Among the report's merits is the fact that privacy is defined not merely as an individual right, but also as part of Canada's social or collective value system, and others are called on to submit its privacy principles to 'public scrutiny and comment.' The policy aim is to revise and refine the blueprint, entrenching rights in a new Canadian Charter of Privacy Rights.

Despite the virtues of the House of Commons report, it contains no substantive philosophical discussion of the meaning and nature of privacy as a *social value* and little substantive discussion of the *ethical justification* of privacy as a human right beyond a normative link with human dignity and autonomy. The committee merely asserts privacy as a human right and social value, but develops no conceptual ethical or philosophical understanding of privacy. In the next chapter, we suggest a way of thinking about privacy as a social value and human right, whose ethical justification resides in freedom and well-being as the necessary conditions of human action in accordance with the principle of human rights.

The Protection of Personal Information: Building Canada's Information Economy and Society

IHAC policy makers warned against the development of comprehensive profiles of individuals or companies that can be sold or integrated across borders, without the express consent of the individuals or groups from whom it is collected (IC, 1994a, 1994b, 1995b). In January 1998 the Task Force on Electronic Commerce of Industry Canada and Justice Canada published the discussion paper, *The Protection of Personal Information: Building Canada's Information Economy and Society* (IC, 1998b). The task force's concern with private sector privacy takes a far more decidedly *economic approach* than earlier IHAC policy formulations took. Consumer trust, market certainty, and comfortable, secure, and confident e-commerce demand clear and predictable rules for balancing business needs with the protection of personal information. A new law is needed that will strike the right 'balance' between the business need to gather, store, and use personal information, and the consumer need to be informed about how that information will be used and protected. Moreover, such legislation would provide Canada's global trading partners with the 'reassurance' needed to engage in cross-border transfers of personal information. Their search for a new law went from draft legislation in the form of Bill C-54, the Personal Information Protection and Electronic Documents Act, to Bill C-6.

Bill C-6: The Personal Information Protection and Electronic Documents Act

The negotiation of the CSA code, the work of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities, and the linking of privacy to the e-commerce agenda by the Task Force on Electronic Commerce of Industry Canada and Justice Canada (not to mention international compliance with the EU Directive) all have been instrumental in moving the patchwork of Canadian privacy protection from a public sector, data protection model to the private sector, legislative model. On 1 October 1998 the federal government introduced the Personal Information Protection and Electronic Documents Act (Bill C-54, now Bill C-6) in Parliament, and Bill C-6 became official legislation on 4 April 2000[2] and came into force on 1 January 2001.

Bill C-6 requires businesses to respect a code of fair information

practices mandating individual consent for the collection, use, and disclosure of personal information. Very early on, the bill was agreed to by a wide range of industry and consumer interest groups.[3] It provides for independent oversight by the Privacy Commissioner of Canada,[4] who is given statutory authority as ombudsman to investigate complaints, issue reports, and conduct audits. Only as a last resort does the bill provide recourse to the Federal Court of Canada and empower the court to grant remedies and award damages, such as ordering an organization to correct its practices to comply with the bill, ordering an organization to publish a notice of any action taken or proposed action to be taken to correct its practices, and awarding damages (not to exceed $20,000) to the complainant, including damages for any humiliation that the complainant has suffered.[5] The bill also contains a 'primacy clause,' meaning that the law takes precedence over subsequent acts of Parliament unless those acts specifically provide otherwise. In accordance with the concerns of the task force on e-commerce, the bill will help Canada to meet new data protection standards set by the European Union, since Quebec is the only North American jurisdiction with a private sector law that meets EU requirements.

The policy debates over C-6 reveal the difficult challenge of balancing commercial and individual rights and interests. Like American business opposition to the EU Directive, critics argue that few businesses abuse private data, and that any new law would make business compliance a nightmare (Owens, 1999). In this view, businesses have generally respected, and will continue to respect, their customers' privacy. Voluntary codes have met a 'reasonable' standard in the past, incorporating enforcement or mediation mechanisms as a viable alternative to legislation. Unlike the earlier CSA code,[6] the bill does not expressly incorporate the notion of 'implied consent.' Even if it did so, the bill follows the CSA code in interpreting 'sensitive information' as including specialized magazine subscription information. If 'sensitive information' were to include customer lists of many retailers, including financial information about those customers' purchases, then the law could negatively affect a business owner's ability to finance or sell the business. An even stronger argument, say the critics, is that law enforcement agencies should be able to access personal information without consent, just as insurance agencies need to collect personal information in order to control insurance fraud. Other critics suggest that the bill will harm health care delivery and the overall management of the Canadian health care system. Law enforcement, insurance

fraud, and health care concerns place reasonable limits on individual privacy in the name of public interest.

Supporters of the bill maintain that it is a reasonable law that actually promotes business in Canada, because it improves consumer confidence (Lawson, 1999). Consumer trust is vital for e-commerce, and by establishing clear rules for the treatment of personal information, the bill provides greater certainty for businesses. Supporters suggest, however, that voluntary codes are insufficient for the task of privacy protection, since they do not provide enough normative specificity and are rarely, if ever, backed up with effective enforcement mechanisms. Voluntary codes tend to cover only those who wish to be covered. As a consequence, profit-mongers intending to make a fast buck by abusing consumer privacy ultimately tarnish the reputation of good businesses. Because privacy is a human right, it must be legislated, not left to industry self-regulation. By putting personal data protection rules in place, the government is encouraging Canadian businesses to design privacy-friendly systems and practices early on so that they will not have to retool down the road. The bill also brings Canada more closely in line with other European countries, thereby enhancing international trade opportunities for Canadian businesses.

With respect to security, fraud prevention, and medical reasons that might make it impossible or impractical to seek consent, the bill acknowledges an exception to the principle of consent. The bill allows an organization to collect personal information *without the knowledge or consent* of the individual if it has 'reasonable grounds' to believe that it could be useful in the investigation of a contravention of the laws of Canada, if it is used for the purpose of 'acting in respect of an emergency that threatens the life, health or security of an individual,' or if it is used 'for statistical, or scholarly study or research purposes that cannot be achieved without it.' Even the supporters of the bill admit that this disclosure section does not give carte blanche to law enforcement officials to pry into the lives of law-abiding citizens, and that insurance companies ought to use the 'least intrusive' means available to control fraud. Lawson (1999, 3) writes that the onus is on the insurance companies 'to explain why they shouldn't have to obtain informed consent before collecting, using or disclosing the often very sensitive personal information of their customers.' Moreover, while endorsing the legislation, supporters also maintain that when it comes to the collection, use, and disclosure of personal health information, the bill is too weak. Public interest groups lobbied for a stronger bill that would allow the

privacy commissioner to conduct random audits of personal information management practices, provide for harsher penalties in the event of repeated violations where publicity has no effect, and provide special protections for personal health information.

With the passing of Bill C-6, there has been a necessary change in the way that privacy issues are dealt with in Canada. At the heart of the bill stand the basic principles of the CSA code. Private sector businesses should not be overly critical of the legislation, because they actually helped to create the standard and thus may rightly claim some ownership of the bill. The bill is not, therefore, some heavy-handed imposition on an unwilling business community of principles foreign to their thinking, but instead reflects a consensus of significant sectors of the business community. The privacy of medical information has not, alas, become a major public issue yet. Perhaps this is because most Canadians care much more about the closing of hospital beds, the waiting lists for surgery and chemotherapy, and the downloading of elder care to the private sector than they do about medical privacy. However, concerns over medical privacy and insurance discrimination are growing. It must be admitted also that the privacy movement has been up against a frightening economic argument about privacy implementation costs that is not likely to abate in the foreseeable future. We shall return to the issue of genetic and medical privacy in the next chapter, since it is one of the most crucial issues in the protection of the basic well-being and human rights of persons in the informational age. Suffice it to say here that under the legislation the health field has been given a one-year extension before the federal law becomes applicable to the health information industry.

Briefs presented to the parliamentary and Senate committees that studied Bill C-6 reveal the diversity of debate and viewpoints concerning what constitutes the proper approach to protect an individual's 'Personal Health Information' (PHI) (Senate of Canada, 1999). Federal and provincial governments have discussed plans to create an 'electronic health record' for every Canadian and the possibility of developing a 'National Health Infostructure.' Who would have access to and control of the information in our electronic health records? How will privacy and security issues be met? What role will or should Canadian citizens and physicians play in defining policy regarding PHI?

The ethical debate turns on the proper balance between the 'need to know' information and the 'need to protect' personal health information. It is clear from the policy debates surrounding Bill C-6 as well as

the Canadian Medical Association (CMA) Privacy Code (CMA, 1998) that a problem arises over the definition and interpretation of 'initial consent' and secondary uses of personal health information. Both Bill C-6 and the CMA Privacy Code contain well-defined guidelines regarding consent, collection, and protection safeguards. The 'need to know' guidelines that attempt to delineate the proper parameters of secondary use of personal health information, by contrast, are vague and do not define reasonable and practical means for getting consent and access for secondary uses of PHI.

Winston Dykeman (2000), co-chair of the Committee on Privacy, Confidentiality, and Security of Personal Health Information (College of Family Physicians of Canada), rightly argues that we ought to separate the 'need to know' and the 'need to protect' agendas and define and develop legislative principles for secondary use in each context. Whereas primary uses of PHI currently are gathered under the principles of primary consent for primary care and are well developed under the 'need to protect' agenda, this is not the case for the 'need to know' agenda. Secondary uses of PHI should be gathered under principles of secondary consent for secondary applications such as health information research, quality assurance, and public health policy development. It is currently impossible to achieve a health balance between the 'need to know' and the 'need to protect,' given the fact that our eleven provinces, two territories, and one federal government, each with private and public sector components, represent twenty-eight possible privacy codes and acts for Canada!

What is needed, therefore, is one National Personal Health Information Research Act (NPHIRA), which will define a uniform set of principles and guidelines for the federal, provincial, territorial governments and the private sector. Without such an act, privacy infringements will inevitably result in a piecemeal and fragmented approach, and a case-by-case procedure in the courts (Dykeman, 1999). Legislation must include clear, consistent, and uniform definitions and principles across governmental jusridictional boundaries and the private sector, including the following:

(i) Definitions of Secondary Consent and how to obtain and monitor it for legitimate secondary uses. Definitions of limits of access of any kind for some types of sensitive PHI.
(ii) What kinds of PHI may be accessed for secondary use; its sources and how it may be obtained. Genome Data Protection.

(iii) Clear definitions of anonymity for PHI including archived data and time frames to access.
(iv) Definitions of access for the Private Sector and how this relates to public databases of PHI such as medicare, hospital, laboratory, and pharmacy databases. Definitions of limits of access to some types of PHI.
(v) Who will access PHI? What will it be used for? How will it be used?
(vi) Definitions of Accountability, Responsibility and Liability.
(vii) Monitoring and policing: Privacy Commissioner, Ombudsman, Hospital and University Ethics Committees, RCMP Commercial Crime?
(viii) Definitions of what constitutes conflicts of interest; potential detrimental uses of PHI.
(ix) Definitions of global participation and how to obtain secondary consent: Specific mechanisms of getting secondary consent. (Dykeman, 2000)

Bill S-27: The Privacy Rights Charter

As a direct outcome of the House of Commons report, *Privacy – Where Do We Draw the Line?* as well as previous Canadian privacy policy developments, Senator Sheila Finestone, P.C., introduced Bill S-27 in the Senate on 15 June 2000 as an act to guarantee the human right to privacy. The bill received a second reading on 27 June 2000 and was referred to the Standing Senate Committee on Social Affairs, Science and Technology for consideration. The purpose of the bill is to provide Canadians with an overarching legislative framework that sets the ground rules for the protection of the right to privacy of all individuals, including physical privacy; freedom from surveillance; freedom from monitoring and interception of their private communications; and freedom from the collection, use, and disclosure of their personal information. Bill S-27 would permit privacy infringements that are 'reasonable' and 'demonstrably justified' in a free and democratic society.

A Cryptography Policy Framework for Electronic Commerce

In 1995 IHAC policy first identified the need for a technological and legal structure to assure the privacy and confidentiality of financial and other sensitive information stored in databases or transmitted over

public networks. Public consultations were set up to determine how best to 'balance' the legitimate use and flow of data, privacy, civil and human rights, and law enforcement and national security interests. What was needed was an information highway that would provide message integrity and authentication. Public scrutiny of encryption algorithms and standards, as well as freedom of choice in their use, were set as goals, along with the building of partnerships among federal, provincial, and territorial governments, the private sector, and other stakeholders in order to develop mutually acceptable security standards. The council called on the federal government for leadership in developing privacy and security through the creation of a uniform public key infrastructure to meet government needs (IC, 1995b). Subsequent policy developments have stressed the importance of e-commerce as the preferred means to conduct business both internally and with external clients (IC, 1998b). The work of these earlier policy phases led to the publication, in February 1998, of the Task Force on E-Commerce's cryptography policy framework (IC, 1998a).

Our present situation is paradoxical. While technology for managing and communicating on the Internet is increasing exponentially and is vital for human dignity and well-being, our borderless communication infrastructure grows increasingly less secure. Cryptography can protect personal information, support e-commerce, and promote public safety and national security, but it can also be used for immoral purposes. Cryptography permits the encryption/decryption of data so that it can be accessed and read only by someone with the appropriate mathematical key or keys. Digital signatures, which are analogous to written signatures, provide authentication, non-repudiation, and integrity of transactions for providing security and developing trust on open networks. *Authentication* provides proof that users or resources are who or what they claim to be. *Non-repudiation* proves that a transaction has occurred and thus cannot be denied by one of the parties. *Integrity* means that the data have not been altered or modified in an unauthorized manner (IC, 1998a, 4; OECD, 1997a).

The strongest form of encryption technology is public-key cryptography in which everyone has a private and a public key. If an individual wants to send an encrypted message or file, he or she encodes it with a private key and the intended recipient's public key. The message can then be opened only using the recipient's private key. Law enforcement and national security agencies are concerned that widespread use of strong encryption, without some capacity for lawful

access, will stymie security capabilities (IC, 1998a, 10). Many governments have sought to prevent widespread use of cryptography unless ubiquitous 'key recovery' or 'escrow' mechanisms can guarantee lawful and timely (real time) access. Key recovery would be used to provide lawful access to wiretapped encrypted telephone conversations. For public key cryptography to work well requires a 'certification authority' (CA) or trusted third-party agent to manage the distribution of public keys or certificates. The banks were some of the first institutions to establish their own CAs in order to provide Internet banking security and to implement Secure Electronic Transaction (SET) protocols for credit card transactions. Some businesses have chosen to outsource to cryptography service providers. Whatever the mode of cryptography-based security, the services raise a host of considerations for business and lawful access: the 'nature of the keys' employed (i.e., whether these are one-off session keys for data in transit that are discarded after use or long-term encapsulation keys); the question of 'who controls the cryptographic keys' at each phase of the keys' life cycle, from key generation through to key archiving or destruction (i.e., is it the data owner or a trusted agent other than the owner); and 'differences that arise whether one is dealing with the encryption of stored data or the encryption of real-time communications' (IC, 1998a, 17).

These challenges are still pressing in the present situation. In the largest known case of cybertheft, a hacker from eastern Europe stole information on more than 485,000 credit cards from an e-commerce site and then secretly stored the massive database on a U.S. government agency's Web site. Either the credit card data were stored by the Web site in plaintext and therefore were readable by anyone who gained access to the computer and the hacker simply copied the data, or the intruder managed to decrypt an encrypted database full of credit card numbers. Most experts think the e-commerce company (CD Universe) had not encrypted their user data, even though all credit card transactions use real-time encryption technologies (Brunker, 2000). Thus, the encryption of stored data is equally as important as encrypting real-time sensitive data transactions, though the latter practice is the general public's conception of what is entailed by encryption policy.

Government of Canada Public Key Infrastructure Policy

The linking of CAs with other cross-certified CAs is referred to as a 'public key infrastructure' (PKI). In 1998 the Government of Canada

(GOC) PKI came online to provide a basis for the use of digital signatures and secure internal and external electronic transactions. Numerous government departments and agencies are actively engaged in its ongoing development and use in securing data files and network communications for e-commerce applications, E-mail, data interchange, database access, and Web interactions. The GOC PKI interfaces with private sector and institutional PKIs that adhere to similar levels of privacy, integrity, and security standards to exchange sensitive information, provide confidentiality, access control, integrity, authentication, and non-repudiation services. The PKI manages the generation and distribution of public/private key pairs and publishes the public key along with the user's identification as a 'certificate' on open bulletin boards (CSE, 1998).

The requirements of key recovery systems entail a complex set of technology and policy challenges for accessing the 'plaintext' of 'ciphertext' information. Plaintext refers to intelligible data, whereas ciphertext refers to data in their enciphered form. The technical details of the cryptography debate are beyond the scope of this chapter and have been treated admirably by others (see, e.g., Diffie and Landau, 1998). Suffice it to say that the requirements of government key recovery and commercial encryption and key recovery appear to be incompatible. The differences are most acute in terms of the kinds of data and keys for which recovery is required, the manner in which recoverable keys are managed, and the relationship between key certification and key recovery. For example, very few commercial users need or want covert mechanisms to recover keys or plaintext data that they protect. They would only need to store backup keys in a bank safety deposit box. Business requires access for the sake of an audit or in order to safeguard against business fraud and error. Intelligence agencies want a fail-safe system for deciphering all encrypted messages regardless of its benefits to an end-user. Law enforcement agencies would need near real-time, twenty-four-hours-a-day, 365-days-a-year access to plaintext, but such a fast path limits the full range of safeguards that ameliorate risks inherent in commercial key recovery systems. Any access-time requirement carries risks, because some sort of network technology will be required to link a large number of law enforcement agencies with different key recovery centres. The securing of critical infrastructures, such as telephone networks, power grids, banking and financial networks, and air traffic control systems, is difficult, because they rely on open networks. The complexity and increased risk intro-

duced with key recovery could actually make these critical infrastructures protected by cryptography more vulnerable to hackers. The technological challenges of encryption are inherently related to problems of granularity and scale. 'Granularity' refers to the kinds of keys – for instance, user, device, session – that are recoverable. Granularity

> defines how narrowly-specified the data to be recovered from an agent can be and how often interactions (by the user and by law enforcement) with the recovery agent must take place. Various systems have been proposed in which the recovery agent produces 'master' keys that can decrypt all traffic to or from individual users or hardware devices. In other systems, only the keys for particular sessions are recovered. Coarse granularity (e.g., the master key of the targeted user) allows only limited control over what can be recovered (e.g., all data from a particular individual) but requires few interactions between law enforcement and the recovery center. Finer granularity (e.g., individual session keys), on the other hand, allows greater control (e.g., the key for a particular file or session, or only sessions that occurred within a particular time frame), but requires more frequent interaction with the recovery center (and increased design complexity) (Abelson et al., 1998)

In the coming years a ubiquitous key recovery system for law enforcement could encompass thousands of encryption products, thousands of agents needing intercountry certification, tens of thousands of law enforcement agencies, 100 million Internet users regularly encrypting communications, tens of millions or more public-private key pairs, and hundreds of billions of recoverable session keys! With such a large-scale system, how can agencies ensure that a mega-key recovery system will not inadvertently or maliciously leak data? 'Insider' abuse also poses a problem.

A major difficulty, then, is that by its very nature a key recovery infrastructure provides a new and vulnerable gateway to unauthorized data recovery. End-users lose complete control over the means to decrypt data. A worldwide key management infrastructure would effectively create new, high-value targets for criminals and other hackers. If they were to gain access to the caches of keys, they would be able to intercept business correspondence, forge digital signatures, and even engage in fraudulent e-commerce transactions. Moreover, it is impossible to tell the difference between an encrypted document and random text. Unless the law makes it illegal to transmit or store illegi-

ble text as such, which would violate freedom of expression rights, key-recovery would not work. International surveys demonstrate that strong encryption is already available and in use worldwide (GILC, 1998a). Most countries encourage a market-driven use, manufacture, sale, and distribution of encryption products. Both the OECD (1997a) and ministers of the European Union support the development and widespread use of strong cryptographic techniques. An ad hoc group of cryptographers and computer scientists concludes in a Report: 'Key recovery systems are inherently less secure, more costly, and more difficult to use than similar systems without a recovery feature. The massive deployment of key-recovery-based infrastructures to meet law enforcement's specifications will require significant sacrifices in security and convenience and substantially increased costs to all users of encryption. Furthermore, building the secure infrastructure of the breathtaking scale and complexity that would be required for such a scheme is beyond the experience and current competency of the field, and may well introduce ultimately unacceptable risks and costs' (Abelson et al., 1998).

Cryptography and Human Rights

Legislation that would prohibit the manufacture, import, and use of non-key recovery products; prohibit real-time communications that are not in plaintext or encrypted with key recovery software; and limit the export of strong cryptography raises a host of domestic and international human rights concerns (GILC, 1998b). The courts have interpreted sections 7 and 8 of the Canadian Charter as guarding against *unreasonable* privacy invasions. According to section 7, 'everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice.' Section 8 states that 'everyone has the right to be secure against unreasonable search or seizure.' Privacy issues have also been recognized with respect to section 10: 'Everyone has the right on arrest or detention (a) to be informed promptly of the reason therefore; (b) to retain and instruct counsel without delay and to be informed of that right; and (c) to have the validity of the detention determined by way of habeas corpus and to be released if the detention is not lawful.' Article 17(1) of the International Covenant on Civil and Political Rights (ICCPR) provides that 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor

to unlawful attacks on his honor and reputation.' Prohibitions against unreasonable search and seizure cover surveillance techniques such as wiretaps and interception of Internet communication. Article 19 provides, in pertinent part, that 'Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, *or through any other media* of his choice' (emphasis added).

Ciphertext speech expressed over the Internet is speech that deserves the full protection of constitutional and international law. Human rights guarantees are not, of course, absolute. Section 1 of the Charter guarantees rights and freedoms 'only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.' Under the ICCPR, the communication of encryption programs may be restricted only as 'necessary in a democratic society' for interests such as national security or public safety. How both the moral and the legal specification of the Charter's section 1 proportionality test will apply to Canadian cryptography policies and practices is unclear. Industry Canada notes that 'privacy rights *will likely* prohibit the state from decrypting data without some fairly compelling justification, and the right to freedom of expression *may* extend to both the production of cryptographic products and their use to protect the messages being expressed or data being stored' (IC, 1998a, 23; emphasis added).

It is at least arguable that the burden of proof for global key recovery rests on the shoulders of its advocates in the same fashion that the overriding of *jus ad bellum* norms rests on those who would initiate war. The onus is on key recovery advocates to make the case that its benefits outweigh the substantial technological, economic, and privacy rights costs and risks involved. Because strong encryption is already available worldwide, and the hardcore cartels and syndicates will surely use it, this fact throws into question the actual utility of a massive key recovery system, as well as export bans for law enforcement. The fact that criminal groups can afford to buy stronger encryption than can the Government of Canada (as we were informed by a member of the security and intelligence establishment) merely weakens the argument for domestic key recovery. The surveillance capabilities that global key recovery provides – even if it were economically and organizationally feasible – makes it a threat to millions of innocent, law-abiding citizens around the world.

Intelligence agencies worldwide have been sniffing e-mail and running 'anonymous remailers' designed to protect the privacy of e-mail for years (Dillon, 1996; Web Review, 1996). Anonymous remailers strip identifying source information from e-mail messages and allow persons to post e-mail messages without traceable return address information. Technology may be used maliciously by flamers, propagandists, and criminals, or benevolently to keep persons out of harm's way. Dinah Pokempner observes that 'principles of human rights and criminal justice are premised on the idea that it is better that the guilty sometimes go free if that is [what is] necessary to protect the rights of the innocent. When the incremental utility of key recovery is weighed against the threat to speech and privacy of individuals worldwide, it is not at all clear that the balance is in favor of law enforcement' (Pokempner, 1997).

Conclusion

Let us summarize key aspects of our privacy and security policy situation. The Canadian Charter guarantees related to privacy protection do not apply to the private sector. The 1982 Privacy Act regulated the collection, use, disclosure, and disposal of personal information held by the federal government, but there are no corresponding rules with respect to the private sector and its remedies have no teeth. The OECD guidelines make no distinction between the government and private institutions, and the conventional principles have offered no criteria for deciding whether or not a given means of data collection is ethically acceptable. The EU Directive has spurred Canadian e-commerce privacy policy and concern for the protection of cross-border exchanges of personal information. Until quite recently and until the passing of Bill C-6, there has existed a large gap with respect to private sector policy regulation where new technologies make it extremely easy to compile, store, manipulate, and trade personal data. Data warehousing and data mining have become common practices in the informational economy. At the same time, ever more citizens have come to value their right to privacy to control the use and exchange of personal information. We expect that our personal information will not be routinely collected, used, or disclosed without our knowledge of informed consent. Bill C-6 is an important legislative policy step forward.

New technologies will certainly provide benefits that improve the quality and well-being of our lives, but data collection and distribution

technologies have generally surpassed both legal and moral norms for protecting citizens against data misuse and privacy abuse. What will become of privacy for the poor, who enjoy less privacy rights than many others? To be poor is to be subject to a substantial degree of state surveillance and intrusiveness in order to obtain benefits. Social assistance recipients increasingly will be subjected to mass monitoring through numerous interlocked, relational databases. No doubt, these monitoring technologies and databases will be developed precisely as values to 'inhibit fraud' or 'facilitate one-stop service for consumers of government services' (Flaherty, 1999, 32).

Will voluntary codes be adequate for the new privacy landscape? Many business advocates maintain that voluntary codes should play a vital role in areas not covered by Bill C-6, citing the 1992 Canadian Code of Practice for Consumer Debit Card Services as an example for the practices of financial institutions. Ethical codes are effective, however, only if the individuals working within institutions are dedicated to acting upon ethical goods and values. Human character and virtue are significant goods, as is clear from the development of corporate codes of conduct and their impact on corporate social responsibility (Mendes, 1997b). In a dominant market system the value code that underlies people's normal decisions and actions often affirms that more money revenues are good and less money revenues are bad, despite the negative implications for the future of civil society.[7] With respect to ethical codes, then, we are forced back to profound questions about an ethics of being or character, not merely an ethics of doing or action. Health information 'mining' is a multi-billion-dollar industry in Canada, and one that will surely grow in the future. We do well to recall Albert Camus's insistence that we be neither victims nor executioners. The medical information gathered by Nazi doctors and their justification for direct medical killing were based on the concept of 'life unworthy of life' (*lebensunwertes Leben*) and proceeded from coercive sterilization to the killing of 'impaired' children in hospitals, to the killing of 'impaired' adults, mostly collected from mental hospitals, to 'impaired' inmates of concentration and extermination camps, and, ultimately, to mass killings, mostly of Jews in extermination camps (Lifton, 1986).

Data protection legislation in both the public and the private sector is a vitally necessary, yet insufficient, element in respecting the human right of privacy, and we shall argue why this is the case in the next chapter. We ought to be realistic about the possibilities of law, since law

is by nature ill adapted to rapid technological change. Law has been used as a means of 'social exclusion' that protects the haves from the have-nots; to use law as a tool fostering human rights against discrimination and abuse is therefore a real challenge. Just as economic growth may help to move social structures in more egalitarian directions, but normally does so only by the strenuous efforts of governments, organized groups, and workers, so, too, law on its own cannot succeed in fostering human rights unless the 'powers that be' succeed in establishing a 'secure society.' Law and legal rights alone, however, always run the risk of creating an 'exclusive society,' where law serves merely 'to protect the privacy of a happy few against the claims of all others' (Laperrière, 1999, 192).

The community of rights we advocate, therefore, goes beyond a notion of a legally 'secure society' because it is not based on individualistic views of human rights. The substantive and procedural requirements of the minimal state do not serve a principle of social exclusion. The community of rights is based, rather, upon a correlative theory of rights and responsibilities that commits individuals and businesses to further the agency-related needs and interests of others besides their own individual interests or the interests of their own organization. The mutuality operative in the community of rights would help individuals and businesses to attain personal responsibility and to work to counteract human greed. An informational community of rights would represent an institutional harmony among its members insofar as they mutually share in the benefits and burdens of technology productivity gains and commit to the procedural rules necessary to obtain a certain harmony between individual interests and the privacy and security interests of the public good. The harmony at the centre of an informational community of rights would have the psychological advantage that members are aware of the rightness of the arrangements as deriving from the rationally justified principle of human rights.

CHAPTER FIVE

Privacy and Security: An Ethical Analysis

It is clear from our survey of Canadian information highway policy and e-commerce strategy that there is no substantive philosophical justification of privacy as a human right beyond its prima facie link with human dignity and autonomy. On what philosophical ground, however, ought legislation seek to instantiate physical privacy, privacy of personal information, freedom from surveillance, privacy of personal communications, and privacy of personal space into public policy? The philosophical meaning of privacy as a social value also has been undeveloped in information policy documents. The government has called upon academics for 'open communication and dialogue' on how best to protect personal information in the private sector and how best to think about the ethical and policy implications of privacy, security, and new surveillance technologies. Fair-information principles appropriate for database forms of surveillance up to the last decade are necessary but insufficient for deciding whether a given means of data collection is ethically acceptable (Marx, 1999). In Bill C-6 an attempt is made to strike the right balance between the business need to gather, store, and use personal information and the consumer need to be informed about how that information will be used and protected. The cryptography policy framework for e-commerce seeks to balance the legitimate use and flow of digital data, with privacy and civil and human rights concerns and law enforcement and national security interests. Yet how may we best achieve ethical balance? What are the limits of legal rights for coping with radically new privacy and security challenges?

There are numerous popular (Cavoukian and Tapscott, 1995) and scholarly texts that outline the privacy and policy implications of new information technologies (Bennett, 1992; Burnham, 1983; Flaherty,

1989). Other scholars have placed privacy and surveillance issues in a broader sociological context (Castells, 1997; Lyon and Zureik, 1996) or provided conceptual frameworks for privacy policy and the technical design and development of information systems (Agre and Rotenberg, 1998). Scholars have also begun to explore how intelligence and law-enforcement organizations work, how they intercept communications, and how they use what they intercept in the information age (Diffie and Landau, 1998). Our concern, in contrast to these approaches, is with the *ethical justification and social value of privacy* that inevitably arises, regardless of the constantly changing technological landscape. The goal of this chapter is to draw an ethical line between negative and positive surveillance and security practices in accordance with the principle of human rights. We will first survey our contemporary technological situation and some well-established legal, social scientific, and philosophical conceptions of privacy. In turn, we set forth an ethical analysis of information highway and e-commerce privacy and security policy using the norms of basic, non-substractive, and additive well-being, the criterion for degrees of needfulness for action, and the principle of human rights. Our argument for grounding privacy in the necessary conditions of human action corroborates, but extends, a view of privacy as a human right and a social value. We offer a thicker theory of ethical justification, whose substantive derivation of norms bears directly upon the question of how best to strike an ethical balance between individual rights and societal interests. We will also take a close look at the limits and possibilities of privacy-enhancing technologies (PETs) before offering some normative ethical and policy conclusions.

Surveying Our Technological Situation

Smart cards are 'credit-card-sized personal computers' (Davies, 1992), which must be distinguished from embossed plastic cards, magnetic-stripe cards, and memory cards (Wright, 1993). Smart cards are moving into the mainstream of Canadian society, and the banks are taking on partners in the development of new e-cash payment systems like VISA Cash that allow consumers to purchase goods and services using prepaid electronic 'value' instead of cash (CESC, 1998). The United Kingdom uses numerous applications of smart cards, such as the Mondex Electronic Purse, the Shell Loyalty Card, and the Social Security Benefits Card. In Spain, smart cards have been introduced for benefit payments and access to government databases (Honeywood, 1997). They

will be central to public and private sector Canadian services in the future. When smart cards confer direct governmental entitlements, they will inevitably discriminate against non-cardholders, but such differentiation begs the question of who holds legal rights and why. It is certain that human freedom, well-being, and dignity will be tied to the new digital icons and the conditions of potential productive agency stored in their chips. Perhaps it is true that we must 'envisage a time when the lack of ownership of a multi-functional smart card will result in a dramatic loss of opportunity and of help in time of need for the "non-citizen"' (Rogerson, 1998, 2).

The technology challenges and privacy implications of smart cards are ambiguous. Computer scientists have discovered techniques to break smart card security by monitoring the card's power consumption and then breaking its internal codes. The head of security for Mondex International has admitted that the company had to completely rewrite its software to deal with the security threat (Wayner, 1998a). Banks want to use smart cards as a virtual branch office that dispenses money and credits accounts to the right persons. Hackers might be able to conduct fraudulent transactions, load counterfeit digital cash onto the cards, and create other forms of mischief. Smart card technology developments are something of an 'arms race,' where the attackers have the upper hand, according to the head of strategy and planning of Mastercard's Mondex smart card division: 'The only defense and the best defense against future attacks is to keep moving and keep changing.' The vice-president of marketing for Bull Smart Cards in the United States, a company that has shipped more than 120 million money-carrying smart cards throughout the world, admits that a smart card is never '100 percent immune' from security breaches (Wayner, 1998b; Monkhouse, 1997).

Smart cards may not be intrinsically detrimental to human rights if they merely provide single or multiple purpose benefits, operational efficiency, and great personal security. It must be admitted that they could also be used as a technology of surveillance and control if fair information principles and practices are ignored or overridden (Flaherty, 1999). They potentially change the individual-state relationship. Citizens need to know what will be stored on the card, who has the right to use it and access the information, and whether they will be party to and notified of decisions affecting the collection, retention, use, disclosure, and security of personal information. Smart cards must not become Big Brother's surveillance assistant, and the much prized

'efficiency' they offer ought not to override human dignity, autonomy, and privacy. Smart card developments must comply with broader ethical norms such as beneficence, non-discrimination, respect, openness/transparency, informed consent, access, matching, gate-keeping, and responsibility (Foran, 1996a).

Biometric encryption refers to digital photographs, fingerprint scans, hand geometry, retina scans, and voice prints, all of which show unique biological characteristics that distinguish individuals. Biometrics have an intuitive association with criminal fingerprinting as providers of unique identifiers. The Metropolitan Toronto Council's implementation of a biometric 'Client Identification and Benefits System' was morally justified on the grounds that its finger-scanning technology is less cumbersome than existing identification methods, that it stops welfare recipients from 'double-dipping,' and that it prevents vendor fraud perpetrated by service providers. Critics claim that finger scanning criminalizes welfare recipients, perpetuates the myth that economic problems are caused by the poor, and violates civil rights to privacy and freedom from intrusion. At ethical issue is the need to balance governmental concerns with convenience and efficiency with individual freedom and privacy.

It is at least arguable that when biometric encryption is not used as a unique identifier, but is used instead for the purpose of authenticating eligibility of recipients, the technology can actually enhance privacy as long as the necessary safeguards are in place. Biometrics then becomes a privacy-enhancing technology. The Ontario privacy commissioner endorses a variety of safeguards, such as restricting encrypted finger scanning to authentication of eligibility, only in order to ensure that it is not used as an instrument of social control or surveillance. If we ensure that a fingerprint cannot be reconstructed from a finger scan or that a latent fingerprint picked from a crime scene cannot be matched to a finger scan, then it will be easier to ensure that an encrypted finger scan cannot be used as a unique identifier. Strict controls need to be in place on *who* may access biometric information, and *what* it may be used for. Access to biometric information ought to require the production of a proper legal warrant prior to permitting access by police or other government departments, thereby ensuring that benefits data are stored separately from personal identifiers such as an individual's name and date of birth (Cavoukian, 2000). We are not suggesting that smart card and biometric technologies ought to be classified, prima facie, as surveillance technologies or be ethically proscribed. In fact,

such technologies can utilize privacy-enhancing technologies (PETs) in ways that protect privacy and, thus, human freedom and well-being, as we shall see below.

The constant monitoring of individuals in public and private places violates a prima facie human right to freedom from surveillance. Many Canadians appear to approve of the use of *closed circuit television camera* (CCTC) monitoring for the sake of crime prevention, but they are uncomfortable with private sector surveillance. When a video recording of a man attempting suicide allowed police to save his life, it was seen as a justifiable 'primary' use. However, when the video was sold to the media – a 'secondary' use – the commodification of the information was seen as contravening the implicit contract that the surveillance will be used only for public safety. Representatives of the security industry admit that they have often failed to apply ethical standards and that the industry is largely motivated by profits (HC, 1997). Massive Millimeter Wave Detectors (MMWDs), Computerized Facial Recognition Systems (CFRS), and Forward Looking Infrared Radar (FLIR) surveillance technologies raise potential human rights concerns. MMWDs scan beneath clothing to detect guns and drugs from a range of twelve feet or more and can 'look' through walls to detect activity (Banisar, 1996). CFRS can be digitized and matched with facial images stored in databases. In the state of Massachusetts this technology has been used to develop a database with digitized photographs of 4.2 million drivers (HC, 1997, appendix I). The potential power of CFRS to monitor individual movements is formidable. Policy advocates argue that camera surveillance technologies ought to reflect 'reasonable' expectations of the individuals about whom information is collected and that institutions need to define clearly and concretely the public interests that justify such surveillance systems. Yet again, this begs the question concerning the ethical criteria for deciding whether or not a given means of surveillance data is ethically acceptable.

Electronic monitoring (EM) entails the direct surveillance of persons on probation or parole. In Ontario, EM is a non-violent offender supervision program that uses technology to verify that an offender remains within his or her home during legally mandated periods as a condition of early release from jail (OMSGCS, 1995a,b). EM has been used in British Columbia since 1987 and in Saskatchewan since 1990. Newfoundland and the Yukon have adopted EM programs, and EM is used extensively throughout the United States. The most common EM technology entails a tamper-resistant ankle bracelet containing a miniature

radio transmitter that sends a signal to a receiver connected to the wearer's home telephone line. The receiver then transmits data via the telephone line to a central monitoring computer. EM officers conduct random spot-checks with a drive-by device that can detect the presence of someone wearing a bracelet inside a nearby building. The value behind EM, at least in theory if not always in practice, is societal protection. Advocates view EM as a safe, cost-effective alternative to imprisonment, which also provides family support and community integration to the offender, thereby freeing correctional authorities to focus limited resources on serious crime. Critics argue that privacy is more than a mere social technique for assuring substantive legal or societal interests and that some varieties of EM are profoundly unethical (Fried, 1984).[1]

Genetic testing entails both genetic screening and genetic monitoring. Genetic screening presents a temporal 'snapshot' of a person's genetic makeup, while genetic monitoring entails the periodic examination of individuals in order to discover indications of genetic mutations that might result from exposure to certain substances such as toxic chemicals, the effects of radiation, or viruses such as human immunodeficiency virus (HIV). Forensic DNA analysis is not a diagnostic tool, but instead looks for a match or a relationship between two genetic samples. The most common type is 'restriction fragment length polymorphism' (RFLP), which does not give diagnostic information about a person. Forensic DNA analysis can be a powerful tool for linking genetic samples from the scene of a crime or from the victim (e.g., through a semen specimen, in the case of rape) with a suspect, and the analysis also has led to the exoneration of suspects and those falsely accused. Both privacy experts and non-experts agree that genetic information involves a qualitative difference – not simply a difference in degree – that sets it apart from biometric identification and video surveillance practices (HC, 1997). We agree that there is no potential surveillance technology more threatening to privacy than that designed to unlock the information contained in human genes. Existing laws may 'not prevent realizing our worst fears about privacy abuses through genetic testing' (PCC, 1992, 2–3). Knowing about an individual's genetic makeup provides information about relatives and possible behaviours and can indicate what will or may happen to health in the future. The Privacy Commission maintains that Canadians have a right to reasonable expectation of genetic privacy 'even if there is a perceived good for society or for the person flowing from the testing'

(PCC, 1992, 10). Conversely, an ethical case may be made for the collection, use, and disclosure of AIDS-related personal information. Privacy rights must give way to other social goods, including the need to permit the collection, use, and disclosure of personal information as part of 'an effective public health response to AIDS' (PCC, 1989, 1–2). The assertion is hedged by an equal affirmation of workers' rights to non-discrimination in the workplace: 'Health and Welfare Canada considers that with the adoption of universal precautions in high-risk work environments it is extremely rare to find an occupational setting where it is essential, in the interests of individual or public safety, to establish being HIV infection-free as a job requirement' (PCC, 1989, 18).

The ethical issues and actual problems surrounding genetic privacy are anything but anecdotal. In a case study published in the journal *Science and Engineering Ethics* it is noted that 200 data subjects reported discrimination as a result of genetic testing (Quittner, 1997). Ethical problems arise when genetic information is passed on to law enforcement agencies, which allows searching in a way that usually requires appropriate and direct legal approval, or when secondary use of information is obtained about an individual's blood relatives. Distributive justice requires that insurance companies find a balance between information that is essential for insurance underwriting and a basic equity where persons are not discriminated against on the basis of susceptibility. The Canadian insurance industry at present does not require insurance applicants to undergo genetic testing. An earlier report of the Science Council of Canada found no workplace programs that screen potential employees for genetic susceptibility to disease and no programs that monitor employees for mutations or diseases resulting from workplace exposure (PCC, 1992). Nonetheless, persons who are aware of genetic abnormalities are expected to disclose this information when they apply for insurance. In the future we must guard against routine genetic testing used to qualify persons for insurance (USOTA, 1991).[2] A right to 'reasonable expectation' of genetic privacy includes, at a minimum, the right not to have others know one's possible genetic destiny and, potentially, even a right 'not to know' about one's genetic self (Cavoukian, 1994). While testing benefits certainly include medical diagnosis, health care, and the promotion of law enforcement goals, the increasingly commercial use of genetic information raises ethical questions about the legal, employment, and insurance discrimination implications (Gostin, 1991, 1995; Lebacqz, 1994). We will revisit these concerns in our conclusion.

Legal, Social Science, and Philosophical Conceptions of Privacy

Conceptions of privacy have generated an enormous literature going back at least a century.[3] It is not surprising that there have been long-standing moral and legal debates regarding privacy and the right to privacy, since a community's agreed-upon conception of norms is a social construction. We generally do not recognize privacy's importance 'until it is taken away ... it is a personal right that we assume we have yet take for granted until something or someone infringes on it' (Flaherty, 1991, 831). Bennett and Grant (1999) maintain that the privacy solutions of the past are inadequate to our present technological and surveillance situation. The statutory codification of fair information principles, their application to organizations that process personal data, and oversight and enforcement by independent data protection agencies are necessary developments, but are insufficient for the implementation of privacy protection today and in the future. Paths to privacy protection in the future entail applying the fair information principles, building privacy into new technologies, factoring privacy into good business practices, thinking about the importance of privacy globally, and protesting overt forms of surveillance out of existence. They are equally concerned with the *conditions* that will facilitate privacy protection in order to prevent the present mosaic of privacy solutions from becoming a confusing and irreconcilable set of strategies. We will contribute to a better understanding of these conditions below.

Privacy, of course, has its critics. Privacy has been seen as a deprivation of things essential to a truly human life (Arendt, 1958). Inflation of a right to privacy has turned the rhetoric into more than a legal concept, becoming 'a religious tenet, a cult, a fetish ... a byproduct of individual competitiveness' (Hixson, 1987, xiv). For still others, the equation of personal privacy with private ownership leads to the decay of societal commonality and its public amenities. Privacy is a cult 'specifically designed as a defence mechanism for the protection of anti-social behaviour' in which the welfare of individuals is conceived as the ultimate end of all social organization, and where the libertarian asserts 'each for himself and the devil take the hindmost' (Arndt, 1949, 69–71). The conflict of interpretations that surrounds privacy concerns balancing individual rights, responsibilities, and goods with societal rights, responsibilities, and goods. This ethical challenge has become far more pronounced in the information age, with interpretive conflicts posing the substantive questions: What is the meaning of privacy?

What are the basic goods sought to be vindicated in the name of individual and societal privacy rights?

Identifying the precise nature or definition of privacy is no mean task, especially if one consciously seeks to avoid begging the questions that inevitably arise in the proposed definitions. Legal views of a right to privacy often obfuscate more than they illuminate privacy's definition and justificatory value. Compare, for example, Warren and Brandeis's 1890 defence of privacy as an individual's 'right to be let alone' and the respect due one's 'inviolate personality' with William Prosser's later argument that privacy is not an independent value per se, but a complex of four torts that deal with intrusion upon one's solitude or private affairs, public disclosure of embarrassing private fact, publicity that places one in a false light in the public eye, and 'intangible property' or appropriation of one's name or likeness for personal advantage (Warren and Brandeis, 1890; Prosser, 1984). Bloustein later repudiated Prosser on the grounds that the value protected by the right to privacy is really a 'dignitary tort.' The legal remedy merely represents 'a social vindication of the human spirit thus threatened rather than a recompense for the loss suffered' (Bloustein, 1984, 188). We must here distinguish moral and legal rights. A loss of privacy, whether instigated by moral claims, loss of control, or violation of access to one's person, raises the question of whether or not an actual legal right to privacy has been infringed. A person might have diminished privacy by revealing his or her mailing address to a telemarketer, but there is no infringement of a legal right unless a relevant proscriptive claim-right has been violated. Still, the question of the moral 'ought' remains.

Social scientists have set forth lengthy descriptions of privacy that characterize it as a social value. Robert Murphy's fascinating anthropological study of the North African Tuareg, in which he notes their custom of veiling the face, has shown that reserve, restraint, and social distance pervade social relationships. The structural components of social distancing or privacy are universal and are related to societal role conflict and differentiation. The Tuareg restricts information about himself and his emotions as a way of protection from the stresses of social interaction. The symbolic removal of a portion of identity allows the Tuareg to act amid conflicting interests and uncertainty. Distance-setting techniques function in some societies through joking and respect or avoidance behaviour towards relatives. In the North American and European contexts, the masked ball allows certain latitude and freedom. In much the same way, modern sunglasses are worn by emirs

and Middle Eastern potentates, both as 'badges of office' and as a means of creating distance. The maintenance of social aloofness is a pervasive factor in human relationships, autonomous action, and personal identity, and is a necessary corollary of social association. Social conduct inevitably implies both limitations upon a range of expected behaviours and closures upon other relations and behaviours. Human actors insulate large portions of social existence by withholding knowledge of their course and commitment in a given action situation. Such action is concretely accomplished 'through distance setting mechanisms – the privacy and withdrawal of the social person is a quality of life in society. That he withholds himself while communicating and communicates through removal is not a contradiction in terms but a quality of all social interaction' (Murphy, 1984, 51).

Alan Westin, in a classic study of the origin of modern claims to privacy, corroborates and expands Murphy's comparative analysis of the Tuareg (Westin, 1984). Westin invokes animal studies to argue that all animals seek periods of individual seclusion or small-group identity, even though our modern norms of privacy are largely absent from primitive societies. Basing his work on leading anthropology, sociology, and ethnographic studies, Westin finds four general aspects of privacy that are culturally universal. First, privacy needs for the individual, intimate family group, and wider community and the construction of germane social norms are present cross-culturally, though the types of privacy norms are contextually varied. Second, in most organized societies human beings believe that they are 'watched by gods or spirits even when they are physically alone,' and personal communication with 'guardian spirits' requires physical solitude in forest, beach, or church, as well as psychological privacy through self-induced trance or dreams. A third universal element is the tendency for individuals to invade the privacy of others because of curiosity and often by means of gossip. At the same time, society guards against anti-social conduct by employing surveillance technologies in order to protect personal and group rights and enforce societal rules and taboos. Fourth, in the anthropological literature it is suggested that modern persons enjoy more physical and psychological privacy than our primitive ancestors and far greater freedom to choose privacy values through sociopolitical means. Nonetheless, he concludes: 'modern societies have also brought developments that work against the achievement of privacy: density and crowding of populations; large bureaucratic organizational life; popular moods of alienation and insecurity that can lead

to desires for new "total" relations; new instruments of physical, psychological, and data surveillance ... and the modern state, with its military, technological, and propaganda capacities to create and sustain an Orwellian control of life' (Westin, 1984, 70).

The contemporary philosophical debate between liberals and communitarians over the proper role of individual and societal privacy rights and responsibilities actually turns out to be a much older debate than one might have expected. If Westin is correct, the struggle to limit surveillance by authorities is embedded in western political and social institutions stretching back as far as the Greek and Roman eras. On the one hand, there exists a tradition, associated with the democratic city-state in ancient Greece, English Protestantism, common-law traditions, and American constitutionalism and property concepts, that seeks to limit the surveillance powers of government, religious, and economic institutions in the interest of privacy for individuals, families, and social groups. On the other hand, the tradition that runs from Sparta, the Roman Empire, the medieval Church, and the continental nation-state provided broad powers of surveillance. No society with a reputation for providing liberty has failed to limit the surveillance powers of various authorities. The challenge is to keep the former tradition meaningful when technological change promises to give public and private authorities the actual power to do what a combination of physical and socio-legal restraints had previously prevented.

Philosophers have generally defined privacy along three main lines (Schoeman, 1984). First, privacy has been regarded as a 'claim,' 'entitlement,' or 'right' of the person to determine what personal information may be communicated to others. The problem with this view is that it begs the question about the moral status of privacy from the outset by assuming that privacy is, in fact, worthy of protection by the individual to whom the information relates. In this view, privacy is certainly important, but the justificatory ground for it is not clearly defined. What exactly is it about privacy that makes it so important that it should be entrenched in binding claim-rights?

Second, privacy is often defined in relation to 'control' over access to information about oneself, over the intimacies of personal identity, or over who has sensory access to a given individual (Inness, 1992; Gavison, 1984). Neither is the definition of privacy as control entirely satisfactory. A person shipwrecked on a deserted island or lost in a forest has certainly lost control over personal information, but we cannot say he has no privacy; in fact, he has too much privacy. Similarly, a person

who wilfully discloses everything about herself to others cannot be said to have lost control over personal information. But do these individuals have privacy? Control-based definitions of privacy are often part of a will theory of rights, which maintains that for someone to have a right is to be in a position to determine by will or choice how another person will act (Hart, 1955), and this is the more relevant meaning of privacy as control.

A third definition of privacy, linked to the previous one but concerning more the respondent of the right, identifies it with a state or condition of 'limited access' to a person, the intimacies of life, or a person's thoughts or body. Is limited access actually a desirable state of affairs? How valuable is this condition in relation to a host of other human goods and values? Privacy understood as limited access leaves open the possibility for a certain autonomy with respect to abortion, birth control, and gender orientation of a person's partner, but it raises, in turn the question of whether privacy is actually derived from an individual's rightful sphere of autonomy. Thomson (1984, 1990), for example, argues that the right to privacy is really a cluster of rights that intersects with two other clusters, that is, 'the right over the person' and 'rights which owning property consists in.' The right to privacy is 'derivative' in the sense that it is possible to explain in various cases involving privacy interests why we have a right without recourse to privacy. For example, if someone tortures an individual to extort personal information, such action is wrong, because the person has a prior right not to be hurt or harmed. Interests protected under the rubric of privacy are not distinctive to privacy per se. Privacy points, rather, to interests or values recognized as significant under different labels, such as the principle of respect for persons, the infliction of emotional distress on another, or the misappropriation of another's property assets. Thomson agrees with the view that 'one can logically argue that the concept of a right to privacy was never required in the first place, and that its whole history is an illustration of how well-meaning but impatient academicians can upset the normal development of the law by pushing it too hard'(Davis, 1959, 230). Thomson's argument that the right to privacy intersects with the *justification* of property rights is perceptive, and we will return to the importance of this conceptual link, below.

Benn (1984) argues that privacy is a norm-dependent and norm-invoking concept and practice that very much affect social life. To speak of 'private affairs' is to speak with some reference to norms restricting unlicensed observation, reporting, or entry, even though

there is no particular norm necessary to cover the concept of privacy. He affirms that privacy deals with a cluster of immunities that curb the freedom of others to do things that are innocent if done to objects other than persons, and even to persons, if done with their consent. Anyone who desires not to be an object of scrutiny has a prima facie claim to such immunity grounded in the principle of respect for persons. Benn grounds this claim not in the subject's mere desire, but rather in the relation that obtains between a person as an object of scrutiny, on the one hand, and as a conscious, experiencing human being capable of having action projects and assessing achievements in relation to them, on the other hand.

Fried (1984) maintains that privacy is integrally related to intersubjective relations and basic human ends such as respect, love, friendship, and trust. Threats to privacy, therefore, are threats to our very integrity as persons among other persons. His fundamental principle of morality seeks to establish the liberty of each person to define and pursue values free from unwanted infringement. Respect is a correlate of this view and is the attitude manifested when a person observes the constraints of morality in dealings with another person and thus respects the basic rights of the other: 'Persons are those who are obliged to observe the constraints of the principle of morality in their dealings with each other, and thus to show respect towards each other. Self-respect is, then, the attitude by which a person believes himself to be entitled to be treated by other persons in accordance with the principle of morality' (Fried, 1984, 206–7). Privacy is also intuitively related to secrecy and limits the access of others to knowledge of oneself. This intuitive notion is necessary but insufficient, because it is still too negative. Privacy is not simply the absence of information about us by others, but is our own control over the information about ourselves. In other words, privacy is an aspect of personal liberty related to action. 'Acts derive their meaning partly from their social context – from how many people know about them and what the knowledge consists of.' As Fried observes, 'a reproof administered out of the hearing of third persons may be an act of kindness, but if administered in public it becomes cruel and degrading' (Fried, 1984, 210). Privacy protects liberty when one does or says things that are unconventional or unpopular but are not forbidden by morality. When we think that our every word and deed will be made public, then we are inhibited from acting in certain ways.

This intuitive conception of privacy supports familiar arguments for

the right to privacy, but Fried admits that it still remains vulnerable to arguments that a given invasion of privacy might actually secure for us other kinds of liberty or goods that more than compensate for what we have lost. The parolee who is freed from the prison environment for the price of being an electronically 'wired' subject is a case in point. Crucial to Fried's view is a notion of privacy as the necessary context for relationships. Privacy confers a title to information about oneself that is the sine qua non of relationship. Love and friendship 'involve the initial respect for the rights of others which morality requires of everyone. They further involve the voluntary and spontaneous relinquishment of *something* between friend and friend, lover and lover. The title to information about oneself conferred by privacy provides the necessary something. To be friends or lovers persons must be intimate to some degree with each other. But intimacy is the sharing of information about one's actions, beliefs, or emotions which one does not share with all, and which one has the right not to share with anyone. By conferring this right, privacy creates the moral capital which we spend in friendship and love' (Fried, 1984, 211).

Fried's conception of privacy as 'moral capital' goes beyond mere voluntary conferral of information to another. There is also a need for privacy of one's innermost thoughts in relation to friends, lovers, and, indeed, the world. There are personal thoughts that we all have, which, if they were expressed to a friend or lover, would arouse hostility, though having them is entirely consistent with the nature of love. These most intimate of thoughts are mere 'unratified possibilities for action,' and only by expressing them do we appropriate and draw them into our relations with others. Herein lies the most complete form of privacy, because 'it is necessary not only to our freedom to define our relations to others but also to our freedom to define ourselves. To be deprived of this control not only over what we do but over who we are is the ultimate assault on liberty, personality, and self-respect' (Fried, 1984, 212). Forced compulsions brought to bear on individuals to make them reveal aspects of their deepest selves is a denial of title to control personal information and, thus, the picture they would have others draw of them.

Control over information about oneself is relative, as is control over one's bodily security and property. The more one ventures into the public realm and pursues interests with others, the more one inevitably risks privacy invasions. If a person cannot stand the heat of privacy invasion, he should get out of the public kitchen. It is the business of

legal and social institutions to define and protect the right to privacy in relation to procedural and substantive justice. Two general conditions must be met. The process itself must be just – that is, 'the interests of all [should be] fairly represented' – and the outcome of the process must protect basic dignity and provide 'moral capital for personal relations in the form of absolute titles to at least some information about oneself' (Fried, 1984, 213).

Social constructions of privacy emerging as products of political processes are inevitable, but convention also plays an important role in designating areas symbolic of privacy that may go beyond their particular importance. Fried's psychological presupposition is that exaggerated respect for conventionally protected privacy areas compensates for the inevitable compromises of a given social system. Privacy is compromised by the exercise of others' rights, by conduct that society does not condone but cannot regulate, and by overt invasions and aggressions. For this reason, social systems have evolved to give symbolic importance to conventionally designated areas such as the excretory functions, norms surrounding sex and health, and privileges against self-incrimination. The latter is contingent in that no set of rules is necessary to the existence of such an institution of privacy. It is symbolic insofar as the exercise of the privilege shows society's willingness to except constraints on the pursuit of valid and vital state interests in order to acknowledge the right of privacy and the respect for the individual it entails.

Action Theory and the Ethical Justification of Privacy Rights

Legal and philosophical attempts to derive privacy rights from trust, respect, autonomy, and inherent dignity are useful, but all incur difficulties. Fried's philosophical conception is the most formidable, because he rightly opens up the human realms of privacy in relation to respect, love, communication, friendship, trust, intimacy, and socially constructed private and public norms. There are also clear merits to control-based definitions of privacy, especially Thomson's derivation thesis grounded in the autonomy of agents. Philosophical conceptions of privacy as a claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others nonetheless beg the question of how ethically to justify privacy 'claims' in contrast to liberties, powers, and immunities (Hohfeld, 1966 [1919]).

For while trust, respect, autonomy, and inherent dignity are not mutually exclusive with a justificatory basis for privacy in the necessary conditions of action, the expression 'A has a right to privacy' and 'A has trust/respect/autonomy/inherent dignity' may seem to be equivalent, so that the latter simply reduplicates the former. If these two expressions are equivalent in meaning, then the attribution of trust/respect/autonomy/inherent dignity adds nothing substantial to the attribution of rights and does not satisfy the logical requirement of non-circularity. Yet privacy must have coherence as a moral and human right if legal claims to its protection are to be rationally justified and public policies legitimated. The principle of human rights as the rights of every person to freedom and well-being as the necessary conditions of human action (i.e., those conditions that must be fulfilled if human action is to be possible either at all or with general chances of success in achieving the purposes for which humans act) provides more specificity and less disputable contents than these other approaches offer. An action-based ground for human rights is similar to control-based definitions of privacy, but different insofar as the right to freedom consists in a person's controlling action, participating in transactions through unforced consent, and doing so with knowledge of relevant circumstances, so that one's behaviour is neither compelled nor prevented by the actions of other persons. A person's right to freedom is violated if she is subjected to violence, coercion, deception, or other procedures that attack or remove her informed control of behaviour by her own unforced choice. The right to freedom includes having a sphere of personal autonomy and privacy whereby one is left alone by others unless he or she unforcedly consents to undergo the actions of others.

Privacy and Security Policy in the Light of the Principle of Human Rights

Privacy rights are best viewed as a species of the generic rights to freedom and well-being, which are the objects of human rights. There exists a general human right to freedom because freedom is a necessary condition of purposive action. Freedom consists in controlling one's behaviour by one's unforced choice, having knowledge of relevant circumstances, and intending to achieve some ends or goals for which one acts. Freedom includes the negative freedom of not being interfered with by others, since this would remove the individual's control of his or her behaviour. It also entails the correlative duty of

others, individuals, and governments to refrain from interfering with individuals' control of their own behaviour.

We must distinguish between freedoms that are essential for action in general and freedoms that pertain to particular or specific actions whose performance or non-performance does not affect the general necessary conditions of action. This distinction is related to a further important distinction between 'dispositional' and 'occurrent' freedom. Dispositional freedom entails having the continuing and long-range effective ability to exercise control over one's behaviour by one's unforced choice. Occurrent freedom entails exercising such control in particular situations. Moreover, the unrestricted ability to act out dispositional exercises of freedom or control is much more important for an individual's status as a rational agent than is the abilitity to perform some particular actions. Examples of dispositional freedom include the exercise of civil liberties, freedom of movement in general, and choices of ways of life. Support of this general right to freedom is essential to the moral legitimacy of governments. Because of the paradox of freedom noted earlier, there cannot be universal or completely unrestricted freedom, but the fact that certain freedoms must be restricted is not an objection to there being a general right to freedom.

The Non-Absoluteness of Human Rights

No human rights are absolute in the sense of not being justifiably infringed on under any circumstances, and this statement holds even for the right to life (Gewirth, 1981). The important question is when, and on what grounds, freedom may be restricted. There is a prima facie presumption in favour of freedom, but it may be overridden by the action-based rights of others. The Principle of Generic Constistency (PGC) requires that each person be left free to perform any actions so long as the individual does not threaten or violate other individuals' rights to freedom (by coercion) or well-being (by direct harm). With respect to individuals, harm consists in removing or threatening basic, non-substractive, or additive goods to which all persons have rights of well-being. Thus, the right to freedom of Smith may conflict with the right to well-being of Jones if Smith uses his freedom to reveal Jones's private affairs, or to disclose embarrassing private facts about Jones, or to place Jones in a public false light, or if Smith appropriates Jones's name or likeness for personal advantage – that is, if Smith violates the privacy rights of Jones. At the social and political level, harm entails

violating laws that provide for basic, non-substractive, and additive goods, including those public goods whose benefits accrue to citizens.

Limitations to freedom of speech on the Internet and certain types of surveillance practices may be imposed on citizens as an indirect application of the PGC. The criterion of 'transactional inconsistency' establishes that if a person or group violates the generic rights of another, then action to prevent or remove inconsistency is justified (Gewirth, 1978, 129). The PGC authorizes and even requires coercion or harm as punishment for the prevention and correction of antecedent basic harm. It sets a limit on the right to freedom for individuals when inflicted in accordance with consensual social rules or institutions. Hence, individuals' right to freedom may include freedom to drink alcohol, but if they drink and drive a motor vehicle, they incur transactional inconsistency. A breathalyser test is a legitimate social practice that operates consensually to support and protect the well-being of persons. Drug testing as a prerequisite for very specific types of employment involving public safety is another example where an indirect application of the PGC would justifiably limit the privacy of the individual. Traffic regulations, like not driving 150 kilometres per hour in a 120-kilometre speed zone, are laws that provide for public goods. These specific examples provide a justifiable interference with freedom on the PGC's grounds of helping to secure each person's right to well-being as instantiated in a physically safe environment.

The Application of Basic, Non-substractive, and Additive Goods

Basic well-being consists in having the essential preconditions of action, including basic goods such as life, physical integrity (including its means, such as food, clothing, and shelter), mental equilibrium, and a feeling of confidence about attaining life goals. While there certainly are different perceptions of the nature of human goods among different human beings and groups, these variations do not affect the present view of these contents of basic goods. The reason is that the assertion that agents necessarily regard these contents as good is made within the context of purposive action. The assertion indicates the preconditions necessary to the very existence of an individual's purposive actions viewed generically and collectively. Since human beings regard their purposes as good, the rational agent must regard these conditions as at least instrumentally good, whatever the particular contingent and variable purposes and evaluations might be. At an extreme, of course, an

individual might have the purpose to put an end to all of his or her purposive actions through suicide, but the conditions would equally hold in order to carry out the suicide. As noted in chapter 1, the argument from an individual's evaluation of his or her purposes and purposive actions as good, to persons valuing freedom and well-being as the necessary preconditions of action, is an inference drawn according to the dialectically necessary method. Because the argument proceeds from within the conscious viewpoint of the individual, it is not affected by evaluations made from other standpoints at this stage of the argument to the PGC. On the other hand, since agency is the necessary and universal context of the whole sphere of practice, the standpoint of the agent inevitably occupies a primacy of position in relation to other standpoints.

Non-substractive well-being consists in having the abilities and conditions necessary to maintain one's general level of purpose-fulfilment and capacities for action. Non-substractive goods consist in retaining, not losing, what one already has and regards as good. To lose a non-substractive good is to suffer a diminution of goods one already has and thereby to have one's level of purpose-fulfilment lowered. Privacy violations certainly may harm an individual's non-substractive goods, for example, when one is adversely affected in his or her abilities to plan for the future (e.g., investment fraud perpetrated over the Internet), to have knowledge of facts relevant to projected actions (e.g., as infringed by intended omissions, misinformation, and disinformation), or to utilize resources to fulfil needs (e.g., public access to the information highway for persons with disabilities and those living in remote, northern regions of Canada). Specific violations entail being lied to, cheated, stolen from, or *defamed*; suffering broken promises; and being subjected to dangerous, degrading, or excessively debilitating conditions of physical labour or housing when resources actually are available for improvement.

Additive well-being consists in having the conditions and abilities necessary for actually augmenting or increasing one's purposes and capacity for action, such as the right to education, self-esteem, and opportunities for acquiring an income and wealth. In an informational economy, physical access to the Internet, access to government and private sector content and services, and education for computer skills and training are additive goods, if not increasingly non-substractive goods for many individuals. The exclusive meaning of additive good refers here to purposes that are comparative and substantive, since it refers to

certain contents of purposes rather than others and compares these contents with those that are more directly tied to the conditions of purposive action. Being lied to by Internet advertising or misled through spam e-mail promotions, for example, tends to lower a person's capacities for success in actions affected by the lies, just as receiving a good education tends to increase, though does not guarantee, an individual's capability of successful action.

One of the important components of additive well-being, and well-being generally, is community. This is the case in both an instrumental and a constitutive respect. In an instrumental way, being a member of a supportive community helps the individual to be more effective in achieving his or her purposes. Indeed, it is only by virtue of being born into a nurturing and sustaining community that the self acquires the abilities and conditions needed for achieving his or her purposes. In this way, community is a means towards the fulfilment of self-interest, as well as the self-fulfilment of others. Socialization into respect for the privacy and security of others as well as for oneself is an important function of community. The constitutive dimension is epitomized in the notion of Plato, Aristotle, and Aquinas that the human being is a social-political animal by nature. As human beings we develop our full humanity only in association with others in a well-ordered society. The comparative anthropological and social scientific studies noted above reveal the important role of privacy as a social value in all human associations, which involves either conscious or subconscious awareness of and concern for other persons' privacy rights and interests as well as one's own. Community is also protective of individual interests that are the objects of rights, including privacy rights.

'Community standards' are often invoked as a moral and legal norm for adjudicating conflicting claims over responsible censorship and freedom of expression rights (Foran, 1996b). It is admittedly difficult to speak of community standards in cyberspace, where freedom of association has become so diffuse and transnational that civil and criminal limits on speech are almost impossible to justify constitutionally. At a minimum, information and knowledge must not forget their actual purposes within and for the human community, just as the human spirit in search of additive goods must not forget its dependence upon bodily existence. Community serves human freedom, whose 'proof' lies not with the 'intellect,' but in communal action and communication attained with others in an authentically free community committed to the principle of human rights.[4]

Although all persons regard their well-being as a necessary good because of its relation to their own purpose-fulfilments as well as to those of others, the components of well-being fall into a hierarchy that is determined by the degree of their indispensability for action. The basic capabilities of action are the most necessary, because persons would be able to act not at all or only in very restricted ways without basic goods. Among the basic goods there is a hierarchy in which life has primacy and includes various other physical and mental goods, some of which are more indispensable than others for action and purpose-fulfilment. With respect to the other two kinds of well-being and goods, non-substractive capabilities rank higher than additive goods because retention of the goods one already has is a necessary condition of being able to increase one's stock of goods. In this way, the hierarchy of well-being is analogous to the hierarchy of needs developed in psychological theory (Maslow, 1954).

The Application of the Criterion of Degrees of Needfulness for Action

The criterion of degrees of needfulness for action states that when two rights conflict with one another, that right takes precedence whose object is more needed for action. 'Basic' well-being is more necessary for action than 'non-substractive' well-being, while the latter is usually more necessary for action than 'additive' well-being. On the basis of the criterion, rights not to be stolen from or lied to are overridden by the rights not to starve or be murdered if the latter rights can be fulfilled only by infringing the former. Specific harms done by violations of a person's non-substractive rights are usually less important in their impact on their recipients' well-being than are harms done by violations of basic rights and, hence, under certain circumstances may not justify the state's coercive legal resources to combat or correct them. Conversely, there are cases where the deprivation of freedom or of life is not prohibited by the principle of human rights as morally wrong. Such deprivations have been inflicted in justifiable warfare or by imprisonment for crimes such as murder. Encryption policies that seek to protect critical information infrastructures that are crucial for the maintenance of life and basic well-being are arguably justified on this basis. In this context, however, what is crucial is the fact that any deprivations that might be inflicted are carried out by agents of organizational institutions in order to enforce social rules agreed upon by consensual and participatory democratic process. When institutional social rules are

enforced by the agents of tyrannical governments and various rights are infringed, including privacy rights, such rules violate the principle of human rights. When global surveillance practices go beyond the reasonable needs and legitimate purposes of defence to become technologies of positive surveillance against non-combatants or innocents, such policies are not justifiable in accordance with the PGC.

Now the sceptic may ask: Does not the criterion of degrees of needfulness for action amount to a 'utilitarianism of rights' (Nozick, 1974, 28–30), whereby minimizing the infringement of individual rights is the main goal and whose means is the infringement of less important rights in order to prevent the harm that would result from the infringement of more important rights? Such a utilitarian calculus might be wrongly used to justify horrid violations of individual freedom as ways of securing positive rights to basic well-being, such as removing a healthy person's kidneys or eyes in order to preserve the life or sight of another individual. After all, not being dead is more 'needful' for action than is having a kidney or eyesight. Similarly, since driving automobiles, which certainly leads to fatalities, is less needful for action than life, would not this criterion justify infringing the right of persons to drive? Or again, since the poor have a greater need for money in relation to their agency than do the rich, is not the right of the rich to retain all of their wealth justifiably overridden by the right of the poor to be helped by transferring some of this wealth to them, as Robin Hood believed?

Ethical Balancing: No 'Utilitarianism of Rights'

Several points must be kept in mind about the criterion of degrees of needfulness for action in response to these criticisms, as well as the conception of ethical 'balance' advocated in our study. First, the objects that are being compared by the criterion of degrees of needfulness for action are, first and foremost, needs of agency, and the goods required must be had either for the very possibility of action or for having general chances of success of action. The goods defined above in relation to basic, non-substractive, and additive well-being are quite objective and are not relative to particular, idiosyncratic standards set by individual preferences or desires. As such, the degrees of needfulness can be compared in a more objective way, taking into account human diversity, differing cultural contexts, and the extents to which persons can actually fulfil these needs.

Second, the word *action* holds primacy in the context of the criterion of degrees of needfulness for action. The criterion differs from a 'utilitarianism of rights,' where the latter implies a restless calculus to interfere with rights in order to come out with a quantitatively weighted minimum of rights infringments (Nozick, 1974; Waldron, 1993). This point bears on our earlier discussion of the concept of 'balance' and Raab's objection to the way that the balancing of data protection is normally construed. According to Raab, the public interest side of the equation typically involves 'social utilities' such as governmental efficiency and the maintenance of law and order or 'personal utilities' such as access to goods and services. These criteria do not sufficiently warrant a balancing process, because they inevitably tend to override privacy protection, which becomes co-opted by consumerism, 'value for money,' or convenience. Certain issues get organized into politics, while others do not, and privacy gets the short end of the stick because money, votes, jobs, time, crime rates, and patients' deaths can be empirically calculated. Raab is correct to note that, when it comes to privacy, we cannot easily calculate the equivalence, and that, to take the metaphor of balancing seriously in this context, we would have to determine if some kind of quantitative parity exists between various factors. In other words, interpersonal comparisons of utility or well-being are impossible. 'There is no reader reckoner for this,' he writes. 'It is a matter of judgement, but that judgement may well be open to dispute about the weights that were deemed to attach to the competing claims or about other considerations that were overlooked' (Raab, 1999, 77). According to Raab, the criterion of degrees of needfulness for action might fall under this same critique, because the criterion holds that one individual's freedom to do X is less important for action than another person's freedom to do Y or to have some well-being component Z.

The 'balance' that we are seeking, however, is not the kind of utilitarianism of rights implied by Raab's critique of balancing, where what is involved is an unending calculus that is ready to interfere with rights in order to come out with a weighted minimum of privacy rights infringements for either individuals or the public interest. If this were, in fact, the case, then it would surely make action difficult or impossible. The context of action entailed by the principle of human rights requires only those comparisons that are restricted to wide and, for the most part, readily ascertainable disparities in degrees of importance between the objects of rights. The aim is not to enfeeble some individu-

als' actions in order to advance the actions of others per se, but rather to make the necessary conditions of action available to all persons and especially to fulfil the social and economic rights of the most deprived members of society. For this reason, the criterion is restricted to areas where the basic well-being of some individuals requires infringing the additive well-being of others or the freedom associated with the latter's well-being. Thus, rights not to be stolen from or lied to may be overridden by rights not to starve or be murdered if the latter rights can be fulfilled only by infringing on the former. The criterion of degrees of needfulness for action is applicable to questions concerning the privacy and security rights of individuals in the information age, because it guards against ideological and absolutist interpretations of libertarian rights (e.g., to free speech on the Internet in the form of child pornography), while avoiding the morass of trying to set up an intricate calculus of the relative strength of variable desires and preferences whose features often lead to 'moral indeterminacy.'[5] Moreover, given the context of action and the criterion's application to wide disparities in degrees of importance between the objects of various privacy rights, we must not expect the criterion to do more work than it is able to do. We would be the first to admit that the criterion can run up against limits with respect to normative specification, as well as the limits that mark human actions in relation to the 'limit situations' of human existence.

For this reason, the application of the criterion of degrees of needfulness is especially apropos to the goods of life and physical integrity that are essential parts of basic well-being. This is precisely why removing a healthy individuals' kidneys or eyes to prevent the death or blindness of other persons is proscribed; such policies are unjustifiable attacks on the former persons' physical integrity that pose serious threats to their own continuing agency. To be sure, persons can survive with only one kidney or one eye, and they may even have voluntarily consented to donating these organs to those they love. Were it not for their voluntary and unforced consent, however, the criterion of degrees of needfulness for action would not justify gross inflictions of bodily harm. It is also disanalogous to assimilate such a supererogatory, sacrificial act of love to governmental taxation policy whereby transfers are made from the wealthy to help to relieve the misery and abject suffering of others. This is not to suggest that the criterion therefore upholds the primacy of economic-social rights to subsistence over and against political-civil rights. Howard (1989) rightly notes that torture, sum-

mary execution, and other violations of political and civil rights are at least as destructive of the conditions of agency as is starvation. Equal distribution of civil and political rights and the protections of law are also needed to secure the elemental conditions of life and economic subsistence, as well as determination of political power that bears on the control of economic distribution policies.

The Ethical Importance of Voluntary and Unforced Consent

Knowledge and unforced consent are at the core of fair information practices, and these features may be directly linked to human action and the ethical principle of human rights and its two interrelated generic features: voluntariness or freedom, and purposiveness or intentionality. The feature of voluntariness is relevant because an action is voluntary[6] when 'its performance is under the agent's control in that he unforcedly chooses to act as he does, knowing the relevant proximate circumstances of his action' (Gewirth, 1978, 27). As we saw, the crucial private sector, privacy protection concern is whether or not the data subject's choice concerning any secondary use of information is voluntary in the sense that the agent controls his or her behaviour by unforced choice. Choices are forced when one is compelled to choose between two undesirable alternatives set up by someone else. As such, there are really three elements in a forced choice: it is a choice between alternatives both of which are undesirable to the chooser; the alternatives are set by someone else who has superior bargaining power; and the individual making the choice is compelled under the de facto circumstances to make the choice, whether or not he or she wants to do so. Forced choice thus entails the three interrelated aspects of undesireableness, compulsoriness, and threat. When one's choice is not forced, one chooses on the basis of informed reasons that do not include these compulsory and other features.

The Opt-in/Opt-out Provisions

Numerous privacy experts have noted the need to move beyond opt-in or opt-out mechanisms of individual choice (Goldman, 1999; Reidenberg, 1999; Cavoukian, 1999). As we saw in the last chapter, early drafts of the EU Directive required that information collected for one purpose not be used for another purpose without informed consent. Individuals were required to 'opt-in' to any new uses of their personal informa-

tion. Businesses generally prefer a more passive 'opt-out' requirement whereby individuals are informed about secondary uses and then given an opportunity to object to or 'opt-out' of having their personal information reused or exchanged. The fact that the European Direct Marketing Association (EDMA) spent over $50 million lobbying against the opt-in requirement and American businesses lobbied hard against an opt-in clause reveals that the alternatives actually were set by those with 'superior bargaining power.'

With respect to the concept of knowledge, when individuals provide information, they have the right to know why the information is being collected; its expected uses; the steps that will be taken to protect confidentiality, integrity, and the accuracy or quality of the information; the consequences of providing or withholding the information; and any means of redress available to the data subject. Persons also have the right to control subsequent use of their information, to object to such uses and to know that information will not be used in ways incompatible with the individual's knowledge and understanding unless there is a compelling public interest, involving, for example, law enforcement, fraud, or health concerns.

In practice, both knowledge and unforced consent as defined above are rarely operative, especially given the nature of information transactions on the Internet. De facto e-commerce practices inhibit individuals from making informed choices about any secondary uses of their personal information. Industry and businesses have the upper hand with the opt-out policy. The opt-out clause compels the data subject to make the choice about the secondary use of information, because it places the burden of restricting information use on the data subject, rather than requiring the data subject to consensually opt in to the secondary use of personal information.

The insufficiency of privacy law and practice in both Canada and the United States is also related to the weak state of constitutional jurisprudence. The so-called reasonable expectation test has been difficult to apply in the information privacy context. In the United States the courts have 'continually held that individuals have no privacy interest in information divulged to the private sector, even though modern society leaves citizens no option but to disclose to others, where, for example, disclosure is a condition of participation in society' (Goldman, 1999,105).

Unauthorized access, secondary use of information, and forced consent create problems not only for individuals, but also for firms and

businesses; hence the desire by some to build privacy into marketing strategies. Studies suggest that individuals are less likely to perceive information practices as invasive of privacy when the information is collected in the context of an existing, good, customer-business relationship; when they perceive that they have the ability voluntarily to control future use of the information; when the information collected or used is directly relevant to the transactions that they choose; and when they believe or know that the information collected will actually be used to draw reliable and valid inferences about them. Individuals are willing to disclose personal information in exchange for some economic or social benefit subject to a sort of privacy calculus whereby individuals assess that their personal information will subsequently be used fairly. 'The self-disclosure literature has focused on interpersonal relationships rather than customer relationships between individuals and firms; nevertheless, its findings are consistent regarding a balancing test. People disclose personal information to gain the benefits of a close relationship; *the benefits of disclosure are balanced with an assessment of the risks of disclosure*' (Culnan and Bies, 1999, 154; emphasis added). Here, the subject's voluntary and unforced consent to disclose are tied to a perception about the benefits of good interpersonal relationships that redound upon the well-being and future actions of individuals who choose to disclose personal information. Where mutuality is at the heart of such informational disclosure, then this becomes more than a self-interested, rational act per se.

Relevant to the principle of mutuality at the heart of the community of rights is the fact that literature on customer service links being treated justly with customer satisfaction (Schneider and Bowen, 1995). Consumers see fairness and service quality as 'inseparable issues.' Service that is perceived as unfair also is perceived as poor in quality. Conversely, perception of fair treatment of customers is related to higher levels of service satisfaction. Moreover, *trust* is crucial for the success of interpersonal and organizational relationships that range from the interpersonal to international trading (Derlega et al., 1993; Fukuyama, 1995). In a business context involving marketing relationships, trust is built up over time through social exchanges and reciprocity that are shaped by the situation. Trust reflects a willingness on the part of buyers to assume certain risks of disclosure. In a business relationship, 'trust is the willingness of one party, here a customer, to be vulnerable to the actions of another party, here a firm, based on an expectation that the firm will perform a particular action of impor-

tance to the customer, *independent of the customer's ability to monitor or control the firm.* Procedural fairness communicates information about the firm's integrity and motivation to act in a trustworthy fashion. Positive or fair outcomes enhance the customer's perceptions of the firm's trustworthiness' (Culnan and Bies, 1999, 156–7; emphasis added).

The fact that the customer is unable to monitor the firm, except after the fact, nonetheless reveals the unequal power structure at the base of the e-commerce transactions. Procedural fairness may promote customer disclosure and trust if the particular activity in which he or she is a participant is conducted fairly, such as providing the consumer with a voice in how his or her personal information will be used and control over actual outcomes. As we have seen, fair-information practices seek to operationalize procedural fairness by defining procedural guarantees, such as knowledge and consent, that allow individuals to balance their own privacy interests with the organization's need to gather personal information to support its marketing programs. Good fair-information practices send a signal to the customer that the firm can, in fact, be trusted with the customer's personal information. Because marketing relationships are characterized by social distance, this 'signalling function' is vital when customers must depend on strangers to represent their interests.[7]

Businesses do not simply need to retain customers; they must also attract new ones. The best way to do so may well be to create a 'culture of privacy' within the firm. Marketing in cyberspace poses new challenges because of the quantity of information that can be gathered from consumers. E-commerce is a point of sale transaction, and firms can record a consumers' 'mouse tracks' without disclosing how their information will be used. Businesses also have harvested e-mail addresses from public places and, in turn, have generated lists for 'spamming' (i.e., sending advertising e-mail without the recipient's consent). It is not surprising that many persons do not register with Web sites, because they do not believe that firms have adequately stated the terms and conditions of how personal information will be used.[8]

In a business context the question of the proper balance of individual and business interests in the gathering and disclosure of consumers' personal information is not a straightforward 'rational process.' The balancing of interests 'is not only shaped by the push and pull of negotiation by managers internal to the organization, but also by court

cases and legislative mandates in the larger political-legal environment' (Culnan and Bies, 1999, 163). As noted above, the criterion of degrees of needfulness must take into account human diversity, differing cultural contexts, and the extent to which persons can actually fulfil needs. At the individual level, harm consists in removing or threatening the basic, non-substractive, and additive goods to which all persons have equal rights of well-being. At the social and political level, harm entails violating laws that provide for these goods, including those public goods whose benefits accrue to citizens. By its very nature, advertising and consumer marketing tends to fall in the area of additiveness, but this makes it no less powerful.[9] Additive well-being consists in having the conditions and abilities necessary for actually augmenting or increasing one's purposes and capacity for action, including opportunities for acquiring an income and wealth. Being lied to or withholding information about what will factually happen to the data subject's personal information lowers an individual's capacity for success in actions affected by the lies or the omission; this is true whether the lie takes place using e-commerce on the Internet or it uses a non-digital means.

Some authors propose the creation of a property right over commercial exploitation of personal information. The right would pertain 'to the sale or trade of personal data for use in selling products or services or in setting the terms of commercial dealings ... the rights ... could be exercised or ignored by the data subject; they could also be retained or sold, much like mineral rights, development rights or air rights' (Rule and Hunter, 1999, 170). The right would constrain organizations not from requesting and compiling data from the persons with whom they deal, but only from releasing this information for any commercial purpose without the express permission of the data subject. In this way, the onus of legal responsibility would be placed on the organization holding the data. The idea would be to pay royalties to agents in exchange for their release of personal data and as implemented by 'data rights agencies.' The default condition would be not opt-out or opt-in, but no-release-by-[legal]-right. There are also recognized limitations to the right. For instance, if someone applies for a mortgage or requests the use of public utilities for electrical or phone services, then that person must authorize release of personal data. The right would not bear on release of personal information for purposes of public debate or deliberation, nor would it prohibit the holder of a debt from selling that debt to a third party who is a collection agency. It would be

reasonable 'to mandate ... that no one be refused medical care, simply because he or she refuses to permit the eventual transfer of information emanating from that care for commercial purposes' (Rule and Hunter, 1999, 176).

One can make a good argument for creating a property right over commercial exploitation of personal information.[10] Earlier in this chapter we noted Thomson's perceptive view that the right to privacy intersects with the justification of property rights. In chapter 3, we argued that the right to private property is primarily a moral claim-right, but also that it also entails legal powers to possess, use, transmit, exchange, and alienate objects. Property consists not only in objects and things, but also in relations between persons and things whereby individuals have rights with correlative duties placed on others. Property rights are negative rights insofar as other persons have duties to refrain from interfering with the owner's possessing, using, and handling, without the owner's consent, the things that are owned. This applies to houses and money, as well as to information, and Rule and Hunter's proposal concerns restricting the property right over commercial exploitation of personal information. *Exploitation* is the operative term, since the right would constitute no obstacle to any organization's maintenance of records of personal data collected from clients and customers. What is at issue is that no information could legally be sold or traded from any personal data file, for any commercial purpose, without express permission from the person concerned.

Let us recall that the consequentialist justification of private property bears directly on the *consequences* for persons as productive agents who have legal rights; it concerns the final cause, the end, or the purpose served by individuals' having property rights. The consequentialist justification is derived from well-being as the substantive generic feature of action and focuses on purposiveness and the consequences that result from an individual's actions. Because it is morally required that each person's freedom and well-being is protected in accordance with the principle of human rights, so it is also morally required that individuals have private property rights. This raises the further question, however, of whether or not the final cause of protecting individuals' freedom and well-being might be enhanced through the creation of a property right over commercial exploitation of personal information. At a minimum, such a right would certainly go far towards helping to generate a new balance of power between individuals and credit and insurance reporting companies.

Privacy-Enhancing Technologies: Possibilities and Limits

Technological solutions to problems surrounding privacy and security are based on the use of privacy-enhancing technologies (PETs) that allow both data subjects and information collectors and users to express their subjective expectations of privacy (Davies, 1999; Goldman, 1999; Reidenberg, 1999; Cavoukian, 1999). PETs refer to 'technical and organizational concepts that aim at protecting personal identity' and usually involve encryption in the form of digital signatures, blind signatures, or digital pseudonyms (Burkert, 1998, 125).[11] PETs hold out new possibilities for the promotion and protection of privacy and security rights. PETs may also provide a basis for the courts actually to recognize certain expectations as 'reasonable.' They may aid 'transparency' as individuals gain greater trust in an interactive Internet environment. Greater transparency, in turn, will mean that individuals will be less reticent to participate in e-commerce. By the use of such technologies and their consequences for transparency and trust, good privacy practices would pay dividends for participatory democracy and free speech as well.

We are not suggesting that smart cards and biometric technologies ought to be classified as negative surveillance technologies that ought to be ethically proscribed. On the contrary, such technologies can utilize PETs in ways that protect privacy – and thus human freedom and well-being. Smart cards may give the cardholder fraud-proof identification without necessarily invading privacy if consensual safeguards are in place and thereby actually serve human freedom and various kinds of well-being. The threat to privacy from an identifiable fingerprint comes from the fact that other persons have the ability to access information about a person in a clearly identifiable form that can be linked to other personal information. With the application of encryption to biometrics, the technologies can be configured in a way that gives power to individuals, as opposed to governments or the police, and thereby potentially enhances privacy. As long as the encrypted finger scan is not intended to function as a unique identifier, but is used instead for the purpose of authenticating eligibility for services or benefits, it can actually protect privacy.[12]

As a policy framework, these procedural safeguards should be consensually agreed upon by citizens. In the case of someone receiving health benefits, the government wants and ought to ensure that only those eligible to receive such benefits actually receive them, thereby

minimizing fraud and conferring both individual and social benefits. Individuals who are eligible are the subjects and the government is the respondent of the right to health benefits. So what is needed to preserve the privacy of the transaction is confirmation that the subject of the right is eligible for assistance and is, in fact, that subject and not another. Biometric encryption can verify authenticity of the subject of the right, without revealing any personal identifier, and the respondent of the right – the insurer – has a justifiable claim to know that the subject is eligible and that the recipient is not an impersonator. In this way, the community of rights may serve both the individual rights of the subject and the public concern to safeguard and manage health care resources. There still exists a paradox at the heart of biometrics: it is a threat to privacy and a technology of surveillance in identifiable form, but it also is a protector and a technology of privacy in a properly encrypted form (Cavoukian, 1999).

In the domain of e-commerce, non-coercive default rules can be embedded in browser software, such as disabling 'logging' and 'cookie' capabilities, without impeding the use of the browser. Internet Web pages may adopt a common protocol like a window box that can be clicked to erase a visitor's traffic data and thus preclude its secondary use. The Canadian Standards Association (CSA) integrates privacy as a technical quality standard emphasizing the important role of PETs for business policy. The CSA has also proposed a privacy quality standard at the International Organization for Standards (ISO). These standards have been seen by European data protection officials as 'significantly' contributing 'to the protection of fundamental rights and privacy' on an international basis (Reidenberg, 1999, n.28).

While these practices and policies offer positive possibilities for the use of PETs, there are also limitations to PETs and, indeed, to any technical 'solution' to the problems of privacy and security. First, most PETs are built on the perception that within a given transaction there is one party that needs to be guarded. Given the power imbalance noted earlier between corporations and individuals, the assumption is that services should be developed whereby consumers can choose whether and to what extent they wish to identify themselves. This assumption is generally true, but it fails to acknowledge the dominance of B2B (business-to-business) transactions on the Internet. The buyer might well be a potent organization and the seller a small company with a legitimate interest in being protected against the buyer's economic power. The point is that the role of PETs is essentially technical, one

that follows normative ethical decisions about the nature and scope of privacy policy. Whether PETs truly protect the correct subjects and thereby enhance social values is a separate question, especially if we choose information policies that make the wrong sort of communications secure. For PETs also make it possible to maintain a given distribution of organizational power, rather than to empower individuals in their dealings with organizations or to enhance the defence of agency needs and human rights. Given the harsh empirical realities of economic inequality in the informational economy (See chapter 3), we must not assume that PETs will necessarily level the economic playing field.

A second limitation to PETs is related to mobilization, mutuality, and, more generally, the impact of modernity on community and social bonds. Fukuyama (1999) argues that interpersonal ties have tended to be less permanent and looser and to involve smaller groups of people. The weakening of community and civil society occurred simultaneously with the transition to the information age. The process of modernization had led to disturbances in social bonds and identities in the family, the neighbourhood, the workplace, and peer groups. Human beings are by nature social animals, and we should not underestimate the force of mobilization as a social need as much as it is a force for political and economic democracy. The anonymity that PETs entail may well lose its attractiveness, or, conversely, privacy concerns may prove resistant to mobilization attempts. The future will probably be marked, therefore, by two parallel developments: On the one hand, mobilization techniques will become more refined in order to overcome resistance generated from a desire for anonymity; on the other hand, PET designs may have to contain doors or switches by which the subect may remain 'reachable,' provided certain conditions set by him or her are met (Burkert, 1998, 135).

Third, PETs may negatively affect the formation of identity and culture. Identity is always en route, in process. Identity develops in relation to others, not by isolating ourselves from others. What others know about us, in turn, shapes our self-understanding. In this context, information serves agency in the form of identity formation. In order to intervene in this information-identity feedback loop, we must be able to intervene in the process through conversation and dialogue. Communication cannot be achieved without this dialogic dynamic, and, culturally, the identities of persons are affected by the appreciative recognition accorded their works of science, literature, music, and visual arts. PETs

could negatively shape the communicative process and, hence, identity by becoming instrumental systems for managing various masks of the self in different social settings. The broad toleration that characterizes the principle of human rights may entail restrictive implications for certain cultural products pushed on the Internet from cyberporn to hate literature. While probably there should not be censorship in this area, the principle of human rights certainly is not indifferent to the impacts of certain kinds of digital productions on the equal freedom and well-being of persons who suffer harm from them or who are 'objectified' by some other person's conception of additiveness.

Finally, PETs could potentially undermine the need to meet the insecurities of life and our relations with others with basic trust or faith in the possibilities of human rationality and the achievement of ethical goods. We are not referring to the notion of trust as used in encryption policy in relation to 'trusted third parties' or 'trusted CAs.' Rather, we refer to the trust that depends on mutuality and authentic communication. Confidence is a necessary, yet insufficient, element of trust because authentic trust presumes a certain leap of commitment, a quality of faith in the other. Trust still frames the limited knowledge that most of us possess about the technological systems that routinely affect our day-to-day activities. We cannot function in the modern world without trust and the faith implied by trust. As a mode of cognition, however, trust tends to resist a calculative, decision-making logic. The faith implied by trust goes beyond the 'intellect' or instrumental rationality. Our attitudes of trust in relation to specific situations, individuals, or systems are grounded in the psychological security of individuals and groups. Because of this fact, the mutuality that is at the heart of the community of rights can aid human trust without denying that the conditions of modernity inevitably unfold between trust and security, risk and danger. Whether the anonymity at the heart of PETs will enhance or inhibit human trust and social bonding remains an open question.

Conclusion

In this chapter we set forth an argument for the ethical justification and social value of privacy that goes beyond existing philosophical conceptions and, at the same time, corroborates but extends recent Canadian information policy approaches. By appealing to the ethical norms of basic, non-substractive, and additive well-being, as well as to the crite-

rion of degrees of needfulness for action, we have provided far greater ethical specification of norms in relation to Canadian information highway policy and the broader guiding research question concerning how best to strike an ethical 'balance' between individual rights and societal goods and interests.

When evaluated in accordance with basic, non-substractive, and additive goods of well-being and the criterion of degrees of needfulness for action, public concern with practices such as 1-800 caller number identification, telemarketing, telephone solicitation, and even some secondary uses of private consumer information without the data subject's voluntary and unforced consent are practical and ethical harms, but they may not be privacy violations as serious as non-consensual medical and genetic privacy breaches. The former group generally may be classified as breaches of occurrent freedom, whereas the latter tend to be breaches of the agent's dispositional freedom. For freedom also may be differentiated in terms of occurrent or particular freedom and dispositional or long-range freedom. Stated differently, a temporary interference with minor freedoms is ethically less significant than interferences with a person's long-range freedom or highly valued actions. We also must distinguish between freedoms that are essential for action in general and freedoms that pertain to particular actions whose performance or nonperformance does not affect the generic rights to the necessary conditions of action. The ability of persons to unrestricted performance of certain actions is far more important than restrictions to some other types of actions. Thus, the exercise of civil liberties, freedom of movement in general, and choices of certain ways of life certainly are far more important than certain privacy interferences.

Concern about the abuse of genetic information is growing in the light of new knowledge of genes that cause or predispose a person to a disease and where biotechnology companies then rush in to develop a test for it. Clearly, we are here dealing with rights to privacy that bear upon the person's long-range, dispositional freedom. Currently, most insurance discrimination is based on information obtained from medical records. Informed consent is the traditional model for the disclosure of patient information, but it is more of a fiction than a realistic model for control over medical records. Consent is rarely informed or consensual, and it usually protects the interests of everyone except the patient.[13] A key unresolved health privacy problem concerns the use of an identification number. Both record subjects and record keepers need

a uniform standard for identification, and both the Social Insurance Number or a yet to be defined health identification number are candidates. Privacy advocates warn against the use of such a number because of the ease of linking it with other records. The main problem with a health identification number is that it would be widely available to many major government, commercial, and health care institutions, with enormous pressure to use it as an identifier for welfare programs, motor vehicle registration, debt collection, child support enforcement, immigration control, and so forth. Here again, the important issue is the procedural and substantive rules that govern access and use of medical records. Encryption can take us only so far, since it will not solve the problem of insiders who can abuse medical records. Moroever, there are legitimate needs for data linkage such as cost containment, fraud control, and public health functions like child vaccination programs that actually support the basic well-being and productive agency of children. Encryption technologies will surely be helpful, but legislation is not good at mandating specific technological applications that are rapidly changing. Decisions about using PETs to protect medical records are probably best left to those responsible for the records 'with statutory standards limited to requiring that reasonable levels of protection – as defined by technologies actually available in the marketplace at a cost-effective price – be maintained' (Gellman, 1999,142). Those persons responsible for medical records, of course, ought to be individuals with high moral character; if not, the sky remains the limit for medical and insurance information abuse.

DNA screening tests for common conditions such as heart disease, Alzheimer's disease, breast cancer, diabetes, and rheumatoid arthritis are now being developed and surely will be commercially available within the next few years. Whether persons will be tested with their informed consent or will be forced to submit to testing by insurance companies, Heath Maintenance Organizations (in the United States), or Health Canada, decisions need to be made *before* commercial genetic tests are in use. Both the securing and maintenance of basic well-being are potentially at stake in cases where persons are denied work opportunities or medical insurance on the basis of their genetic profile. Denial of life and disability insurance policies that discriminate on the basis of genetic predispositions also violate the human rights to freedom and well-being, even though life insurance is less necessary than ongoing disability insurance, which is, in turn, less necessary than access to life-threatening basic medical insurance.

It may be impossible to know exactly where to draw the line in the case of life and disability insurance, since the business of insurance is, after all, about classifying risk. Cost-benefit analyses and an ethic of care for the protection and promotion of basic human rights will always entail a certain amount of conflict. A universal and national health care system that seeks to provide basic health care coverage is not optional, in accordance with the principle of human rights. Canadians can be proud of their universal health care system, despite the economic sacrifices health care taxation inevitably entails.

Video surveillance rules and health institution rules must serve to protect and foster meaningful consent and the equal freedom and well-being of the persons subject to them, thereby ruling out secondary uses of information and restoring or aiding the mutuality of non-harm prescribed by the PGC. As we shall see clearly in the next chapter, mutuality of trust in the information operations arena ought to stress a more proactive role for effective communication on vital issues of concern. Public safety video surveillance, genetic testing within the limits of voluntary and unforced consent, and even some forms of information warfare practices, might be morally justified if persons acting in accordance with them fulfil their moral duties within the community of rights. In accordance with the consensual procedures of the democratic state, citizens need far better knowledge of the ostensible threats to their medical privacy, public safety, and national security in order to make informed judgments about legislation that might restrict privacy rights through medical data linking, global surveillance practices, and public key infrastructure policies in accordance with the indirect applications of the PGC. Thus, it is to questions surrounding national and international security interests and developments in the field of information warfare that we must now turn.

CHAPTER SIX

Information Warfare

Canadian information highway policy and e-commerce strategy support cryptography policy that encourages the growth of e-commerce, allows software producers to export their products globally within the terms of the Wassenaar Arrangement (see chapter 2, n.7), and contains measures that maintain the capability of law and security agencies to ensure public safety. A problem arises because encryption technologies may be used to hide criminal activity and threaten public safety and national security. Policy makers are concerned that the enforcement of laws and regulations could be hampered without lawful access to evidence pertaining to illegal activity.[1] What is our empirical situation? How far should surveillance and security measures be allowed to go in order to investigate and prosecute informational terrorism, violence, and crimes against domestic and international commercial, financial, and government systems? Do existing privacy and security policies achieve the sought-after 'balance' between individual rights and the public interest? These questions pose some of the most difficult challenges for policy makers, governments, and concerned citizens, because they are directly related to the rise of 'information warfare' (IW) technologies and practices.

We will begin by situating IW within the historical context of the 'revolution in military affairs' (RMA), and by defining recent theoretical conceptions and some actual practices of IW. Because the human right to peace embodies all of the constructive peace and social justice related endeavours of the international community since the proclamation of the UDHR (Alston, 1992), we next link IW practices to international human rights law, on the one hand, and to the indirect application of the principle of human rights, on the other hand. As an

extension of the Principle of Generic Constistency (PGC), we apply classical norms of the justifiable war tradition to IW and ask: Can there be a just information war? After systematically thinking through the role of *jus ad bellum* and *jus in bello* norms in an IW context, we note the limits and possibilities of the justifiable war tradition in the information age. Kant's classical philosophical question must be raised anew: Is a 'perpetual peace' possible? In accordance with the consensual procedures of the democratic state and the principle of human rights, we argue that citizens need far better knowledge of the empirical threats to national security and public safety in order to make informed judgments about legislation that seeks to restrict privacy rights through global surveillance practices and to establish security and intelligence policies that bear upon the protection of the state.

The 'Revolution in Military Affairs'

IW definitions and concepts of IW originate historically in the so-called RMA and the electronic and digitized warfare of modernity. During the past hundred years, armed forces have vastly improved battlefield integration and coordination through technological developments. By the time of the Vietnam War in 1965 modern armed forces utilized a variety of 'electronic, optical, and acoustic sensors such as cameras, television, radar, infrared and sonar' (Van Creveld, 1989, 240). In 1976 General William Westmoreland, commander of the U.S. forces in Vietnam, predicted a revolution in military affairs: 'On the battlefield of the future, enemy forces will be located, tracked, and targeted almost instantaneously through the use of data links, computer assisted intelligence evaluation, and automated fire control. With first round kill probabilities approaching certainty, and with surveillance devices that can continually track the enemy, the need for large forces to fix the opposition physically will be less important ... [A]n improved communicative system ... would permit commanders to be continually aware of the battlefield panorama down to squad and platoon level ... Today, machines and technology are permitting economy of manpower on the battlefield ... But the future offers even more possibilities for economy' (cited in Edwards, 1996, 43).

At around the same time, Soviet theorist Marshal Nikolai Orgarkov was speculating about a revolutionary transformation in warfare (Cohen, 1996; USAF, 1974, 1977; Grechko, 1977). The term 'military technical revolution' (MTR) or, more precisely, the 'revolution in

military affairs' (RMA) denotes the phenomenon in which 'extreme transformations in warfare occurred as a result of the exploitation of technology to achieve ... operational and organizational innovations' (Krepinevich, 1992, 3; Whitaker, 1995; Blaker, 1997). The Soviets were unable to realize the vision of the RMA, but the idea of an integrated battlefield was hotly pursued by the western Allies and the United States Department of Defense. New information technologies would be the means for beefing up NATO's defence of western Europe. Innovative technologies were a qualitative means to the needed 'force multiplier' against a projected, massive Soviet attack. 'Precision-guided-munitions' (PGMs) were a means to raise the nuclear threshold by creating a credible substitute for theatre nuclear weapons. The introduction of PGMs led, in turn, to a new military paradigm and the creation of a global military hierarchy increasingly based on the ability of states to develop, acquire, and use RMA and IW technologies. Only technologically advanced nations are well positioned to exploit the RMA, but some warn about the prospect of a 'Rogue States' doctrine based on the force projection capabilities of RMA technology (Klare, 1991, 1995).

According to Michael Klare, U.S. foreign policy makers are obsessed with what they believe are a handful of 'rogue states,' particularly Iraq, Iran, Libya, Syria, and North Korea, which pose major threats to U.S. and western security (Klare, 1995). The Rogue States doctrine appears to be a product of a determined Pentagon effort to create a new foreign threat to justify military spending in the wake of the Cold War, and at a time when social programs are being severely cut. Under the direction of General Colin Powell, then chairman of the Joint Chiefs of Staff, the J-5 (Strategic Plans and Policy) Directorate of the Joint Chiefs of Staff worked throughout the winter and early spring of 1990 to devise the Rogue States doctrine based on a non-Soviet threat. The doctrine has enjoyed bipartisan support in the U.S. Congress and has been pushed by a politically defensive White House. Unless it is tempered by domestic or international developments, the Rogue States doctrine might well embroil the United States in another Gulf War–like military clash with a rising Third World power.

With the end of the Cold War in 1989, military cutbacks, and the miniaturization of nuclear weapons, the concept of an RMA gained even more momentum. 'Operation Desert Storm' (the Gulf War) became identified as 'the first information war,' given the Allied advantages in information acquisition, processing, and exploitation (Mann, 1994;

Campen, 1992). The Gulf War encouraged an emphasis on versatility, deployability, lethality, visibility, and agility, all driven by high-tech weapons and communications and information systems (Vuono, 1991; Gray, 1997).[2] The information edge provides a new condition of possibility for the projection of 'soft power,' defined as 'the ability to achieve desired outcomes in international affairs through attraction rather than coercion' (Nye and Owens, 1996, 21). Soft power works by information sharing and by convincing others to effect democratic transitions; to protect new democracies; to prevent and resolve regional conflict; and to fight international terrorism, crime, drug smuggling, proliferation of weapons of mass destruction, and global environmental degradation. The goal of soft power is to produce a desired policy outcome by shaping other nations' preferences by means of information, thus obviating the need for costly traditional economic and military resources.[3]

Information Warfare: Definitions and Conceptions

Definitions and conceptions of IW are numerous and complex. They invoke a variety of theoretical foundations of military strategy, economics, and psychology. Warfare may be understood as the set of all lethal and non-lethal activities undertaken to subdue the hostile will of an adversary or enemy. According to this definition, warfare is not necessarily synonymous with lethal warfare, and warfare does not require a declaration of war or a state of war. Lethal and non-lethal tools of warfare may be understood as 'weapons' used against external adversaries, but IW weapons may also be employed against internal constituencies. The concept of IW is a relatively new term, which has found its way into the national and international security lexicon. The use of information *in* warfare is hardly new, of course, but the emergence of IW and its prominence is directly tied to the information age revolution and the emergence of a new kind of warfare and 'cyber' soldier (Walters, 1998b; Waller, 1995).

The term 'information warfare' surged in the early 1990s among military strategists, then languished somewhat because of a lack of conceptual clarity. A major concern has been that enemies might exploit the tools and techniques of the information revolution to harm national critical information infrastructures. In the document *Information Warfare and the Canadian Forces*, the Department of National Defence (DND) defines information warfare as 'actions taken to achieve a goal by influencing and controlling adversary information, computer processes and information systems, while protecting one's

own information, computer processes and information systems' (IWCF, 1996). Along with DND and its electronic intelligence agency, the Canadian Security Intelligence Service (CSIS), the Royal Canadian Mounted Police (RCMP), and the Treasury Board have formed an interdepartmental committee on 'information operations' (the term is used synonymously with information warfare, though the former carries a less aggressive connotation) to assess, prevent, and respond to IW attacks on Canadian government agencies and businesses. Such attacks might be launched by groups like the Hong Kong Blondes, a group of Chinese hacker dissidents based in Canada (Bronskill, 1999).

The United States Department of Defense (DOD) describes IW as 'information operations (IO) conducted during times of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries' (DOD, 1996a, 1-1). The de facto world of IW includes:

- Command-and-control warfare, or strikes against an enemy's head and neck (nodes and links);
- Intelligence-based warfare, or the design, denial and protection of systems that seek to dominate battlefield awareness;
- Electronic warfare, in the electromagnetic spectrum;
- Psychological operations, perception management, or information used to change opposing wills, including operations against the national will, opposing commanders, troops, and cultural conflict);
- Hackerwar, or software-based attacks on information systems;
- Economic info-warfare, or the manipulation of information exchanged in trade (either denial or exploitation) as an instrument of state policy; and
- Cyberwar or the use of information systems against the virtual personas of individuals or groups. (Libicki, 1995)

Leon Trotsky once remarked: 'you may not be interested in war, but war is interested in you' (cited in Toffler and Toffler, 1993, 252). So true – for we want to forget about the twin threats of political totalitarianism and nuclear annihilation that haunted humanity throughout the Cold War. The fact that in any given year approximately thirty wars of various sizes are raging on the planet from Chechnya to Chiapas seems far removed for most Canadians; the threat of war has a quaintly archaic ring. But whether or not we are interested in war, military strategists are preparing for the next information age war. The old adage – *si vis pacem para bellum* – still applies, but with this difference: 'If you

want peace, prepare for [*information*] war.' The world of information warfare is a world where logic bombs, computer viruses, Trojan horses, worms, sniffers, non-nuclear high-explosives, precision-guided-munitions, stealth designs, radio-electronic combat systems, new electronics for intelligence gathering, interference, deception, high-powered microwave weapons, futuristic designs for space-based weapons, and automated and robotic warfare all are being discussed, developed, and deployed.

Now a sceptic might ask: If information warfare ranges from command-and-control warfare, to computer hacker warfare, to various psychological warfare tactics,[4] can IW really mean anything at all? Or is IW merely a linguistic repository for the difficult issues national security and military institutions face in a post-Cold-War context? Strategic IW threats to major critical information infrastructures may appear to be the material of information warfare science fiction, but readers should not be sceptical of the costs of network security and strategic IW planning. Millions of dollars are being allocated to provide new databases, network architectures, advanced software, and other sophisticated capabilities, all under the rubric of IW (Rothrock, 1997).

Netwar and Cyberwar

One way of simplifying the concept of IW is to reduce its components to 'cyberwar' and 'netwar' (Arquilla and Ronfeldt, 1997a). Cyberwar refers to conducting and preparing to conduct *military* operations according to information-related principles. Netwar, by contrast, involves *societal-level conflict* waged through communications on the Internet or Intranets. Netwar is the domain of organized hackers, who steal proprietary designs, corporate merger and acquisition secrets, and new products coming out of research labs. The San Francisco based Computer Security Institute (CSI) polled 520 specialists at corporations, government agencies, financial institutions, and universities. They estimated the total loss from computer crime at more than $236 million dollars (CNN, 1998). The global cost of computer-based crime exceeded the combined value of all other property crimes, and losses from credit-card fraud totalled $88 million for Canadian banks (Foot, 1998). Netwar applies to struggles most often associated with low-intensity conflict by terrorists, drug cartels, black-market proliferators of weapons of mass destruction, and even governmental antagonism to political activism by means of counter-intelligence programs (Wehling, 1995).

Netwar as a type of 'cyberspace security' and safety issue has become a growing concern (Hundley and Anderson, 1997). Computer hackers engage in 'social engineering' to obtain passwords and confidential and credit information by means of deception. Many hackers are juveniles and university students, but expert hackers pose serious threats to businesses and national security. Information brokers commission hackers to steal proprietary information and resell it to foreign governments or business rivals of the organizations hacked. Meta-hackers, as the Greek prefix implies, go beyond typical hackers by surreptitiously monitoring other hackers. They exploit the vulnerabilities identified by the hackers they monitor and effectively and instrumentally use other hackers as tools to attack networks. Elite hackers form closed clubs and look down on ordinary hackers employing commonly used attack tools. Elites develop their own hacking tools, thereby gaining a technologically based camaraderie and, in turn, appreciation for their prowess from their peers. Darksiders use hacking techniques either for financial gain or in order to create malicious destruction. Their ends are more material and destructive than classic hackers, whose motivation traditionally has been to gain a feeling of achievement and authority. Banks, brokerage houses, and investment firms in both the United States and the United Kingdom have had to pay off criminals who threatened to attack their computer systems. On-line terrorists have amassed up to $400 million worldwide by issuing threats that they will destroy the computer systems of companies that do not meet their monetary demands (Shelton, 1996). Whereas hackers attempt to legitimate their electronic trespass by some putative appeal to instrumental values, darksiders intentionally cross the line for malign reasons such as greed or wanton destruction. A malicious meddler who tries to discover sensitive information by poking around (e.g., 'password hacker,' 'network hacker') is correctly termed a 'cracker.' There may well be no fully adequate technological solution to the problem of hacking, and organizations will need to concentrate on minimizing the damage caused by attacks.

It is often argued that the early digital hackers of the MIT artificial intelligence lab in the 1950s and 1960s, the populist, hardware hackers in California in the 1970s, and the young game hackers of the early 1980s are really not evil individuals. They promoted a philosophy of sharing, openness, decentralization, and getting one's hands on a computer at any cost, in order to improve the machines and the world (Levy, 1984). In Levy's view, the 'hacker ethic' is a gift to the world.

Whatever the early origins of authentic hackers, today we should reject the term 'ethical hacker' as an oxymoron. It lends itself to a hacker ethos that justifies computer break-ins by claiming that hackers are merely making use of idle machines or that such unauthorized break-ins serve a greater utilitarian purpose of pointing out security gaps in information systems. These putative moral justifications for hacking are flawed and are invoked far too often in order to legitimate immoral hacker behaviour (Spafford, 1992).

Information Warfare Weapons

Information networks require computer software to manage them. If the software is corrupted, the system will fail. Several different types of program have been intentionally designed to interfere with the proper function of computers. 'Trojan horses' are programs that are harmful because they insert corrupt information into a program so that, for example, it makes payments to a bogus bank account or otherwise profits the culprit. 'Logic bombs' are programs that execute some program code, usually harmful, once a set of conditions has been fulfilled. A typical bomb might be programmed to crash a computer or to erase hard disk drives. 'Viruses' include self-replicating computer code that requires execution and they carry negative side effects. Viruses attempt to spread by hiding for as long as possible before executing the bad effects. Thus, computer viruses resemble biological viruses, which are most infectious during an incubation period when the victim manifests no outward symptoms. Viruses can successfully subvert a mainframe computer within an hour, and international networks with thousands of computers can be disrupted by illicit intrusion very rapidly (Andrews, 1989). The Michelangelo computer virus, which was designed to wipe out the hard disk drives of infected computers, disabled over 65,000 computers worldwide (Spinello, 1995, 190). 'Worms' are programs that are similar to viruses, but they replicate in their entirety and do not need a carrier program. The difference between a worm and a virus is that a worm normally seeks out idle machines, while a virus preys on active systems.

Transnational Informational Crime

As noted in the introduction, the global criminal economy involves drug trafficking, weapons trafficking, trafficking of nuclear material,

smuggling of illegal immigrants, trafficking in women and children, trafficking in body parts, and money laundering. Flexibility and versatility are keys to the success and expansion of global crime, and networking between criminal organizations and within organizations has become the standard modus operandi. Distribution networks supply goods and services to local gangs, just as major criminal organizations employ ruthless means for enforcing deals such as intimidation, torture, kidnapping of family members, and killings. They maintain a security apparatus that includes a large network of law-enforcement agents, judges, and politicians all of whom are on their payroll. In order to escape political repression, criminal groups form strategic alliances, thus forming convergence points across national boundaries. While rooted in tradition and identity, local crime groups are now combined with flexible networking. The organizational strength of these sinister strategic alliances, based on networked alliances and tactics of information warfare, makes global crime a fundamental actor in the economy and society of the information age (Castells, 1998, 166–205).

Transnational criminal organizations (TCOs), such as the Colombian drug cartels, Chinese triads, and Japanese *yakuza*, undermine civil society, destabilize domestic politics, and undercut the rule of law. Most democratic governments are forced to work within a framework of rules, but TCOs, by definition, work outside the rules. They can be ruthless in carrying out their policies and do not have to be democratically accountable (Williams, 1997). RCMP Commissioner Philip Murray maintains that bikers, the Mafia, and Asian-based organizations all are on a roll in Canada. 'Because of organized crime,' declares Murray, 'we have higher taxes. We have businesses at a competitive disadvantage because others have used laundered money to set up their competition' (Murray, 1998, A4).

In the twenty-first century we will likely see more terrorist and criminal gangs attempting to use computer hacking techniques to neutralize military, police, and security services. The research agency Dataquest estimates that spending on computer security software is going to balloon from $6.3 billion in 1997 to $13 billion by 2001 (Malik, 1998). The international move to outlaw money laundering is a consequence of the liberalization of cross-border capital movements resulting from free trade, deregulation, and globalization. Canadian law enforcement organizations try to stop credit-card fraud and computerized transfers of so-called 'black' (i.e., tax evasion) and 'dirty' (i.e., illegal) money between Canada and other nations. Some RCMP officers

view their attempts to enforce legal rights and obligations as stymied 'by privacy laws and the need for search warrants, full disclosure of investigative methods, and the like' (German, 1995, 11).[5]

The Protection of Critical Information Infrastructures

Why is cyberwar drawing so much attention in recent years? Canada and the United States are vulnerable to cyber attacks because they depend on electronic information systems more than many other countries. American fear of physical and information attacks in the wake of the World Trade Centre and Oklahoma City bombings, as well as numerous cyber attacks on U.S. military installations, is given voice in the *Report of the US President's Commission on Critical Infrastructure Protection*. The commission concludes that waiting for disaster is a dangerous strategy and that 'now is the time to act to protect' the future (PCCIP, 1997, 6). If a threat is a capability linked to a hostile intent, then an offensive cyber attack would be the perfect utilitarian means to a hostile intent. Cyber attacks are less risky than sabotage, assassination, hijacking, or hostage taking. Unlike conventional warfare there is a *low cost* for developing nations or terrorist groups. The right set of skills and less than $10,000 of computer equipment can turn anyone into an information warrior – hence the fear of an electronic Pearl Harbor (GAO, 1996).

The ice storm that struck eastern Ontario and Quebec in 1998 made Canadians more aware of the physical, social, and economic stakes of shutting down the powergrid. A full-fledged cyber attack, however, whether or not combined with a physical attack, would disrupt not only the powergrid but the flow of money, air traffic and transportation, and other information-dependent items. At the same time, and quite ironically, strategic military analysts are intrigued with information warfare because it is seen more as a military *opportunity* than as a threat. The idea is to improve defence capabilities against hostile attack and to defeat any aggressors at the lowest possible cost. Information warfare would be the cyber equivalent of the neutron bomb, leaving buildings and people standing, while destroying information systems.

Global Surveillance Practices: The ECHELON Network

Human rights scholars have raised concerns about *global surveillance* practices as a form of netwar for the past few years (Walters, 1998a),[6] but these admonitions have, at times, been met with scepticism. The report

to the director general for research of the European Parliament's Scientific and Technological Options Assessment (STOA) Programme Office, *Development of Surveillance Technology and Risk of Abuse of Economic Information*, should make believers out of the most ardent sceptics (EP, 1999, vol. 1/5).[7] Its authors consider the state of the art in communications intelligence (COMINT), that is, 'of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to Comint targeting and selection, including speech recognition.'[8] They survey technology assessment issues in electronic surveillance, the legality of the interception of communications under international, European and national law, and the perception of economic risks that arise from the vulnerability of e-commerce to interception. COMINT and its highly automated UKUSA English-speaking avatar for processing ECHELON, was set up at the beginning of the Cold War in 1947, but it gradually grew to include a network of surveillance-interception stations spread across the globe. ECHELON is a global surveillance system that allows spy agencies to monitor most of the world's e-mail, fax, telex, and telephone communications. The intelligence group is led by the United States and includes Great Britain, Canada, Australia, and New Zealand. Former intelligence agent Nicky Hager first blew the whistle on the secret workings of New Zealand's Government Communications Security Bureau (GCSB) and the United States National Security Agency's (NSA) global network of intelligence gathering (Hager, 1996, 1996–97). The NSA and GCSB are bound together under the five-nation UKUSA 'Signals Intelligence Agreement' that includes the Government Communications Headquarters in Britain (GCHQ), the Communications Security Establishment (CSE) in Canada, and the Defence Signals Directorate (DSD) in Australia. With the demise of Communism in eastern Europe, intelligence agencies searched for a new justification for their surveillance capabilities in order to protect their prominence and bloated budgets (Goodspeed, 2000). Their solution was to redefine the notion of national security to include economic, commercial, and corporate concerns.

Designed and coordinated by the NSA, ECHELON is used for non-military targets such as governments, organizations, businesses, private individuals, politicians, trade unionists, and private companies. ECHELON has indiscriminately intercepted vast quantities of communications using five global surveillance stations targetting international telecommunications satellites, non-Intelsat communications (including the Leitrim, Ontario, station), and land-based systems consisting of

water cables under the oceans and microwave networks over land. Hager (1996) suggests that computers or 'dictionaries' perform real-time searches through the piles of intercepted messages for pre-programmed keywords that are, in turn, linked back through a four-digit code. Thus, the code 1911 might refer to Japanese diplomatic cables from Latin America handled by CSE. Or the code 3848 might be Nigerian political communications, and 8182 could be messages about distribution of encryption technology. These messages are then sent to the five agency headquarters. ECHELON has been used to collect terrorist, economic, and especially political and military intelligence that assists allies to pursue their interests. Anyone and anything can become a target of the system. British intelligence insiders who felt that they could no longer remain silent about the 'gross malpractice and negligence' of the system, note how telephone calls of three charitable organizations – including Amnesty International and Christian Aid – were directly targeted. Hager further suggests that Canadian embassy collection operations listen to telephone calls using voice recognition technology to monitor keywords. Individuals, organizations, and governments that do not use encryption are easy interceptions for ECHELON.

Are these allegations fact or fantasy? In February 2000 the European Parliament opened an international meeting on spy practices, claiming that ECHELON had methodically violated privacy rights and that the rapid rise of surveillance technologies presents a serious threat to liberties in Europe. The EP's Civil Liberties Committee accused Britain of aiding the United States in conducting economic and commercial espionage on a grand scale and at the expense of its European partners. Although Europe appears to be concerned about global electronic espionage by Americans, its very own police forces are drawing up, in conditions of utmost secrecy, a project for telephone and Internet surveillance (Rivière, 1999). Indeed, one of the top priorities of the French intelligence service is industrial spying. The director of the French secret service from 1970 to 1981 observes that spying is very profitable: 'It enables the Intelligence Services to discover a process used in another country, which might have taken years and possibly millions of francs to invent or perfect' (Schweizer, 1993, 13). Duncan Campbell, author of *Interception Capabilities 2000*, defines STOA's key findings as follows:

1. Comprehensive systems exist to access, intercept and process every important modern form of communications, with few exceptions ... ;

2. Contrary to reports in the press, effective 'word spotting' search systems automatically to select telephone calls of intelligence interest are not yet available, despite 30 years of research. However, speaker recognition systems– in effect, 'voiceprints' – have been developed and are deployed to recognise the speech of targeted individuals making international phone calls;
3. Recent diplomatic initiatives by the United States government seeking European agreement to the 'key escrow' system of cryptography masked intelligence collection requirements, and formed part of a long-term program which has undermined and continues to undermine the communications privacy of non-United States nationals, including European governments, companies and citizens;
4. There is wide-ranging evidence indicating that major governments are routinely utilising communications intelligence to provide commercial advantage to companies and trade. (EP, 1999, vol. 2/5, 5)

Because strong encryption is one way of curbing illegitimate uses of global surveillance capabilities, the ECHELON system poses some probing questions. To what extent have global surveillance imperatives driven governmental cryptography policy? What role will covert or overt surveillance imperatives play in future policy? Has cryptowarfare become the extension of politics by other means? To what extent are international encryption policies influenced by strategic military and intelligence interests, especially the emergence of 'strategic information warfare' policy?

Strategic Information Warfare Rising

Charles Swett of the United States Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict, at the Pentagon, was one of the first American analysts to offer a 'strategic' assessment of the Internet, long before official IW policy (Swett, 1995). Swett notes that new political parties operating though the Internet will emerge and make the political scene more complex. Multiple and simultaneous 'political wars' will occur in cyberspace with party information vulnerable to disruption by false messages and the proliferation of encrypted messages. The monopoly of the traditional mass media will erode. The filtering and slanting of news by editors, television networks, and newspapers will give way to direct consumption of unanalysed information, which will result in a greater cognizance of

current events. Government officials will be inexorably drawn into the Internet, which will be used as a tool of statecraft by national governments.[9] The Internet will play an increasingly significant role in international conflict. Text-oriented e-mail will be replaced by video/audio messages. Video footage of military operations now may be captured by inexpensive, hand-held digital video cameras and operated by locals. In a conflict situation, unedited data files may be uploaded and may instantly reach millions of people over the Net. As a consequence, public opinion and calls for action, or the termination of action, may be formed before national leaders have a chance to take positions or react to Net developments. This development will add to the burden that is already placed on military commanders, whose actions are subjected to an unprecedented degree of scrutiny.

Subsequent to Swett's study, the RAND corporation's policy document on Strategic Information Warfare (SIW) highlights the low entry cost for state-sponsored IW, the blurring of traditional boundaries between public and private interests and between warlike and criminal behaviour, and the loss of traditional geographic boundaries in cyberspace (Molander et al., 1996). The authors point to an expanded role for psychological operations or 'perception management' due to increased powers of deception and image-manipulation, as well as to a diminished effectiveness of classical intelligence collection and analysis methods. Difficulties surrounding tactical warning and attack assessment will plague cyberspace warriors, not to mention the building and sustaining of coalitions. Most important, in their view, is the vulnerability of infrastructures involving the control of electric power, money flow, air traffic, oil and gas, and other information dependent items in comparison with earlier 'in-theatre' targets.

The problems raised by the emerging potential of SIW led to a second RAND study in 1998 commissioned for the U.S. Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence). The goal of the project is 'to formulate a common DOD strategy and policy framework for addressing the challenge of strategic information warfare' (Molander et al., 1998, xiii). In this second study the authors recognize that the future of the United States national security strategy will be profoundly affected by the evolution of national and global information infrastructures. The danger is not so much that adversaries will try to destroy key national strategic assets as that they will attempt large-scale or massive disruptions of the energy, telecommunications, transportation, and finance sectors. SIW weapons are

especially useful in so-called 'asymmetric' strategies, where adversaries avoid directly challenging conventional battlefield superiority by indirect means of attack or threat involving some combination of nuclear, chemical, biological, highly advanced conventional, and SIW weapons. The two most significant threats of SIW tools and techniques entail threats to national economic security, on the one hand, and national military strategy, on the other hand. The United States is the global leader in the development and exploitation of information systems and thus has the potential to be an offensive SIW superpower. Given its political, economic, geographical, and technological position in the world, however, the United States is also a natural target for an SIW attack. E-commerce transactions, cyber payments, disruption of delivery of telemedicine and government communications over the GII, all present potential targets for an SIW attack. Offensive SIW could hold at risk a country's 'central nervous system' or critical infrastructure networks. It is noted in the RAND study that SIW is ethically far more 'sensitive' than information operations that support conventional military warfare, and the assumption is that conventional warfare may violate the moral norm of non-combatant immunity in a way that SIW targeting policy does not (Molander et al., 1998).

Information Warfare and International Human Rights Law

Despite the foregoing definitions, conceptions, and emerging IW and SIW policy approaches, many IW problems appear to lack concrete operational solutions. This is true, a fortiori, concerning the legality of IW in the light of international human rights law. The year 1998 marked the fiftieth anniversary of the Universal Declaration of Human Rights (UDHR). The adoption of the UDHR by the United Nations General Assembly in 1948 came on the heels of the Second World War and the demise of the principle of unrestricted state sovereignty. The formulation and adoption of the UDHR were motivated in large part by the effects of mass warfare such as carpet bombing and Nazi genocidal practices. Over fifty years later, we are witnessing the rise of the 'virtual state' and the emergence of a different kind of warfare using IW weapons (Campen, 1992). The post–Cold War period has shifted national security concerns from use and deterrence of nuclear weapons to use and deterrence of IW weapons, involving nation-states, individuals, and groups not attached to governments (Whitaker, 1995; Libicki, 1996). The *ethical* aspects of information warfare have been treated only curso-

rily, if at all (Arquilla, 1999; Kuehl, 1999; MacNulty, 1996; Schwartau, 1994).

In Humanitarian international law the 'law of armed conflict' refers to the rules governing two nation-states already engaged in armed conflict (*jus in bello*), not to the norms governing the justificatory basis for resort to conflict (*jus ad bellum*) (Schindler and Toman, 1973). The information age poses new questions for the law of war and international treaties that takes up and goes beyond earlier Geneva Protocols (Protocol, I, II, 1977; Kalshoven, 1991). How the law of armed conflict and international human rights treaties may or may not proscribe the scope and use of information warfare to a large extent turns on a definition of information warfare. In what sense is information warfare 'armed conflict' or 'armed force'? Under shared article 2 of the Geneva Conventions the term 'armed conflict' was specifically chosen over the term 'war' because of its broad scope, but 'armed conflict' seems inadequate to reach the kinds of IW conflicts possible today. Given the various dimensions of IW just noted, IW would be an activity engaged in both during peacetime and during conflict. Calling a peacetime activity information *warfare* may unnecessarily suggest the applicability of the laws of war, which is probably why both the Canadian DND and the United States Army prefer the term 'information operations' to information warfare (Aldrich, 1996).

Is IW, or should it be, considered a use of force prohibited by article 2(4) of the United Nations Charter? Todd Morth, professor of law at Case Western Reserve University, answers in the affirmative. His definition of information warfare is 'state activity which has an incapacitating effect on the ability of the owners of any information network to use or manage that network. This includes, but is not limited to, telecommunications, electrical power systems, gas and oil storage, transportation, banking and finance, military forces, and emergency services including medical, police, fire and rescue, to use or manage that network' (Morth, 1998, 571). This definition appears to be legally significant insofar as it focuses on actions engaged in by *states* to incapacitate information networks by means of physical destruction of the network, information degradation or corruption, or inundation of the network with so many requests that it ceases to function, the so-called denial-of-service attack. Netwar, computer crime, and espionage are not included in this definition. The transnational nature of IW, the difficulty of determining when and if an IW attack has occurred, and the weakness of unilateral solutions (e.g., the extraterritorial application of

domestic laws) all work to underline the difficulties of prohibiting IW in international law. The UN Charter was designed to allow states to peacefully resolve disputes without the resort to force. The charter sought to resolve the limitations of the Kellogg-Briand Pact by means of article 2(4): 'All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations' (cited in Claude and Weston, 1992, 414). Article 51 of the Charter exempts the prohibition of article 2(4) in the case of self-defence and collective self-defence. Thus, 'Nothing in the present charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.' (UN Charter, art. 51, cited in Claude and Weston, 1992, 412) Despite article 51 and other UN resolutions creating the right to use force in support of self-determination movements, the UN reaction to the Iraqi invasion of Kuwait reaffirmed the legal support of the international community in viewing article 2(4) as applicable in the Gulf War (which some analysts consider the first information war). The key issue in the application of article 2(4) as a legal basis for sanctioning an activity is the determination of whether or not that activity is truly 'armed force.' General consensus holds that economic coercion, such as sanctions or embargoes, does not violate article 2(4), although some argue that economic coercion does indeed constitute 'force' according to the article (Paust and Blaustein, 1974). One argument for the applicability of article 2(4) to IW is similar to the logic that biological and chemical weapons constitute a use of 'force' (Brownlie, 1990, 362). Just as biological and chemical weapons should be viewed as force because they destroy life and property and cause widespread destruction, so, too, IW has the ability to destroy lives and property and therefore should be viewed as 'armed force.' We agree with this argument because IW would not be bloodless and would cause real physical damage and the destruction of property and would even harm or kill persons in potential violation of the principle of human rights.

Another important issue in attempting to apply the law of armed conflict to IW is the problem of establishing where events occur in cyberspace. Jurisdiction does not really matter in information operations. If IW is defined as a state activity, jurisdiction is not an issue, because only states can turn to international law. The International Court of Justice or the UN Security Council still would have to decide, however, if a country suffered from an IW attack violating article 2(4). The test for where and whether an IW attack occurs should be as expansive as possible. It might be reasonable for states to use the 'passive personality principle' when establishing jurisdiction. The principle authorizes states 'to assert jurisdiction over offenses committed against their citizens abroad. It recognizes that each state has a legitimate interest in protecting the safety of its citizens when they journey outside national boundaries' (Morth, 1998, 598, n.202). The principle of 'collective self-defence' is also invoked to alleviate concerns about jurisdiction and spatial location when IW is confronted. Under this principle, any state can intervene to defend any other state victimized by an attack. The physical location for an attack is irrelevant, since one or more states can aid another state that has been illegally attacked. In this way, articles 2(4) and 51 of the charter work together to codify the rights of individual and collective self-defence. 'The ability of states to exercise these powers in response to an IW attack,' Morth concludes, 'provides a critical deterrent element. Article 2(4) allows the international community to condemn IW and preserve the community's right to strike back against those who employ IW. This combination provides the most effective means of discouraging states from using this weapon' (Morth, 1998, 599–600).

Information Warfare and the Principle of Generic Consistency

Human rights are as much moral rights as they are legal rights, and we do well to recall that the principle of human rights, the Principle of Generic Consistency (PGC), has both 'direct and indirect' applications (Gewirth, 1982, 60ff.). In the direct applications, the PGC's requirements are imposed on the actions of individual agents. Actions are morally right and the agents fulfil their moral duties when they act in accordance with the generic rights of their recipients as well as of themselves. Thus, murder and slavery are morally wrong because they inflict basic harms on their recipients in ways that violate the equality of generic rights. Individual criminal hacking actions would be pro-

scribed by the direct application of the PGC. In the indirect applications, the PGC's requirements are imposed on social rules and institutions. These are morally right, and persons acting in accordance with them fulfil their moral duties when the rules and institutions express or serve to protect or foster the equal freedom and well-being of the persons subject to them. Thus, by the indirect applications, recipients may even be coerced or harmed, but their generic rights to freedom and well-being are not thereby violated, because the rules and institutions that require such correction or harm themselves are justified by the PGC.

The indirect applications of the PGC are of two kinds. The 'procedural' applications derive from the PGC's freedom component and provide that social rules and institutions are morally right insofar as the persons subject to them have freely consented to accept them or have certain consensual procedures freely available to them. The 'instrumental' applications derive from the PGC's well-being component and provide that social rules and institutions are morally right insofar as they protect and support the well-being of all persons equally. The procedural applications may be either 'optional' or 'necessary.' They are optional insofar as persons consent to form or to participate in entirely voluntary associations. The procedural applications are necessary insofar as individual consent operates as a general decision procedure. Here, consent entails using civil liberties to provide the authoritative basis, through elections and other consensual methods, of specific laws or governmental officials.

The PGC's instrumental applications may be either 'static' or 'dynamic.' The static applications, embodied in the so-called 'minimal state' with its criminal law, serve to protect persons from occurrent violations of their rights to basic and other important goods – including the rights to life, physical integrity, and reputation – and to punish such violations. The PGC sets standards or limits for how this protection is to operate, so that only persons who have violated the rights of others are to be punished, all persons must be equal before the law, trials must be fair, habeas corpus must be guaranteed, and human punishment must not be cruel, vindictive, or inhuman. The dynamic applications, embodied in the welfare state or 'community of rights,' serve to provide longer-range protections of basic and other rights where these cannot be obtained by persons through their own individual efforts.

Now the point that we must stress is that any potential deprivations

inflicted in the case of justifiable information warfare, or by imprisonment for crimes like murder, might not be morally wrong because the deprivations to individual freedom are inflicted by agents of organizational institutions responsible for enforcing institutional social rules, such as police and military personnel, in accordance with the indirect application of the PGC. Having acknowledged this point in theory, we must also emphasize that institutions with their social rules and practices may also be prohibited by the PGC as unethical, as in the case of corrupt officials and tyrannical governments. For institutions and their rules must also conform to the principle of human rights. In this way, conformity to the PGC takes precedence over the direct harmfulness entailed by the corresponding actions serving to enforce consensually agreed upon rules and policy.

Ethical Norms and the Use of Information Warfare Weapons

How, then, might such conformity and precedence be established in the case of information warfare? One major historical approach has been to invoke norms of the western 'justifiable war' tradition. Military, security, and intelligence institutions generally presuppose an affirmative answer to the question: Can there be a 'just' information war? The sceptic, however, might well ask: Once IW weapons and an extensive organizational structure for conducting IW is in place, will it be possible *not* to have a 'just' information war?

Western 'just war' theory has essentially used the logic of Augustine, Aquinas, Grotius, and others to articulate a right of self-defence or defence of the innocent in the absence of a centralized international order. The development of biological, chemical, and nuclear weapons in the twentieth century has placed the 'just war' doctrine under severe strain. It is at least arguable that the historical function of the doctrine was not to legitimate the state's claim to *compétence de guerre*, but rather to limit the state's proclivity to settle disputes by lethal means. The tradition begins with a strong *presumption against war*, which is binding on all, and then examines when this presumption may be overridden in the name of a peace that protects human dignity and rights. For war to be morally justified it must meet two sets of criteria. The right to go to war (*jus ad bellum*) is established by the criteria of just cause, legitimate authority, comparative justice, right intention, last resort, probability of success, and proportionality of goal. If and when these seven stringent norms have been met, then the actual con-

duct and means of war (*jus in bello*) also are subject to scrutiny by norms of proportionality and non-combatant immunity.

In the light of this tradition and as an extension of the indirect application of the PGC's normative rules, we will now turn to a hypothetical application of the traditional norms in our new IW context. This move is necessary if we are to avoid the problem of moral indeterminancy and if we are not to avoid the difficult challenge of ethical specificity on the grounds that it would be better not to think about IW strategy and policy at all. Unfortunately, the ethicist cannot prescind from the emerging policy debates, since, as noted earlier, the reader may not be interested in war, but war is interested in the reader. In what follows, then, *we are not proposing an argument for a justifiable information war.* In fact, we will raise as many questions as we answer in the process of ethical specification and seek, by means of the movement of thinking itself, to raise the questions of the very limits of ethical norms and the pressing human and social problem of new forms of warfare in the information age.

Jus ad Bellum Norms

Just Cause. Warfare has traditionally been justified only for the sake of protecting innocent human life, preserving conditions necessary for decent human existence, and/or for the securing of basic human rights. It is arguable that once just cause is established, other *ad bellum* norms tend to fall by the wayside. However, the just cause norm is not, in theory, impossible to meet in the context of information warfare. Ought the United States, Britain, or Canada use information weapons to slow Saddam Hussein's development of biological and chemical weapons? Without judging the justice or injustice of the Gulf War, our question is not irrelevant, given the fact that more than a million Iraqis died – 567,000 of them children – as a direct consequence of the Gulf War and subsequent economic sanctions (Kelly, 1997). Would a cyber attack on Iraq's power plant or other critical infrastructures have had any less devastating consequences on the Iraqi people (Mann, 1994)? Here again, we must not assume that information weapons are bloodless simply because they are non-conventional weapons.

Dan Kuehl, professor of military science at the United States National Defense University, argues that the ethical assessment of a just cyberwar turns on the question of *when* the action is being taken. If a country is at peace, an act of cyberwar could range from being a

criminal act to being an act of information age statecraft. If a country is at war or in a state of 'armed conflict,' then such a move could be interpreted as a legitimate act of belligerency. Where does one draw the ethical line between preparation, pre-emption, or prevention, on the one hand, and outright belligerency, on the other hand? For example, computer 'chipping' involves modifying or altering the design or use of integrated circuits for purposes other than those originally intended by the designers. Would 'chipping' constitute a hostile military or intelligence action if the chips are sold, with the intention to deceive, to adversary nations? Or, if espionage now probes an adversary's databanks and control system functions, is this passive, ethically correct intelligence conducted in accordance with so-called 'national technical means'? Or should this type of espionage be considered an act of war, especially if a virus or logic bomb is planted in a computer in order to lower shields on demand?

Professor John Arquilla of the Naval Postgraduate School in Monterey, California, argues that cyberwar makes it possible to conduct *preventive strikes* against an enemy because of its disruptive rather than destructive nature. A preventive strike might be ethically allowable if (1) strikes were aimed strictly at military targets (e.g., command and control nodes) to avoid or generally limit damage to noncombatants; (2) the amount of IW employed was enough to deter or substantially slow an attacker without being so excessive as to have dire economic or social effects; and (3) the good done by preventing an adversary from being able to start a particular conflict, or type of conflict, could be said to outweigh the wrong of using force beyond the realm of clearly definable self-defence. Thus, in his view, '*jus in bello* considerations may be seen as mitigating a serious *jus ad bellum* constraint on information warfare' (Arquilla, 1999). Arquilla's interpretation of 'preventive' war as a morally licit means falling under the umbrella of 'just cause' is certainly not beyond dispute. His serious, strategic guidelines may reveal how quickly *in bello* norms would be given de facto lexical priority once the justice of cause is assumed.

Legitimate Authority. This norm states that war must be initiated and carried out by legitimate authority and tied to the common good. Private groups or individuals may not act on their own. Nation-state institutions tend to be hierarchical, whereas transnational organizations are networked. Castells's (1998, 166ff.) analysis of the global criminal economy suggests that the net flow of power is increasingly out of

the nation-state into non-state actors. National governments not only have less control over currencies, markets, and the movement of persons and commodities across borders, but they may be losing their monopoly on war (Nichiporuk and Builder, 1997). The low cost for cyber attacks by transnational criminal groups and terrorists places severe strains on legitimate authority. Would military and intelligence agencies have any recourse other than to wage IW against non-state actors? Would Canadian IW policy and practice conflict with or exceed the imperatives of the national will in the name of 'national security' and thus potentially undermine privacy protection in both the public and the private sectors? What impact will IW policies and practices have on other rights and values such as liberty, freedom of expression, and freedom of association?

Comparative Justice. Comparative justice delegitimates a crusade mentality and stresses that no state ought to act on the basis of its own absolute justice. The question of which side is sufficiently 'right' in a dispute to override the prima facie norm against war is difficult to ascertain under normal conditions, that is, when the actors are nation-states with deeply rooted identities and histories. With the rise of non-state information warfare actors, what role might this norm play?

Right Intention. Right intention is related to the norm of just cause and the reasons noted earlier for overriding the initial presumption against war. Traditionally, right intention has meant pursuing peace and reconciliation, avoiding unnecessarily destructive acts, and not imposing unreasonable conditions like unconditional surrender. Paradoxically, information warfare may make war more thinkable because the declared intent is to disrupt or deny an adversary's information or information systems, not to kill or destroy human life. This intent seems intuitively right and good. We do well to recall that moral evil often hides behind the appearance of value and rarely appears as a serial killer. The 'road to hell is paved with good intentions,' as the old saw goes, and actions have unforeseeable effects whose moral implications cannot be predicted in advance.

Last Resort. Moral justification for the resort to war requires that all less violent alternatives to settling the dispute be exhausted. Strategic IW analysts morally justify cyber attacks on the premise that *physical* violence now defines 'last resort.' The ability of individuals and groups to

act exceedingly fast with disruptive information weapons may work against meeting the moral requirement of last resort under the consensual procedures required by the community of rights.

Probability of Success. This norm has functioned to prevent irrational resort to force or hopeless resistance if an outcome will be disproportionate or futile. The norm is difficult to apply under normal conflict situations. Here again, thinking about the probability of success may make information warfare more thinkable if nation states or other actors believe it is easier to succeed with information weapons than with conventional force. Conversely, small groups, crusaders, terrorists, or conspiracy theorists may act on the grounds that they have a far greater probability of success in meeting their ideological goals and in not getting caught if they use information weapons rather than other tactics.

Proportionality of Goal. This norm asks: Is the damage inflicted and the costs incurred by war proportionate to the good expected to result from the resort to force? Information warfare may weaken the just war tradition's prima facie presumption against war, since, assuming just cause, the argument will surely be that if damages can be limited, say, to cultural disinformation or disruption of computer processes and information systems, then this is far more proportionate to the goal of national security than resort to force at higher, physical levels of destruction.

Jus in Bello Norms

Proportionality of Means. Proportionality of means weighs the harm caused by a tactic against the tactical advantages gained by this means. The *in bello* judgment of proportionality *does not* balance the harm caused by a particular tactic against the overall good defended by the conflict as a whole. If that were the case, then *in bello* proportionality would have the effect of removing all restraint from the use of force in defence of a just cause. No good end, however, can justify means that are evil in themselves, for example, targeting non-combatants or executing hostages. This would lead to what Michael Walzer, quoting General Sherman, calls the 'war is hell' doctrine: 'War is entirely and singularly the crime of those who begin it, and soldiers resisting aggression (or rebellion) can never be blamed for anything they do that brings victory closer' (Walzer, 1977, 32).

In contrast, *in bello* proportionality seeks to weigh the harm caused by a tactic in a just war against the tactical advantages gained by the means used. What happens to the norm if a cyber attacker strikes Canadian infrastructure assets, but has no information assets or very few of his own? Would the use of a non-information retaliatory weapon strike then violate proportionality, assuming that the attacker can be identified? Electronic warfare, like directed energy-type weapons, also falls under the category of IW noted above. While it is one thing to disable the electronics of a fighter plane or air defence radar during wartime and another thing to disable the electronics of a civilian airliner or air traffic control radar, even if done during wartime, there is no morally significant distinction between the use of a laser-guided bomb or an electronic device to destroy an adversarial target. Consider, for example, the destruction of the Iraqi power plant in Baghdad during the Gulf War: the immediate loss of life may have been less with a HERF Gun (Bunker, 1996), but the long-term collateral damage or harm to civilians might be less. Moreover, if attacks are aimed at the knowledge or belief systems of adversaries, are these information attacks not as unpredictable as attacks aimed at the physical destruction of property, combat equipment, or human beings? Unless *consequences* are considered and evaluated in advance, information attacks could include counter-attacks against friendly information systems that are indistinguishable from the 'collateral damage' caused by the information analog of friendly fire. The 'stochastic' effects of information warfare could well violate *in bello* proportionality (Szafranski, 1995).

Martin Libicki, a senior American military IW strategist, maintains that conventional forces survived the nuclear era because nuclear war was unfightable. Information warfare, on the other hand, is 'eminently fightable' and holds out the prospect of a conventional military victory without mutual suicide (Libicki, 1996). We are less optimistic. The Russian Ministry of Defence analyst V.I. Tsymbal notes: 'Russia will reserve the right to respond with weapons of mass destruction to any use of information warfare against it or its armed forces' (cited in Porteous, 1997, 20; Thomas, 1996). Here again, we see the way in which use of IW weapons might be erroneously encouraged on grounds of proportionality of means.

Non-combatant Immunity. This criterion states that non-combatants must not be injured in a 'just' war. Non-combatant immunity has

always posed serious ethical problems for the 'just war' doctrine. It is an empirical fact that 'from 1500 to 1990 the worldwide total number of civilian deaths from war has been higher than military deaths' (Sivard, 1991, 25). While it is easy to criticize the destruction of civilian life both during and after the Gulf War, it must also be recalled that Saddam Hussein violently used chemical weapons against innocent Kurdish men, women, and children in northern Iraq in the mid-1980s. The crisis in the Gulf War was simply not an issue of 'blood for oil,' as some suggest, but also concerned serious human rights violations of non-combatants (Miller and Mylroie, 1990; Al-Khalil, 1990). But who is a 'combatant' in the information age? The cyber soldier with sophisticated high-tech weapons surely is. What about the computer hacker who covertly installed a sniffer program on computers at Griffiss Air Force Base in Rome, New York? He turned out to be a sixteen-year-old boy from Britain, who liked to attack '.mil' sites.

We argue that information warfare blurs the ethical distinction between civilians and combatants even further because a very high percentage of military communications travel along civilian owned and operated systems. A cyber attack aimed at a nation's powergrid, transportation, communications, and/or financial infrastructures could never be morally acceptable. School children, hospital patients, the elderly, the ill, the average worker producing goods not directly related to military purposes, farmers, and other non-combatants would suffer from such an attack. The question thus arises: 'If Bits and Bytes offer an alternative form of exerting national power or defense than bombs and bullets, which ethical mandate should be followed? That which attempts to hold separate the military from the civilian, no matter what the overall cost in blood and suffering, or that which attempts to minimize the destructiveness and duration of the conflict, even at the expense of affecting systems or functions that are clearly and unquestionably civilian?'(Kuehl, 1999) This question assumes that IW would, in fact, result in less combatant blood and suffering, even though it affects civilian systems and functions. In a century in which there has been obliteration bombing, atomic attacks on Hiroshima and Nagasaki, MAD or Mutually Assured Destruction nuclear policies, and the use of chemical weapons against non-combatant women and children, it may be even easier to legitimate non-combatant deaths with the good intent to minimize both the destructiveness and duration of conflict in the information operations arena.

A 'Just' Information War?

The foregoing 'just war' normative analysis should not be construed as legitimation of information war. Indeed, we have argued that paradoxically, the framework may even contribute to the legitimation of IW. We do believe, however, that everyone who has enquired out of 'prudence, piety, or pity into the propriety of the use of force' has constructed an analogue of the 'just war' doctrine (Potter, 1969, 61). It is difficult to avoid categories of moral reasoning that reflect some aspect of the historical 'just war' doctrine, and this is the case even for those who oppose war on religious pacifist grounds (Zahn, 1980) or those who appeal to non-violent means of resistance to evil on secular or pragmatic grounds (Sharp, 1965). The normative force of the *jus ad bellum* and *jus in bello* categories is difficult to avoid and certainly accords with the further specification of the indirect application of the PGC. During the Cold War nuclear arms race, ethicists increasingly questioned the use of nuclear weapons on the basis of utilitarian, deontological, and just war ethical foundations. As moral philosopher Kai Nielsen wrote regarding the question of the use of nuclear weapons in defence of western values, 'the human devastation to "victor" and "vanquished" alike is just too great to make it a morally tolerable option. On moral grounds it is intolerable and on prudential grounds it is insane' (Nielsen, 1985, 59). To a lesser extent, ethicists also challenged the morality of nuclear deterrence as a long-term basis for peace (Hardin et al., 1985; MacLean, 1984; Walters, 1990).

We will examine the ethics of information warfare deterrence in depth in the next chapter, but the fact is that the classical, philosophical problem of war has not been eradicated by technological developments of the information age. In fact, the post–Cold War order and the revolution in military affairs may actually have made the world less stable now than during the Cold War in a world of individual infowarriors in search of destructive connectivity (O'Berry, 1998). For, whether conducted in agrarian, industrial, or informational modes of development and history, war does not generally manifest exteriority and the other as other; instead, war 'destroys the identity of the same' (Levinas, 1969, 21).

After the Second World War the international community of nations understood clearly that physical force between states could be excluded only if international law came to prevail. The central idea

now, as then, is to subordinate force to law. Where force is legal within the mimimal, democratic, or international state, the goal is to use only the minimum force necessary to subdue a 'rogue' actor, or actors rebelling against the community of other states. A state of law exists only if force was risked in founding a legal order, and domestic and international law is effective only if the decisions of authorities are legally enforced against all possible resistance. The idea of an objective, universally valid law is quite pervasive, but the realization of international human rights law can be realized only if opposing parties, convinced of the truth of their own positions, are willing to submit to a higher legal authority like the United Nations. Countries have to admit that legality is better than force. If countries do not recognize a higher legal authority and think that they have right on their side, then war will often ensue. By this logic we come up against a crucial limit of the 'just war' or justifiable war tradition: For it does not help us to differentiate between aggressive and defensive wars, 'just wars' and 'holy wars,' offensive IW and defensive IW if such judgments are not pronounced by a superior legal authority. They remain partisan judgments, even if the parties are not identical with states but cut across them, as is likely to be the case in the information age. Indeed, at least twelve countries are formally developing the capability to conduct attacks on information networks, and twenty-six other countries might be developing the capability (Morth, 1998, 569); and these figures do not account for non-states actors. The ultimate deciding factor in war is force, not law. As such, the idea of law can prevail only by allying itself with force. Legal norms are ultimately grounded in moral norms, but law is real only because it has the backing of force. Countries maintain themselves by the use or threat of force, which, as we have seen, is a 'limit situation' of the human condition. Can the violent struggle for existence be converted into a communicative, loving struggle for Existenz? As Kant asked: Is 'perpetual peace' possible?

Is 'Perpetual Peace' Possible in the Information Age?

Might a rational resolution to the problem of warfare be historically achieved in the information age? Is a 'perpetual peace' possible now that information warfare weapons may be able to lower the possibilities of conventional, atomic, biological, and chemical warfare? Two hundred years before the appearance of the UDHR, Kant wrote his famous essay, *On Perpetual Peace*, in which he refers to 'just war' theo-

rists as those 'sorry comforters' who are frequently quoted in order to *justify* military aggression (Kant, 1971 [1795], 103). Kant's disdain for 'just war' thinkers seems partially justified, since there would appear to be few instances of a state ethically proscribing war by appeal to 'just war' ethical norms, and, as we have suggested above, contemporary IW practices and strategies paradoxically may make IW war more likely. We fail to grasp the meaning of the information age revolution if we do not see the communicative challenges it poses to our modes of thinking about warfare and international community and peace with justice. Let us also recall that for Kant, the passage from war to peace, from the old politics to the 'new politics,' requires relinquishing the reductionist mode of instrumental rationality or the 'intellect' in favour of a larger rationality or reasonableness. If politics says, 'Be ye wise as serpents,' morality qualifies this by adding 'and guileless as doves.' For Kant's 'moral politician,' the problems of political, international, and cosmopolitan right are not *technical tasks*, as they are for the 'political moralist.' Reasonableness makes intelligible the idea that morality does not yield to Jupiter, the god of war, because force is always subject to destiny.

Shall we, then, beat swords into fibre-optic cables in the information age? The 'technological imperative' insists that whatever can be done by technological means will, in fact, be done (Rapoport, 1986). The military environment offers a particularly tempting milieu for the imperative's manifestation, even as the state needs a credible long-term 'enemy' to keep funds flowing for production and procurement processes. IW strategies and planning are not immune from the technological imperative. At the dawn of the nuclear age, Albert Einstein passionately called for a new mode of thinking, a more 'reasonable' mode that is more expansive than scientific rationality. 'The invention of the atomic bomb has changed everything except our modes of thinking,' he wrote, '[and] thus we drift toward unparalleled catastrophe.' Commenting on the adage *si vis pacem para bellum* ('If you want peace, prepare for war'), he noted that when one prepares oneself for war, one always finishes by actually making war (cited in Alston, 1992, 203). IW practices may very well make war more 'thinkable' by making it easier to override the prima facie presumption against war and to invoke in its behalf the norms of right intention, probability of success, proportionality, and non-combatant immunity. Kant knew that human dignity and human rights must be held sacred and that politics 'must bend the knee to reason and morality.' If these precepts are not

honoured, and as long as nations have not eliminated war as an instrument of policy, then biological, chemical, nuclear and/or information warfare have a chance of triumphing sooner or later.

Conclusion

In this chapter we have argued that encryption technologies and security policy open onto broader questions and ethical concerns surrounding national and international security and, in particular, the ethics of information warfare policy and IW weapons use. We know that encryption technologies are being used to hide global criminal activity. We also know that global surveillance and security practices risk harming individuals and violating the principle of human rights if they are allowed too much licence, as appears to be the case with the ECHELON system. When intelligence agencies spy on ordinary citizens or breach privacy unlawfully, they upset the balance between individual rights and the public interest. On the other hand, wired nations are highly dependent on e-commerce and communications, and cryptography is and will continue to be the centerpiece of communication security and the main countermeasure to communications intelligence.

The communicative challenge of the information age is no more apparent than in the domain of IW practices and policies. Just as good personnel security is essential to communications security, which, in turn, makes a contribution to information operations security, so too, good communications and the mutuality that is at the heart of the community of rights are essential to navigating the threats and challenges of privacy and security in a world of information warfare.

In accordance with the indirect and procedural application of the PGC, its requirements may be imposed on social rules and institutions that serve to protect or foster the equal freedom and well-being of the persons subject to them. Recipients may even be coerced or harmed, entailing certain restrictions to privacy, without necessarily violating generic rights to freedom and well-being, because the very rules and institutions that require such correction or harm may be justified by the PGC. The defence of citizens' basic rights to freedom and well-being and to life and physical security will remain ethical priorities in the information age and in accordance with the criterion of degrees of needfulness for action. At a minimum, citizens need greater knowledge of the empirical threats to their privacy and security in order to contribute to good policy making. The knowledge and informed con-

sent required to establish procedurally justified rules and practices become more delicate in the area of security and intelligence.

Fortunately, we have not yet seen an example of strategic information warfare in its pure form, and no nation appears, as yet, to have attacked another nation's computers using information. It also seems that no 'politically motivated attack on computers using information alone has been made by terrorists or other non-national groups' (Diffie and Landau, 1998, 103). Past performance is no guarantee of future possibilities. The history of human conflict and warfare may not give us grounds for great optimism when viewed solely from the perspective of instrumental rationality or the 'intellect.' It remains to be seen whether or not human beings will move closer to a global community of human rights that can serve to mitigate human conflict and the avoidance of warfare, a point to which we shall return in the conclusion to the book. In the interim, and as we move towards Kant's 'perpetual peace,' it appears that we have a breathing spell. Because policies that entail the use of IW weapons now are being devised and implemented, deterrence policies and practices may or may not make the actual use of information weapons less possible. We turn, therefore, to an ethical analysis of information warfare and deterrence, with a view to the reasonableness and mutuality that must stand at the heart of the community of rights.

CHAPTER SEVEN

Information Warfare and Deterrence

While security, military, and intelligence strategists have been preparing for an information age war by rethinking organization, doctrine, strategy and tactics (Arquilla and Ronfeldt, 1997b), they are just beginning to think about the relation between information warfare (IW) and deterrence. The idea of information warfare deterrence (IWD) poses, from the outset, definitional and conceptual challenges related to the constituent terms, information warfare and deterrence. Our use of the term 'information warfare' throughout this chapter assumes the definition of IW articulated in the last chapter. If we are to make use of practical reason to answer the question as to what policies we ought to follow in an information age, then it is necessary to distinguish further between practical rationality, reasonableness, and motivation in relation to IW policy. Is IWD both rational and reasonable? In this chapter we argue that a policy of IWD could be both rational and reasonable only if it were able to establish and stabilize alternatives that do not involve the threat of noncombatant murder and that do not violate the principle of human rights by imposing substantial risks of harm without consent. In a post-Cold-War world, where the distinction between combatants and noncombatants is increasingly blurred by military and civilian communication networks, we should not depict IWD along the same lines as nuclear deterrence policy. The challenge is to move beyond political realism, idealism, and even a necessary pragmatism, to a mutuality of human rights and a moral reasonableness that makes both trust and security possible. The problem of deterrence in the information age brings us to the limits of politics and technology for solving the problem of war, and it becomes first and foremost a challenge of rational selfhood. The condition of possibility for human trust and real security

requires a suprapolitical revolution in our ways of thinking and acting on a daily basis that is commensurate with the privacy and security challenges of the information age. This revolution entails a human transformation towards ethics and rationality whereby 'mutuality' becomes operative within a global community of rights.

Information Warfare Policy: Clarifying the Terms of the Debate

Canadian Forces policy defines IW as 'actions taken to achieve a goal by influencing and controlling adversary information, computer processes and information systems, while protecting one's own information, computer processes and information systems' (IWCF, 1996). The de facto operational world of information warfare is quite large. If we follow the conceptual map of Martin Libicki (1995), senior fellow with the U.S. Institute for National Strategic Studies Center for Advanced Concepts and Technology, IW includes command-and-control warfare, intelligence-based warfare, electronic warfare, psychological operations or 'perception management,' hackerwarfare- or software-based attacks on information systems, economic information warfare, and cyberwar. We prefer John Arquilla and David Ronfeldt's notion of 'cyberwar' that emphasizes command and control warfare (C^2W) rather than Libicki's definition of the use of information systems against the virtual personas of individuals or groups. We are using the terms 'information warfare' and 'cyberwar' synonymously throughout this chapter. 'Netwar' struggles associated with low-intensity conflict by terrorists, drug cartels, or black-market proliferators of weapons of mass destruction cannot easily be decoupled from IWD practices, since the boundaries between the military, law enforcement, security and intelligence agencies, and the commercial sector are radically breaking down. The spectrum of IW theory and doctrine ranges from IW as a powerful force multiplier for kinetic warfare not substantially different from industrial-age war; to small, distributed combat cells knitted together by a robust infrastructure; to conflict in the purely digital realm consisting of remote attacks on critical information nodes, links, and databases to disrupt, exploit, disable or deny service (DOD, 1996b; USAP, 1994).

The concept of deterrence existed in military strategy long before the recent revolution in military affairs (RMA). It was actually the Soviets, especially Marshal Nikolai Orgarkov, who began the discussions regarding an RMA. It took on new meaning, of course, with the advent

of atomic and hydrogen weapons after 1945, and it is taking on new meaning in our present situation. Deterrence involves the dissuasion of a potential adversary from initiating an attack or conflict, often by threatening unacceptable retaliatory damage. Deterrence seeks to prevent other parties from doing something that they have not yet done; it is a military means to achieve an essentially uncertain psychological effect. Deterrence may best be seen as a game of strategy or a 'strategic dynamic' that revolves around shared information and rationality. Deterrence is a state where 'the challenger seeks to produce as much freedom of action as possible by devising technical, tactical, and operational innovations that reduce (ideally to zero) the prospective costs of actions against an opponent. The deterring state or organization focuses on confounding the challenger's search for acceptable alternatives by developing a comprehensive response that approaches a guarantee of inflicting unacceptable costs on any state or organization that initiates an offensive challenge' (Harknett, 1996, 93). What constitutes 'unacceptable' damage, what precisely is to be deterred, and what constitutes extended deterrence in an IW context are emerging questions. What, in short, is the fit between information warfare and deterrence? IW and deterrence appear to form a logical pair in strategic military thinking. On other levels, they seem to be orders of magnitude apart. A common supposition among military analysts seems to be that both concepts are highly relevant to the post-Cold-War era even if conflict has been transformed from a bipolar global competition to multi-sided local and regional conflicts or 'third wave' war forms (Toffler and Toffler, 1993). In their summary findings from a workshop 'Information Warfare and Deterrence' held at the U.S. National Defense University in 1996, Richard Hayes and Gary Wheatley note the following:

- IW covers a huge domain while deterrence is a narrow topic. Their relationship is spotty – highly relevant on some topics, marginally so on others, and not at all relevant in many areas.
- Deterrence is part of IW only when the attacker is known (or can be discovered), the defender has a credible capability to threaten important interests of the attacker, and the attacker cannot defend those interests.
- A visible set of defenses is the beginning point for deterring attacks on important computer systems. Attacks are essentially instrumental acts that will not occur if the attacking party perceives little opportunity for success.

- Media warfare (i.e., countering an adversary's propaganda) can put enormous time pressure on decision makers, particularly when an authoritarian state adversary, with little or no necessity for consultation, targets unsuspecting, easily manipulated publics. (Hayes and Wheatley, 1996)

Finally, it is increasingly necessary to differentiate 'declaratory' and 'action' IWD policies and the historical development of IWD policies over time. The direction in which one moves in an IW deterrence strategy is morally significant. The historical development of IW is linked, of course, to larger 'military technical revolutions' and the 'revolution in military affairs' (Whitaker, 1995; Krepinevich, 1992, 1994). Because IW deterrence is in a nascent stage of development, it is difficult to determine what constitutes declaratory or action deterrence policy. Hayes and Wheatley point out that 'The United States already has basic policies in place that serve as effective deterrents in many circumstances. In essence, information warfare attacks on the United States are deterred by the same policy that deters other types of attack. Acting under its rights as a sovereign state, the United States stands ready to respond to any attack on its interests with all appropriate means, including law enforcement as well as military capacity' (Hayes and Wheatley, 1996, 4). General Habiger has concluded that 'In the future, weapons may take different forms – perhaps energy, perhaps information – but these new weapons may be just as devastating as nuclear weapons in their impact ... Deterrence will continue to be an indispensable element of national strategy to ensure that conflict does not take its most violent, destructive forms' (Habiger, 1997).

Instrumental Rationality, Reasonableness, and Motivation

What can and should be done in order to avoid the dangers of cyberwar? Rationality and reasonableness are two main concepts of practical reason.[1] Like notions of the 'intellect' or Kant's *Verstand* (chapter 1), *instrumental rationality* entails calculating the most efficient means to a given end. Because ends are usually, though not always, self-interested, instrumental rationality is a feature of self-interested action, action that must take into account the empirical landscape. Instrumental rationality is an application of inductive inference. Calculating a means-ends relationship is simply a species of inferring from causes to effects, which involves probabilistic generalizing from past experience

to its necessary causal connection. To say that the criterion of instrumental rationality is concerned with the pursuit of self-interest is to say that the scope of these selves may vary from individuals, to groups, to nations. In addition, the 'state' may entail the ruling group in each nation or span to include the whole population. In the context of information warfare, the self-interest with which rationality is concerned is the national interest and, in turn, security from an offensive IW attack. National interest also includes the central value of freedom, both personal and political.

Reasonableness, in contrast, is more expansive than instrumental rationality or the 'intellect.' It consists in impartial consideration of the human rights and interests of individuals affected by given actions or policies, that is, in mutual positive concern for the rights of others. Reasonableness is an application of deductive inference. It appeals to the principle of non-contradiction, which states that what is right in one case must be right in any relevantly similar case; or, again, that the rules you apply to yourself must apply to all other individuals who fall under those same rules. The opposition between instrumental rationality and reasonableness is a version of the traditional conflict between egoism, or an exclusive preoccupation with self-interest, and morality, especially the moral quality of justice. Throughout the ages, various philosophers have sought to remove or to a certain extent mitigate this conflict by showing that it is indeed rational to be reasonable. In the *Republic* (IV, 444), Plato held that it is rational to be reasonable, because it is in the agent's own self-interest: being reasonable is the only way to be mentally healthy. Hobbes (1982 [1651]) argued, on more pragmatic grounds, that it is irrational to be unjust, because one cannot deceive all of the individuals who would be adversely affected by one's own injustice (*Leviathan*, chapter 15, paras 4ff.). There are, of course, difficulties incurred by these attempts and others at reconciling instrumental rationality and reasonableness.[2]

The Principle of Generic Consistency (PGC) requires that individuals 'act in accord with the generic rights of your recipients as well as of yourself.' The 'reasonable self' accepts such a principle because he or she is aware of one's own agency needs and rights, and has a sense of personal responsibility for their fulfillment (Gewirth,1988). The reasonable self takes due account of the agency needs of other individuals, respecting their rights as well as his or her own, maintaining a certain equitableness or mutuality of consideration between the self and others, as required by the universality of human rights. Rights and

obligations must be embodied not only in individual actions, but also in social and political institutions that constitute a community of rights. The emphasis on individual rights not only is compatible with the common good, but requires a conscientious concern for the common good in both its distributive and collective meanings. In its 'distributive' meaning, common good means that some good is equally common to, shared by, or distributed among all the members of a community. In its 'collective' meaning, common good means that the good in question pertains to the collectivity as a whole, but not necessarily to its individual members taken separately. The collective meaning of the common good is precisely relevant to the meaning of a community that is constituted by and is the very protector of human rights. The obligation and responsibility of military service in a morally justifiable war constitute one form, among others, that support for the common good by the reasonable self might take on.

Motivation functions differently for instrumental rationality and reasonableness. Individuals and groups are usually, if not always, motivated by self-interest. If instrumental rationality is the efficient calculation of the means to self-interested ends, then it follows that motivation is directly built into the use of or appeal to instrumental rationality. This is not the case with reasonableness. To be sure, individuals and groups may and often do have strong moral motivations that have a direct and perdurable impact on military policies. It is often the case, however, that in pursuing their own interests, individuals and groups are not motivated to give direct consideration to the interests of others.

This contrast between the fully motivational character of instrumental rationality, on the one hand, and the incomplete or negative motivational character of reasonableness, on the other hand, has implications for IWD in the same way that it does for deterring 'weapons of mass destruction' (WMD). The solution to the problem of modern war might seem to be based in common sense: we need simply to stop production of weapons of mass destruction, destroy those already produced, and enter into serious and sincere negotiations with a view to a lasting and just peace. Evolving IW weapons should be spared the kind of arms race we saw during the Cold War. International disagreements ought to be handled not by the force of arms, but by impartial consideration of each conflict on its own terms and with due concern for the human rights and interests of each side.

Why has such a reasonable solution to the problem of war not been

adopted? Among other reasons, it has not happened because the perceived and effective motivation or political will for its adoption is lacking. Mutual distrust of Americans and Russians fuelled the arms race for over forty years, and this same distrust is operative today between numerous nation-states, groups, and individuals, as revealed in the encryption policy debates noted above. Distrust is not merely external to networked organizations, but internal as well. Indeed, the greatest 'hackerwar' crimes are often done by so-called 'insiders,' or those who work within a given firm, organization, or government. The motivational pull of narrow self-interest threatens the motivations individuals derive from their rational recognition of the reasonableness and mutuality required by the principle of human rights. Thus, the nation-state must have coercive laws, uniformly enforced, that threaten punishment to individuals who, out of narrow self-interest, violate the requirements it sets up in accordance with human rights and responsibilities. Similarly, if the confrontation over emerging IW is to receive a solution, it must be both practically effective and morally reasonable.

Is a policy of IWD rational for all actors involved? It is at least arguable, as proponents of the policy of nuclear deterrence have argued in the past, that IWD is, indeed, rational for each side. A state can be trusted to act, insofar as it can, in what it considers to be its own best interests. Such actions by other nations also imply that they will act so as not to be subjected to offensive IW. If a hostile nation were to attack, then, according to the policy of IWD, and assuming a credible threat of IW retaliation, the other country would, in fact, be subjected to offensive IW. Precisely because of this policy, one can trust a hostile nation not to attack. By parity of reason, the other country may also trust that another country will not attack it or its allies. Therefore, because of its invaluable contribution to the avoidance of IW and its deadly consequences, IWD is rational for each side.

The ironic aspect of this deterrence argument is that two adversary countries' paramount, yet distinct, interests in security now actually become a common interest. The argument states that it is precisely the two countries' desire to avoid an offensive IW attack that provides this coincidence of interest. Without, say, mutually assured information denial, degradation, and disruption, there would be no common interest. So, the argument goes, because of the mutuality of interest involved, IWD is not only rational but reasonable in its effects, even if its primary motivation is not reasonable but only self-interestedly and instrumentally rational.

This argument for IWD may be graphically illustrated in reference to the so-called Prisoner's Dilemma. When viewed solely from the standpoint of rational self-interest, the primary interest of two states in conflict is said to consist in offensively IW 'bombing' the other without being bombed in return. Mutual abstention from IW 'bombing' is only second best. Mutual IW 'bombing' is third best. Finally, being 'bombed' by the other side is the fourth best. On this model, the logic is that Canada or the United States must suppose either that another country or transnational criminal agency will information 'bomb' or that they will not. If the other side IW bombs, then making a counter-attack is better than doing nothing, because the attacker may think it can be pulled off with impunity. On the other hand, if the enemy nation does not commit offensive IW, then our offensive IW is better than not engaging in information war, because in this way we can do away with outsider threats once and for all. Hence, it is better, according to this logic, for Canada or the United States to maintain and use an offensive IW capability rather than not to maintain and use one. The other country thinks the same way, of course, and follows its self-interest. By following its own narrow self-interest and engaging in offensive IW, however, each state paradoxically does less well for its self-interest than if it were actually to cooperate.

Strategic Information Warfare Deterrence and the Prisoner's Dilemma

The paradox of the Prisoner's Dilemma reveals that the rationally best solution for each side is to cooperate with the other side in reducing tensions and keeping IW weapons reduced, but continuing mutual distrust and ruptures in communication lead to policies of non-cooperation and self-aggrandizement. Narrow self-interest has the de facto consequence of being rationally worse for each side. It is the policy of IWD that prevents the scenario of each side's bombing the other, thus guaranteeing that the upper right and lower left boxes of the Prisoner's Dilemma will not be effective, so that a policy of IWD is rational for each side.

An objection against this attribution of rationality to IWD is that deterrence is self-contradictory. IWD policy states, in effect, that 'If you want to prevent the use of IW weapons, then you should credibly threaten to use them.' As is the case in the paradox of nuclear deterrence, however, intention to use and prevention of use seem to run in opposite directions. The *end* (the prevention of an IW attack) and the

		Information Warrior Country B	
		IW Bomb	Don't IW Bomb
Information Warrior Country A	IW Bomb	3,3	1,4
	Don't IW Bomb	4,1	2,2

means (the credible threat to use virus, logic bombs, and other IW means) are opposed. Leaving aside for the moment whether there is a morally significant difference between the *intent to use* and *actual use*, if the threat is to be credible, then one must be prepared and actually intend to do the very thing one is trying to prevent being done, namely, use IW weapons. This means-end paradox contains a mode of rationality. For while the means of threatening to use IW weapons contain components conceptually opposed to the end of prevention, they are also causally effective in promoting or achieving the end. So, despite its means-end paradox, IWD policy has elements of rationality.

This rationality is limited for several reasons. First, it assumes that the information warriors on each side can always be trusted to be rational. Leaders are only human and may make IW mistakes happen by accident. Leaders may also be driven to unreasoning fury by what they perceive to be insults or threats. IW attacks aimed at the knowledge or belief systems of adversaries are just as unpredictable as attacks aimed at the physical destruction of property, combat equipment, or human beings. These are what Szafranski (1995) means by the 'stochastic effects' of IW.[3] Unless IW effects are considered and evaluated in advance, a cyber attack may not have the desired effect. Indeed, an adversary's response could include counter-attacks against friendly information systems that are indistinguishable from 'collateral damage' caused by the information analogue of 'friendly fire.'

A second reason for the limited character of IWD policy's rationality bears on the relation between threat and execution. Assume that the United States or Canada credibly threatens to subject another country to IW 'bombing' if it attacks. If this threat were actually carried out, it may well be suicidal unless it is 100 per cent effective. The other country would probably have enough IW weapons to launch a devastating counter-attack that could destroy a large part of the information infrastructure of North America. Such disruption would not be bloodless. Moreover, the other country may rationally attack with weapons of

mass destruction. Russian Ministry of Defence analyst V.I. Tsymbal has stated '*Russia will reserve the right to respond with weapons of mass destruction to any use of information warfare against it or its armed forces*' (Porteous, 1997, 20; emphasis added). Whether the retaliation of a massive cyber attack were carried out with either counter-IW weapons or WMDs, it would surely lead to great suffering and destruction. For IWD to work, the threat of retaliation must be genuinely credible to the other side. This need for credibility, as is the case in nuclear deterrence, rules out mere bluffing. If IWD exists with a certain amount of ambiguity, mixed signals, or uncertainty, then IWD's stochastic effects may create a dangerous instability. A partial disruption of a military network will not preclude the rest of the military force from achieving its offensive goals. Therefore, the initial deterrent threat directed towards the other's connectivity must be substantial or it will not be seen as prohibitive; yet the greater the connectivity, the greater its lethality. Dominance in cyberwar can always be 'contested' both before and after war begins. As Richard Harknett notes, 'Command, control, communications, computer, and intelligence (C4I) assets are susceptible to disruption and failure. The employment of computer viruses, electronic disinformation, or direct destruction of sensing equipment could therefore become increasingly prevalent as the importance of connectivity increases' (Harknett, 1996, 7).

There is a third reason for limiting the rationality of IWD. National defence is designed to keep the political community autonomous, free, and safe from physical or virtual attacks on its freedom and well-being. A rational policy goes to the very heart of the reason for states. We assume that defence policy is underwritten by the strongest means-ends rationality possible. But do we adequately account for *non-rational* or even irrational elements in policy making? The 'bureaucratic politics' model (Nossal, 1995) portrays defence policy making as crowded with numerous individuals in different roles and capacities. The various 'players in positions' have differing conceptions of national interest or national goals. These particular interests are based on the agency or unit to which they are attached, as well as to the personal interests of the individuals involved. The bureaucratic politics model is concerned with how these very different interests interact, how the conflicts work themselves out, and how competing power bases and authority carry the day. The point to note is that this mix of players tends to produce policy outcomes that are often far less rational than we like to admit if we are honest with ourselves.[4] So, while

IWD may be rational in the short run, it would be irrational to rely on it in the long run, especially if the use of weapons of mass destruction is an integral part of IWD.

Now we may ask: Is a policy of IWD morally 'reasonable'? While the criterion of instrumental rationality was concerned with the security interests of one country alone, the criterion of reasonableness concerns the mutual interests of Canada and other countries, especially where basic human rights and well-being are at stake. The political application of reasonableness requires 'mutuality' of consideration in the relations between governments, of governments to their citizens, of governments to the inhabitants of other countries, and between individuals in accordance with their generic rights of agency. But the mutuality entailed by the community of rights is not a merely formal relation of equality between two actors such as entailed by a policy of 'mutually assured information destruction' or MAID. Reasonableness entails a substantive, positive consideration for the rights of others, as for oneself, and in accordance with the moral concern that all humans, as actual or prospective agents, be enabled to live lives of dignity, self-fulfilment, and mutuality of respect. Reasonableness seeks to move beyond a common interest based on the threat of MAID, distrust, and fear.

One of the strongest moral objections against Cold War nuclear deterrence was that it potentially threatened the lives and basic human rights of non-combatants in other countries as well as in Canada and the United States. Has our empirical situation changed so radically? No; and traditional morality has always held that if it is morally wrong to bomb innocent persons, then is also morally wrong to intend or to threaten to bomb them. It matters not whether the bombing is done with conventional, nuclear, or information weapons. A policy of IWD entails, by definition, just such an intention or threat, especially when the intent is tied to a full-blown cyberwar policy or even aggressive economic IW.[5] Thus, IWD policy cannot be morally justified, since, far from being reasonable, it is simply a policy of indiscriminate harm that would violate *jus in bello* proportionality and discrimination should it fail.

Numerous attempts have been made to avoid this conclusion about the morality of nuclear deterrence based on the ethical link between intention and action. One distinction offered as morally relevant is the distinction between possession and intention. The contention might be that mere possession of IW weapons is morally permissible, while actually intending to use them is not. If there is not a conditional inten-

tion to use IW weapons, however, then what is the point of possessing them with a view to deterring an offensive IW? This distinction seems less relevant in the information age. Another distinction is between merely threatening and actually deterring by retaliating against an offensive IW attack. The argument is that one may have IW weapons without actually threatening other countries with their use. This distinction is linguistically incoherent; by definition deterrence entails the will to retaliate against offensive IW. A third distinction is that between the intention *to use* IW weapons and the intention *to prevent* their use as noted above. The intention behind the threat of IWD is to prevent their use. The intention *to deter* offensive IW still is an intention to make a *credible threat* to use IW weapons, since deterrence, in theory and in practice, involves this threat; but the intention to practice massive IWD will conditionally threaten numerous innocent individuals with hardship or death.

Suppose we drop the emphasis on intention and instead focus on the *anticipated consequences* of an IW deterrence policy. Intention is still present, but the emphasis is now on the effects of the action that embody the intention to use IW weapons. Is it still wrong *to threaten* to kill or harm large numbers of innocent individuals if this were the only practically effective way of assuring that they will not *actually* be harmed or killed and that other basic human rights will not be destroyed? If a choice must be made between the *threat* of IW and the *actual infliction* of harm or death, it is certainly arguable that the former is more reasonable than the latter on the basis of the lesser of two evils argument. When a choice must be made between two evils, the lesser evil should be chosen over the greater evil, especially if this is the only way of preventing the greater evil.

The lesser of two evils argument will be strongly in favour of IWD. This is true, a fortiori, when it is linked with the operational view that IW weapons lower the threshold of overt physical violence in a way that conventional or nuclear weapons do not. So, while it is true that 'whatever is wrong to do is wrong to threaten to do,' it is also true that actually to do a wrong is worse than merely threatening to do that same wrong (cited in Walzer, 1977, 272). When the threat is made with a view to preventing offensive IW and when it makes this prevention more likely, then IWD receives a moral justification that the dictum obscures.

The key supposition in this argument is that IWD will not lead to any actual harm or killing because deterrence will not break down. Just

as we must not commit the fallacy of *post hoc ergo propter hoc* – that is, nuclear deterrence is the only thing that kept the Soviets from bombing the United States and its allies – so, too, nobody has a crystal ball to predict the future. More important is the supposition that there are no alternative ways of preventing the actual inflictions except by IW threats. The lesser of two evils argument is not without difficulty, because the alternatives it proposes must not be gratuitously imposed by the agent or government. When a gunman says, 'your money or your life,' it involves the question of whether the recipient, the individual or individuals on whom the evils are impending, has actually done anything to deserve them. Like the gunman's case, that of IWD begs a distinction between governments or state/group actors and innocents. Millions of innocent persons whose lives are threatened by massive cyberwar have done nothing to merit such a threat. This is why nuclear deterrence or IWD is quite different from ordinary penal deterrence, wherein the threats are addressed directly to individuals who actually commit or contemplate committing crimes, in accordance with the direct application of the PGC. They could have avoided the execution of the threat by avoiding the crime. The alternative evils with which IWD policy confronts millions of innocent civilians is imposed on them gratuitously. They have done nothing to merit such a predicament. This point imposes a serious limitation on the moral reasonableness of IWD policy and the lesser of two evils argument invoked to justify it. This is because the individuals whose lives are threatened by IWD policy are not, for the most part, the same as those who will determine whether lethal IW attacks will occur. This difficulty requires that the criterion of reasonableness be extended to citizens, so that democratic control of policy can be more fully assured within the community of rights.

The answer to the question of whether or not IWD is morally 'reasonable,' then, is similar to the conclusion regarding its instrumental rationality. Such a policy is morally reasonable as a temporary device to the extent that the threat of IW serves to prevent its actual occurrence; but – and this point is crucial – a policy of IWD could be followed only as a means of establishing and stabilizing alternatives that do not involve the threat of non-combatant murder or the violation of other human rights, such as the right of innocent persons to be free from threats of MAID that could lead to great harm or death. An anti-IWD argument can be based on grounds other than the strict deontological claim that it is wrong to intend that which it would be wrong to

do. IWD may also be understood as a form of hostage holding whose moral wrongness resides in its threat to non-combatant third parties by imposing substantial risks of harm without the voluntary consent required by the principle of human rights.

Rethinking Policy Alternatives for the Information Age

A sceptic might say that this perspective may be theoretically correct, but can the shortcomings of IWD policy be avoided in practice? What are the alternatives? Political realism or idealism have tended to be the two main alternatives in history. Political 'realism' or *Realpolitik* has been the dominant approach throughout human history and certainly during the Cold War context of the use and deterrence of nuclear weapons. Political realists generally base their pro-deterrence argument on the primacy of power and self-interest in human affairs. This concept is coupled with a negative philosophical or theological anthropology and a generally pessimistic view of history. The realist says: 'All the weapons that human beings have ever invented have been used. IW weapons are no exception to this rule. It is naïve to think that the meaning and nature of war has changed simply because we live in an information age.' Moreover, despite the fall of the Berlin Wall and the end of the Cold War, Russia still is seen as a formidable adversary who necessitates a strong deterrent predicated upon the actual use of IW weapons. IWD is necessary, then, for the traditional *raison d'état*. As Robert Tucker notes: 'Deterrence lays bare and points to the depressing fact that even a democratic version of reason of state need admit of no limits to the measures that may be taken to preserve the political community's independence and continuity. The necessity of democratic states may reach out to take and to justify the same extreme measures as the necessity of non-democratic states' (cited in Hardin et al., 1985, 53). Colonel Edward Mann expresses IW realism when he writes that 'a new chapter in warfare was written on 17 January 1991 [i.e., the air assault against Iraq]. With the advent of postindustrial warfare, information warfare ... warriors who make the most of it increase their chances for victory in the next round' (Mann 1994, 4). General Eugene Habiger writes: 'The United States must be prepared to pose unacceptable risks to any potential adversary. Nuclear weapons are one – but not necessarily the only – means of doing that. As then-Defense Secretary Perry noted on more than one occasion last spring, *"Anyone who considers using a weapon of mass destruction against the United States or its*

allies must first consider the consequences. We would not specify in advance what our response would be, but it would be both overwhelming and devastating."' (Habiger, 1997, 4; emphasis in original).

Political realists uphold the extreme motivational concern with national egoism or self-interest. Interstate conflict was and continues to be understood with reference to 'security dilemmas, crisis bargaining theory, power politics, deterrence failures, and so on' (Harvey, 1997, 140). Like nuclear realists, IW realists will relentlessly push for IW weapons superiority in preparation for cyberwar. Information operations planners must 'prepare for the next war instead of the last' (Arquilla and Ronfeldt, 1997b, vi). IWD is morally justified because it will keep the peace in the same fashion that nuclear deterrence kept the peace during the Cold War. IW realists may accept a declaratory doctrine of 'no first use' of information warfare against largely civilian targets, but they allow for IW strikes against military-oriented targets such as operations centres, logistics, and command and control nodes as a vital part of a robust IW deterrence. They allow for IW retaliation in the event that one's own civilian targets have been hit and presuming that the attacker's identity can be determined.

Admiral William A. Owens links American strategic deterrence strategy to an emerging technological 'system-of-systems.' The system-of-systems comprises three general categories: (1) Intelligence, surveillance, and reconnaissance (ISR); (2) Advanced C^4I (command, control, communications, computer applications, and intelligence processing; and (3) Precision force, the latter term being a broad concept in which the knowledge and orders generated from the first two areas are translated into precise action and results. The meta-system would putatively provide qualitative and quantitative domination of 'battle space knowledge' while acting as a deterrent threat. In the admiral's words:

> '[D]ominant battle space knowledge (DBK) ... involves everything from automated target recognition to knowledge of an opponent's operational plans and the networks relied on to pursue them ... The growing capacity to infuse DBK into all our forces will be coupled with the real time awareness of their status and the understanding of what they can do with their growing capacity to apply force with speed, accuracy, and precision. This means we will increasingly match the right force to the most promising course of action at both the tactical and operational levels of warfare ... This new system-of-systems capability, combined with joint doctrine

> designed to take full advantage of these new fighting capabilities, is at the heart of the [revolution in military affairs] RMA.' (Owens, 1996)

The essence of a system-of-systems is the ability to collect, process, store, and transmit militarily relevant information as the need arises. If the reach of the meta-system is global, then all information could be conveyed as 'bit streams' to American allies, who would provide the weapons while the United States provided the aimpoints. The United States would use remotely delivered bit streams to form 'virtual coalitions.' Libicki describes an image of conventional conflict circa the year 2015 in this way:

> In support of AWACS [Airborne Warning and Control System] and JSTARS [Joint Surveillance Target Attack Radar System], high-flying and stealthy UAVs [unmanned aerial vehicles] oversee the battlefield, relaying interesting imagery (optical or synthetic aperture radar – SAR) to the command center. Bolstered by infrared and electronic intelligence, analysts in fusion centers translate readings into targets. Moving targets are posted to long-range attack aircraft; others, to long-range missiles. Where discrimination is difficult or the risk of collateral damage is high, small mobile teams supply the final go/no-go decision. After standoff strikes disorient and decimate foes, larger maneuver teams rush in to put foes to flight and occupy important terrain. A Revolution in Military Affairs – RMA – would emerge from a combination of information dominance, precision strikes, and maneuver warfare. The System, in turn, is being oriented to support such operations.' (Libicki, 1998, 133–4)

In short, then, political realists maintain that both nuclear deterrence and IW deterrence are morally justified and here to stay. Thus, Martin Libicki, in his comparison of information and nuclear RMAs, can write that 'Conventional forces survived the Nuclear RMA because nuclear war was unfightable. But the Information RMA is eminently fightable and holds the prospect of conventional military victory without mutual suicide – indeed with even less collateral damage. However, most of what a nuclear war would have done to conventional forces can be applied to the Information RMA – but this time for real' (Libicki, 1996, 82). We are less optimistic than Libicki about the prospect of IW being eminently fightable while it holds out the prospect of conventional military victory without mutual suicide. As we noted earlier, Russia claims a right to respond to IW with weapons of mass

destruction and seems to be well aware of their organizational and technological limitations (Thomas, 1996).

A second alternative is an *idealistic* one. Instead of focusing on exclusive considerations of power and national egoism or self-interest, the idealist stresses the other-regarding aspects of reasonableness. Political idealism maintains that the ethical ideal can guide the role and use of force in human affairs. In its classic and contemporary western form, for example, Christian pacifism has insisted on taking up the non-violent Cross of Christ as the only way to break the cycle of violence that besets humanity (Douglass, 1983). Pacifist idealism also appears in Gandhian (Iyer, 1991) and pragmatic and secular versions (Sharp, 1965; Schell, 1982). If nuclear weapons are weapons of mass destruction, then IW weapons are, similarly, weapons of mass disruption, but with no less violent consequences.

The problem with idealism is that it often fails to admit the reality of existing power relationships and self-interested motivational considerations that drive individuals and states. Idealism fails, theologically speaking, to appreciate the reality of sin in the world. It may be morally licit to give up one's own life in the name of non-violent resistance, but Christian love also requires the defence of the innocent, wrongfully placed in harm's way.

A third alternative, operative during the latter part of the Cold War, stressed incremental, reciprocal steps towards the goal of nuclear reductions. Whereas realism is grounded in extreme egoism, and idealism is rooted in a vision of total altruism, *pragmatism* assumes the self-interested motivations of each party for national security. Thus, John Arquilla can maintain that the 'arms control paradigm is difficult and complex,' but nevertheless it provides a 'useful framework' to deal with the security dilemma posed by IW (cited in Porteous, 1997, 20). If offensive IW were executed in anticipation of conflict without an open declaration of war, it would run counter to any concept of a justifiable war. Arquilla argues that 'wherever possible, we must reject this option' and make IW 'a weapon of last resort.' Moreover, 'we need something like the CWC [Chemical Weapons Convention], an Information Warfare Convention' that would commit signatories to making no-first-use declarations. An IW convention based on confidence-building measures and behavioural restraints would provide for information exchanges that would take place within existing security alliances like NATO and entail cooperative efforts to track down violators and punish countries that provide a safe haven for hackers. Arquilla's

vision of ethically waged information warfare is ultimately pragmatic: 'In a world where adversaries may soon have well-developed capacities for striking at the target-rich United States, *just war conventions, in the information realm, may swiftly prove as practically useful and valuable* – even when the opponent is a nonstate criminal or terrorist organization – as they are ethically or morally desirable' (Arquilla, 1999; emphasis added).

Just war conventions are problematic because, if two parties do not recognize the authority behind them and they think that they have adequate power, the result will be war. It does not help to differentiate between aggressive and defensive wars or to speak of 'just wars' or 'holy wars.' If such judgments are not pronounced by superior authority, they are partisan judgments, even if the parties are not identical with states but cut across them.

Arquilla's realist-leaning pragmatism may be combined with or modified by a higher vision of human possibilities. Recall that the U.S. Catholic bishops were led, after three years of debate and consultation with pacifists, just war thinkers, military and political strategists, to a 'strictly conditioned' moral acceptance of nuclear deterrence in 1983. They invoked three criteria in their moral assessment of deterrence, which we adapt to our IW situation. First, if information warfare exists only to prevent the use of IW weapons by others, then proposals to go beyond this use to planning for prolonged periods of repeated strikes and counter-strikes or to 'prevailing' in offensive IW are not morally acceptable. Second, if information warfare deterrence is the goal, 'sufficiency' to deter is an adequate strategy; the quest for IW superiority must be rejected. Third, information warfare deterrence should be used as a step on the way towards progressive IW 'disarmament.' Proposed additions to a strategic IW system or changes in strategic doctrine must be assessed precisely in the light of whether it will render steps towards a different kind of basis for national and international security (USCC, 1983, para. 188).

While these criteria provide direction for thinking about IWD, the latter of the three incurs difficulties, especially when viewed in the light of the problems posed by 'netwar' and transnational criminal activity. Distrust among states may continue to undermine joint action to reduce the danger of IW. Mutual distrust may be 'rational' insofar as it counsels caution in the face of unprecedented danger. Citizens need far greater knowledge of the actual threats to national security and the common good if they are to support IWD policy with their tax dollars

and trade off privacy rights in the interest of national security (Walters, 1998a).

Pragmatism holds that mutual distrust is irrational in that it adds to the danger and heightens the risk of IW against which IWD would guard. Yet the distrust that drives IWD is not total distrust. Trust still operates in the party that rationally refrains from IW attack because of the real threat of retaliation inherent in IWD policy. This form of trust is based on threat and fear, however, rather than being grounded in the 'mutuality' that characterizes the community of rights.[6] At the limits of deterrence theory, we are driven back to the existential point that all policy depends on something above politics, reasonable human selves, ethics, and the willingness to sacrifice and compromise (Jaspers, 1958, 1961). IWD may be rational and reasonable if it is able to establish and stabilize alternatives that do not involve the threat of non-combatant injury or deaths, or the violation of other human rights by imposing substantial risks of human and environmental harm without consent.

In order for IWD to be rational, one of the competitors must actually be in a position to win out over the other. IWD will increasingly find this condition hard to meet, since the ability to wreak havoc is now diffused to non-state actors and individuals. Fifteen years ago the worldwide population with skills for conducting cyber attacks was in the thousands. 'In 1996 it was about 17 million, and by 2001 it is predicted to be about 19 million' (PCCIP, 1997, 9). Who wins or who loses in a world of 19 million infowarriors? IWD also requires that an opponent be identified. The anonymity of terrorists, organized crime, and hackers means that they can threaten instant, society-wide damage. High-tech networks challenge the usefulness of geographical boundaries. It is now almost impossible to separate disruptions in connections between national and global levels.

Conclusion

The argument of this chapter has been modelled analogously on nuclear weapons use and deterrence. Yet if we continue to think of IW deterrence in terms of nuclear deterrence, we fail to miss the radical challenge of the information age. What makes the relation between nuclear deterrence and IW deterrence *disanalogous* is that thousands of IW weapons do not already exist and are not already targeted at enemies. This gives military strategists, politicians, and concerned citizens some time to think more seriously about deterrence in a new security

environment. The United States has already unilaterally reduced its non-strategic nuclear arsenal some 90 per cent from Cold War levels and, under the START I Treaty, the United States and the former Soviet Union are reducing by half the 12,000 strategic nuclear weapons deployed in 1990 (Habiger, 1997). The decisions that IW strategists make today about the development and deployment of IW weapons will have morally significant consequences, just as strategic decisions about the use of 'multiple independently retargetable re-entry vehicles' (MIRVs) did for the nuclear arms race.[7]

Expanding strategic arsenals into the information realm will not safeguard the earth or human civilization in the long term. We must not seek a technology-based, 'system-of-systems' solution to the problem of cyberwar. Rather, we need a human solution based on moral reasonableness and respect for the human dignity and rights of individuals. Technologies may support human values or be instruments of degradation and domination. They are social constructions moulded, through human will, by particular interests, goals, and values. Deterring IW in a wired world brings us to the limits of politics and deterrence theory. Human change and resolve are needed, including a pragmatic view that supports the Canadian Forces Statement of Defence Ethics to respect the human rights, responsibilities, and dignity of individuals (National Defence, 1997). Our ultimate challenge is to move to a mutuality of human rights and a moral reasonableness that makes both trust and security possible, since *'there can never again be a major war between states without nuclear risk'* (cited by Habiger, 1997, 3). In short, we need both an existential 'conversion' or 'revolution in human affairs' grounded in reasonableness and an opening to mutual trust, commensurate with the ongoing technological revolution in military affairs (Walters, 1988). The community of rights, which promotes and protects generic rights to freedom, well-being, and human dignity, must become a global community in the information age. Is this possible?

Conclusion: Towards a Global Community of Rights in the Information Age

This book has been guided from the outset by the assumption that all philosophical reflection must begin with our historical and technological *situation.* Canadian information highway policy (1993–98) and e-commerce strategy provided our historical point of departure and defined the three key policy domains for subsequent ethical analysis: The impact of information technology on work and employment (chapter 3); privacy and security challenges (chapters 4 and 5); and emerging information warfare practices and deterrence (chapters 6 and 7). We have sought to achieve an ethical 'balance' between individual rights and societal interests by means of the application of the principle of human rights whose justificatory ground resides in the necessary conditions of human action. We have seen that human rights have as their objects the generic rights to freedom and well-being to which individuals are entitled and that require duties on the part of others. Community protects and fulfils human rights, especially for individuals who do not effectively have them, on the basis of the human mutuality and social solidarity of individuals who recognize and fulfil common needs. Human rights require community for their implementation, while community requires human rights as the basis of its morally justified economic, political, and social operations and enactments; hence the need for a community of rights in the information age.

Across the broad spectrum of policy issues and concerns that we have analysed both empirically and ethically, we have seen that the values of mutuality and social solidarity are increasingly vital to the promotion and protection of human dignity and rights in the global informational economy, to the privacy and security challenges posed by the network society, and amid the emerging practices of netwar and

cyberwar. We have argued that technology provides no ethical operating system for the deeper problems that plague communicative reason among individuals at this juncture of human history. At the limits of technical design and planning, and even at the limits of legal and ethical specification of norms, Canadian information highway policy issues and developments challenge us today to a wider rationality than the mere instrumental rationality of the intellect that creates and manages information technology.

The ethical stakes of Canadian information highway policy and e-commerce strategy have become more compelling when we situate information policy developments within the context of the broader information age revolution, the worldwide historical and technical situation of modernity, and a philosophical framework that views the community of rights and a deeper, more authentic and transparent human communication as vital to the resolution of the ethical challenges of informationalism (chapter 1). Our reading of Canadian information highway policy has been a rather sympathetic one insofar as we have avoided a polarized view of the information highway as either a singular private sector space for e-commerce or an exclusive public e-commons (chapter 2). Beyond these two competing ethical policy visions, we have advocated a positive role for the right to productive agency in the informational economy and for participatory, public access to the information infrastructure that serves the community of rights and the quest for economic and political democracy.

Our survey of the historical emergence and sociological development of Canadian information policy has, revealed at times, the twin principles of 'technological imperative' and 'technological determinism' at work (Babe, 1995). A reductionist understanding of human freedom and will support a technocratic world view in which instrumental rationality and determinism dominate at the expense of a wider rationality. For what seems to be a technological imperative often turns out to be merely a 'self-interested choice imposed on others'(Laperrière, 1999, 186). Technological imperative fails to distinguish manipulative from non-manipulative forms of relationship on the grounds that technology causally drives all historical and material relations and change. Technological determinism fails to appreciate the limits of scientific knowledge, the limit situations of human existence, and even systematic unpredictability in complex systems. In turn, techno-managerial expertise masquerades as social control and power when 'effectiveness' lacks rational justification and when authority

and expertise are ideologically legitimated on the basis of claims to technology-neutrality, value-neutrality, or law-like generalizations in the social sciences.

Such false claims of instrumental rationality, however, reject the Aristotelean link between evaluative claims that inevitably function as a kind of factual claim. In the western philosophical tradition, 'mechanisms' have been understood as *efficient causes* in a world that can be comprehended correctly only in terms of *final causes*. Information, we suggest, is ultimately in the service of final causes, including human wisdom. The final ends to which humans move are ethical goods, and movement towards or away from various goods must be explained with at least partial reference to the virtues and vices that we either learn or fail to learn and the forms of practical reasoning that such activities employ. In one sense, then, the principles of technological imperative and technological determinism are merely symptomatic of modernity's displacement of final causes and a teleological view of the self. When the self becomes a mere function of material, technological, or bio-technological means, when, in Kant's famous words, we treat other human beings as means rather than as ends, then the objectification and functionalization of individuals appear to be a natural and inevitable reality. The denial of human dignity and human rights follows in turn. Herein lies perhaps one of the greatest ethical challenges of the information age: We must be vigilant against the human being's degradation of our own humanity, as well as the degradation of all life.

Our human rights framework has insisted on policy alternatives and human choices, grounded in freedom and truth, that are operative in a two-way interaction between technology and society. Technologies are ambivalent, neither good nor bad, but neither are they neutral. They contain possibilities for emancipation and domination. A reasonable information policy strategy will continually seek to avoid the demonization of technology or its wholehearted embrace as a salvific solution to economic problems, human temporality, and finitude. Scientific thinking and technological know-how do not pose the questions we must answer, weigh, and resolve in thinking about ethical goals. The science that gives birth to new information technologies can provide premises of material information, but ethical problems arise on a different level of thinking, even as norms of ethical specification extend asymptotically along the x-axis of historical and technological developments.

In chapter 2 we situated Canadian information highway policy and

e-commerce developments within a more universal 'public policy cycle'. The value of mutuality at the heart of the community of rights is necessary to support physical access and access to content and services on the Internet as well as to provide funding for public space community networks. Moreover, we argued that the best 'virtual' community is an extension of the community of rights. The etymological link between virtue the 'virtual' and unveils the possibility of bringing together power and ethics in an informational community of rights wherein the Internet is not a regulation-free zone in relation to the spreading of hate propaganda and child pornography. The courts may be willing to impose screening responsibilities for Internet Service Providers in accordance with consensual, societal rules.

Furthermore, the principle of 'lifelong learning' at the heart of information highway policy is sound, but we miss the ethical mean or tensive balance if public education becomes a 'pay-as-you-go smorgasbord' (Moll, 1997; Noble, 1996) or if research partnerships between industries and universities exchange the internal goods of research for external goods such as money, power, or fame (cf. Kenny, 1986). While business and labour were at odds throughout much of IHAC policy development, there exists common ground on the roles of education, training, and skills development in the informational economy. The challenge is to turn the policy debate between business and labour into a communicative, loving struggle, where the economy, as the material basis of existence, serves human beings, not vice versa. Otherwise, a non-violent, communicative, loving struggle may well turn into a violent, non-communicative struggle for sheer existence.

The serious challenges of the global and Canadian informational economy are as much, if not more, ethical challenges as they are technological, economic, and political ones (chapter 3). In accordance with the principle of human rights, conceptions of productive agency, productivist welfarism, work, human capital, and private property rights stress individual and state rights and responsibilities that may help to reduce economic inequalities during our present epoch of great social transformation. The human right to development, which, we have argued, is in the first instance a right to productive human agency, is not present in its full scope either in global societies or even in many modern welfare states. At issue, however, is a vision of a normative ethical order that might supply the basic needs of all human beings in the wake of globalization's challenge to social and economic rights, and the failure of basic development strategies since the Second World War.

While we have shown that there are ethical and empirical problems with the 'end of work' thesis, a key ethical challenge of the twenty-first century will be to extend a rationally grounded right to productive agency and human development to the *humanum*, to a global community of rights. The community of rights begins with a right to productive agency that allows individuals to develop their own capacities for producing goods and commodities and requires institutional efforts to remove poverty, work towards full employment, and harness information and communication technologies for productive agency. Such policy developments not only would go far towards avoiding the risks of barbarism, but would also help to close the gap between the so-called information haves and have-nots. Future empirical data may resolve the productivity paradox. In our present historical situation, however, the new libertarian wave and utilitarian contention that the well-being of some individuals may be sacrificed through their being unemployed, if this leads to the greater good on the whole, is difficult to accept as morally justified policy for rich nations. Global policies, in which millions in the Fourth World are subject to pervasive poverty or the trauma of unemployment for the purpose of maintaining a general level of well-being in which they do not share cannot be ethical. It remains to be seen whether the IT revolution will lead to an analogous revolution in mutuality and solidarity for the so-called losers in the informational economy. We are all losers in a world where basic human rights are not met, and poverty and unemployment remain non-virtual.

Fair information principles appropriate for database forms of surveillance up to the last decade still are necessary, yet insufficient, for global and Canadian privacy and security policy (chapter 4). Bill C-6 attempts to strike the right balance between the business need to gather, store, and use personal information and the consumer need to be informed about how that information will be used and protected. The cryptography policy framework for e-commerce seeks to balance the legitimate use and flow of digital data with privacy and civil and human rights concerns, on the one hand, and law enforcement and national security interests, on the other hand. Our exposition has revealed that Canadian information policy has lacked substantive justification of privacy as a human right and that the philosophical meaning of privacy as a social value has been undeveloped.

For this reason we have responded directly to the federal government's call for 'open communication and dialogue' on how best to protect personal information in the private sector and how we might most

effectively think about the ethical and policy implications of privacy, security, and new surveillance technologies (chapter 5). Cryptography key recovery systems entail a complex set of technology and policy challenges for accessing the plaintext of ciphertext information. The requirements of government key recovery and commercial encryption and key recovery appear to be incompatible because of differences in the kinds of data and keys for which recovery is required, the manner in which recoverable keys are managed, and the relationship between key certification and key recovery. Yet there exists a legitimate need to protect critical information infrastructures by means of consensually based, governmental action. Ethical justification for policy choices in the realm of security and intelligence are no different from the need for countries to provide for protection and defence through law-enforcement agencies. Making cryptography tools that protect information and communications available to the private sector and encouraging their use in the networked society are tantamount to the needs for physical security provided by locks and alarms in civil society. As we have seen, however, a difficult ethical problem arises because cryptography tools are potentially 'dual-use': they can be used for good or evil, either as privacy-enhancing technologies or as tools that threaten the privacy and security of law-abiding citizens. Technological tools are good precisely to the extent that their end-users are good human beings. As technological tools proliferate and become increasingly complex and differentiated, why should we not expect to see the need for a corresponding complexity and differentiation in our human ethical becoming?

Our survey of contemporary technological practices and our review of legal, social scientific, and philosophical conceptions of privacy set up the need to make an argument for where to draw the ethical line between negative and positive surveillance. The normative specification we have brought to privacy and security policy debates has been grounded primarily in the principle of human rights, norms of basic, non-substractive, and additive well-being, and the criterion of degrees of needfulness for action. In this way the ethical justification of privacy as grounded in the necessary conditions of human action corroborates, but extends, the government's view of privacy as a human right and social value in earlier policy documents.

Going beyond the question of ethical justification per se, we have also offered a substantive derivation of norms in accordance with the principle of human rights that balances human rights and societal

interests with respect to the use of smart cards, biometrics, closed-circuit television surveillance, electronic monitoring, genetic testing, and informational privacy and security. The 'balance' we have achieved is not a 'utilitarianism of rights' implied by an unending calculus that is ready to interfere with rights in order to produce a weighted minimum of privacy rights-infringements for either individuals or the public interest. Instead, the context of action entailed by the principle of human rights has provided us with wide comparisons of fairly ascertainable disparities in degrees of importance between the objects of rights. For this reason we have restricted the criterion of degrees of needfulness for action to areas where the basic well-being of some individuals requires infringing the additive well-being of others or the wider freedom associated with additive well-being, and we have tried to take into account human diversity, differing cultural contexts, and the extent to which persons and organizations actually can fulfil human needs.

Our ethical analysis of voluntary and unforced consent, that is, 'informed consent,' was also linked to the principle of human rights and private sector privacy protection. For real knowledge and consent seem to be rarely operative in online transactions. The 'opt-out' clause tends to compel data subjects to make a 'forced' choice, and there tends to be an unequal power structure at the base of e-commerce transactions today. Current practices tend to lower an individual's capacity for success in actions affected by lies or omissions concerning the withholding of information about what will factually happen to an individual's personal information. We should not assume that the only ethical concern is with the private sector, however, in the wake of recent policy developments. The revelation by Canada's privacy commissioner, Bruce Phillips, in his *Annual Report 1999–2000* that the government held files with over 2,000 pieces of information on most citizens set off an angry storm of protest across Canada. Jane Stewart, minister Responsible for the Human Resources Development Corporation (HRDC), initially defended the collection on the grounds of the government's 'need to know,' but she later reversed her stand and ordered the 'Big Brother Database' to be dismantled (McCarthy, 2000, A1).

In the light of both public and private sector developments, we have argued for the creation of a property right over commercial exploitation of personal information based on the consequentialist justification of property rights. Such a property right would help to generate a new balance of power between individuals and, at a minimum, credit and

insurance reporting companies. Here again, however, legal rights alone will not solve the ethical challenges of mutuality and solidarity within a flourishing informational community of rights. Although we admit that new privacy-enhancing technologies (PETs) hold out positive possibilities for the protection of privacy and security rights both on and offline, PETs encounter limits: they do not determine normative policy goals, they potentially negatively affect mobilization and mutuality and identity and culture, and they may even undermine trust and mutuality.

By means of a concrete application of the goods of basic, non-subtractive, and additive well-being and the criterion of degrees of needfulness for action, we have drawn normative conclusions about the use of caller number identification, telemarketing, phone solicitation, secondary uses of private information, genetic privacy, health identification numbers, medical data linkage, DNA screening, video surveillance, and encryption policies, in accordance with the principle of human rights. A major contribution in this book has been the setting of these normative recommendations in a justificatory framework of human rights, especially the right to privacy, whereby their connection with the generic rights of human agency – freedom and well-being – has been illuminated.

Our historical and technological situation required extending the ethical analysis of Canadian information highway, privacy, and security policy in relation to the needs of law, security and intelligence, military agencies, and the rise of information warfare technologies and practices (chapter 6). We have traced the historical origins of IW to the 'revolution in military affairs' and identified the conceptual world of IW, the nature of IW 'weapons,' the problem of transnational informational crime, and the state's need to protect critical information infrastructures. We have evaluated global surveillance practices (e.g., the ECHELON network) and strategic information warfare policies, first, in the light of existing international human rights law and, second, in accordance with the principle of generic consistency. As an extension of the indirect application of the PGC's normative rules, the ethical analysis of information warfare drew upon classical *jus ad bellum* and *jus in bello* norms. A systematic application of both sets of norms to information warfare has brought us to the limits of traditional 'just war' doctrine, to an understanding of force as a limit situation of human existence, and it has raised anew Kant's classical question concerning the possibility of a 'perpetual peace,' but now in the informa-

tion age. We argued, again in accordance with the direct and indirect applications of the PGC and the consensual procedures of the democratic state, that citizens need far better knowledge of the ostensible threats to public safety and national security in order to make informed judgments about legislation that might restrict privacy rights through surveillance practices.

Because government and military policies that entail the use of IW weapons are now being devised and implemented, our ethical analysis of information warfare deterrence (IWD) logically and necessarily followed the ethical analysis of the use of IW weapons and the application of *jus ad bellum* and *jus in bello* norms. In the context of deterrence and information warfare (chapter 7), we have argued that a policy of strategic information warfare deterrence (IWD) could be reasonable only if it were able to establish and stabilize alternatives that do not involve the threat of non-combatant murder and do not violate the principle of human rights by imposing substantial risks of harm without consent. We should not mirror IWD in the information age along the same lines as nuclear deterrence policy in the nuclear age, but we should move instead, towards a mutuality of human rights and moral reasonableness that makes both trust and security possible.

The problem of deterrence in the information age brings us to the limits of politics and technology for solving the problem of war, which is above all a challenge of rational selfhood. We fail to understand the true meaning of the revolution in military affairs if we do not grasp the commensurate revolution needed towards reasonableness in a world of 13 million infowarriors and state and non-state actors that possess information warfare weapons. Contrary to the optimistic view that information warfare is 'eminently fightable' and holds out the prospect of a conventional military victory without mutual suicide (Libicki, 1996), we have argued that our situation is not an either/or – either atomic, biological, and chemical weapons or information warfare weapons – but is, rather, a situation of both/and. Nations possess IW weapons along with weapons of mass destruction, and those nations that do not possess thick information structures and sophisticated IW weapons will invariably rely on conventional weapons. The information age requires a human transformation towards ethics and rationality whereby mutuality, social solidarity, and a more sophisticated and refined intersubjective human communication can work to lower the possibilities of human violence, if not completely eradicate conflict within the global, informational community of rights.

The sceptic again will ask: Is our vision of a global community of human rights really possible? This is also the question we were left with at the end of the last chapter. The question is not merely academic, since the resolution of many of the ethical challenges surrounding the informational economy, privacy and security, and information warfare requires global cooperation and reasonable policy decisions. Ultimately, the question concerns what we want, what we are willing to work and sacrifice for, and to what extent we believe in the rationality of other human beings and, thus, in our own rationality.

The idea of a community of rights, much less a global community of rights, has been met, of course, with vehement opposition in recent years from individualists and libertarians alike who, invoke negative rights of freedom, construed solely as non-interference, to reject what they see as totalitarian governmental interventions into economy and society, including information policy. Such individualist depictions of rights, however, turn a blind eye to the oppressions endured by masses of individuals whose ability to compete in the informational economy has been seriously weakened by historical, economic, technological, and socio-political forces beyond their control. For despite the empirical and ethical problems with the 'end of work' thesis (chapter 3), we must admit that not all is well in western, liberal democracies. Capitalist market economies continue to be plagued by problems of poverty, unemployment, crime, and homelessness, not to mention the loss of collective solidarity. The community of rights we have espoused herein is far from a cyberlibertarian vision of techno-frontierism that ideologically legitimates rugged individualism, social greed, monoculturalism, and an unregulated information infrastructure (cf. Winner, 1997). Nor does the community of rights advocate individualistic privatization of cyberspace that we sometimes encounter in libertarian notions of virtual community. Computer networks may or may not facilitate local, physical communities, but they cannot ensure political and economic democracy. Networks can provide marvellous means for individuals who act to build a community of rights within their local situations while thinking and communicating globally.

If the Canadian and global information highway has increasingly brought down borders between nations, it may also turn national cultures into an emerging global culture that could rekindle ethnic, regional, and religious conflicts that the modern liberal and democratic state has sought to transcend (Porter, 1997). This paradoxical feature of modern communications goes back to the rise of mass communications

and radio/television technology. The important difference today is that the Internet provides 'interactivity' in a way that earlier technologies did not. This is no doubt one of the reasons why Canada and many European Union member countries have insisted on adding linguistic and cultural diversity to the design of the Global Information Infrastructure during the past decade of policy development. As Michel Dupuy noted in a speech delivered at a G7 Ministerial Conference on the Information Society in 1996, 'neither a vehicle of cultural homogenization, nor a mechanism for one kind of monopoly or another, [the information highway] must instead embrace a diversity of international perspectives and languages, for the benefit of all citizens. It should not thrive at the expense of national cultures and identities ... We must prevent the creation of any form of cultural monopoly on the information highway' (cited in Raboy, 1997, 204). At the same time, we must not confuse digital interactivity with human interactivity.

If the historical origin of the Internet, as well as modern human rights, are clearly western developments, how then is a truly global community of rights possible? Will not the very groups that reject human rights as a form of western 'ethnocentric imperialism' also reject any vision of an informational and global community of rights? Apart from the empirical limitations of access to the global information infrastructure, sceptics will argue that a global community of rights is not possible because cultural relativism poses a serious obstacle to the universal claims of human rights. We turn, then, to the criticisms of radical, strong, and weak cultural relativism in relation to the possibilities for a global community of human rights.

For radical cultural relativists, for example, there are no transboundary legal or moral standards against which human rights practices may be judged right or wrong (Geertz, 1973; Herskovits, 1964). Instead, human rights standards vary among different cultures, and what may be judged right or lawful in one culture should not be imposed on other cultures. Thus, mutilation and flogging as a form of criminal punishment, female genital circumcision, the subjugation of women, and various authoritarian methods of government are unlawful by international standards, but are defended as permitted or required by existing cultural traditions. This position sees culture as the source of all values and holds that there are no rights that everyone is entitled to equally, simply as a human being in need of freedom and well-being as the necessary conditions of action. Thus, a global community of rights cannot be obtained, in the words of the American Anthropological

Association, 'except insofar as it permits the free play of personality of the members of its constituent social units and draws strength from the enrichment to be derived from the interplay of varying personalities' (cited in Winston, 1989, 120). Ultimately, for radical cultural relativists, right and wrong are matters of convention and opinion, and opinions differ between cultures.

Strong cultural relativists hold that even if there exists a substantive body of human rights norms as a matter of customary or conventional international law, the meaning of these norms varies from culture to culture. Their emphasis is on cultural variation, relativity, and *difference*. Socialist and Third World conceptions are held to be 'communitarian' or group oriented, in contrast to atomistic, individualist western approaches. They deny universal standards by which all cultures may be judged, and decry the legitimacy of using values taken from western culture to judge institutions of non-western cultures. To impose on Third World societies norms taken from the UDHR is a form of 'moral chauvinism and ethnocentric bias' (Pollis and Schwab, 1979, 14). On these very grounds, Abdullahi An-Na'im defends, against article 5 of the UDHR and article 7 of the International Covenant on Civil and Political Rights, the Muslim practice, grounded in Islamic law (*Shari'a*), of amputating the right hand for theft (*sariqa*) when it is committed by a Muslim who does not need to steal in order to survive and who has been properly tried and convicted by a competent court of law (An-Na'im, 1992).

A third group, weak cultural relativists, maintains the fundamental universality of human rights norms, but believes that the norms are subject to secondary cultural modifications (Donnelly and Howard, 1989). Internationally recognized human rights provide the guarantees necessary for a life of dignity against the unchecked power of the modern state, as well as national and international markets. Rights to life, liberty, privacy, security of the person, protection against slavery, arbitrary arrest, racial discrimination, and torture, as well as rights to food, health care, work, and social insurance are basic to any plausible conception of equal human dignity. Weak cultural relativists reject claims that because of age, sex, race, or family a person is not entitled to the same basic rights as members of other groups. The concept of human rights is particular and modern and represents a radical rupture from the many status-based, non-egalitarian, and hierarchical societies of the past. The concept does not spring from a consensually based philosophical anthropology, but is best interpreted by constructivist theory

'as the result of the *reciprocal interactions of moral conceptions and material conditions of life*, mediated through social institutions' (Donnelly, 1985, 35). Human rights thus tend to be confined to liberal and/or social democratic societies. While one may find analogues for the actual content of internationally accepted human rights in many religious and cultural traditions, human rights constitute a radically new concept in human history that requires a liberal political regime to enforce the basic political right to equal concern and respect. Communitarian societies that give ideological and practical priority to the community over the individual are antithetical to the implementation and maintenance of human rights.

The moral philosopher Alasdair MacIntyre also denies the possibility of a global community of human rights. Rights claims, in his view, have a highly specific and socially local character and presuppose the existence of quite specific types of social institutions. Where cultures lack such social forms, 'the making of a claim to a right would be like presenting a check for payment in a social order that lacked the institution of money' (MacIntyre, 1984, 66–7). As evidence of the non-universality of rights, he notes that there is no expression in any ancient or medieval language that correctly translates the modern term 'right' until near the close of the Middle Ages. 'From this,' he admits, 'it does not follow that there are no natural or human rights[;] it only follows that no one could have known that there were.' The truth appears plain to him: rights do not exist and belief in them is tantamount to a belief in 'witches and in unicorns' (MacIntyre, 1984, 69).

The problem with MacIntyre's critique of human rights is that he attempts to assimilate the ontological status of human rights to the ontological status of witches and unicorns (Gewirth, 1985). Even if it were the case that attempts to give good reasons for rights had failed in the past, this fact would not ground MacIntyre's assertion that there exists an equivalence between the ontological status of rights and the ontological status of witches and unicorns. Human rights are normative entities with 'empirical correlates' in precisely the way that witches and unicorns are not. The term 'existence' has a secondary meaning of social recognition and legal enforcement such that one cannot provide empirical correlates for the past or future existence of witches and unicorns. When we consider the murderous or oppressive phenomena that have occurred in Nazi Germany, the Soviet Union, Chile, or elsewhere, we are not seeing mere 'fictions.' These oppressions are empirical phenomena that are undeniable violations of

human rights. Similarly, where certain basic freedoms and phases of human well-being are, in fact, protected, regardless of race, religion, and soforth, then the referent is the empirical existence of human rights that are socially recognized and legally enforced. There also exists extensive historical evidence for a concept of rights in ancient Greece, Rome, the Middle Ages, and non-western societies (Gewirth, 1978, 97–102; Tuck, 1979; Walters, 1999b). Just because cultures do not have some linguistic expression like 'human rights,' it does not follow that such rights do not normatively exist. As long as persons and cultures have a homeomorphic equivalent of the concept of human rights, it can be shown that rights and responsibilities correlatively exist.

Furthermore, as we saw in chapter 1, an agent's right-claim is logically prior to an existing set of social rules except in a quite minimalist sense. For in some cases right-claims are demands that certain social rules or institutions actually be established. Thus, when slaves revolted against their masters, when revolutionaries revolted against oppressive regimes, or when an individual's informational privacy is wrongly violated for the sake of commercial gain, the prior issue concerns rights to the necessary conditions of human agency itself. 'These rights and the claims to them have a prior status because it is for their sake that the most important social rules should exist. Thus, from the agent's standpoint, a community will be legitimate only if it recognizes his or her rights. Hence, far from rights presupposing a community which recognizes them, the relation is rather that a legitimate community presupposes the claiming and respecting of rights' (Gewirth, 1985, 74). Burdens (duties) exist for the sake of benefits (rights).

Human rights and the search for the 'right' law within the state exist as elements of the 'struggle' for existence. Because human existence is marked by inevitable conflict, rights have an inevitable and legitimate place in the life of the individual. As a regulative idea, universal human rights are compelling, whereas rights in the service of merely egoistic opportunism undermine original realizations by persons. In the 'limit situation' of struggle, the question is not whether we ought to replace rights with responsibilities, as some communitarians suggest, but rather 'where to give in and to suffer, where to fight and to dare' (Jaspers, 1970, 212). Human rights are not inevitably egoist, emotivist, or ideological. In contrast to the violent struggle for existence, the communicative, loving struggle is possible only on the basis of human community, mutuality, and solidarity. The loving struggle is not so much concerned with having one's day in court, since juridical rulings

and the will to legal right ideally give way to victory in the court of truth. The recognition of the other solely on the basis of legal rights, achievements, and successes gives way to a deeper human contact in mutuality and solidarity, as noted in chapter 1. Without a will to mutuality and solidarity, legal rights alone become a mean morality, and legal rights always presuppose moral rights against the view of legal positivists.

Indeed, we view radical cultural relativism as simply another manifestation of modern nihilism that has led to the deification of man and absolutist creeds of modernity. The horrors of the Holocaust testify all too vividly against the relativity of basic human rights. Western libertarianism overlooks the social dimensions of freedom, since human freedom is tied to historicity and is found only in human solidarity and community. States and communities have human duties to respect the right of humanity, as a whole, whose *telos* is towards greater human freedom between all persons on the planet. The crisis of modernity and of the two world wars was wrought by 'western' science and technology and is first and foremost a European crisis; there is no western 'ethnocentrism' or 'imperialism' in this admission. The normative question is not so much how to reconcile cultural differences in the interpretation of human rights, but rather how the 'Axial Age' civilizations (the west, India, and China) may find new spiritual forms within the technical tradition of modernity that has given rise to political totalitarianism and nuclear annihilation (Jaspers, 1953; Walters, 1997b).

Raimundo Pannikar argues that there is no 'endogenous theory of human rights capable of finally unifying contemporary societies' (Pannikar, 1982, 100). The fact remains, however, that mutual fecundation, mutuality, and trans-cultural communication are human imperatives in the information age. Contemporary global information policies push us towards the creation of an informational, global community of rights, whose condition of possibility presupposes the rationality, mutuality, and solidarity of individuals in relation to others. At its heart, the global, informational community of rights represents a caring society but also, in a parallel way, an institutionalization of love based on mutuality, solidarity, and the rights of others and duties towards others. There is an important, undeveloped spiritual dimension in the community of rights that is reflective of the moral concern that all humans, as actual or prospective agents, be enabled to live lives of dignity, self-fulfilment, and mutuality of respect. It is a spirituality that goes hand in hand with an emphasis on living a good life, a life of

flourishing autonomy and fruitful, communicative association with others. New information technology tools, combined with reasonable information policies and the mutuality, solidarity, and communication at the heart of the community of rights, may yet help us to achieve the much needed, but never complete, ethical 'balance' between individual rights and societal and global interests.

This page intentionally left blank

Notes

Introduction

1 Castells's philosophical supposition is that human societies are moulded by historically determined relationships of production, experience, and power. '*Production* is the action of humankind on matter (nature) to appropriate it and transform it for its benefit by obtaining a product, consuming (unevenly) part of it, and accumulating surplus for investment, according to a variety of socially determined goals. *Experience* is the action of human subjects on themselves, determined by the interaction between their biological and cultural identities, and in relationship to their social and natural environment. It is constructed around the endless search for fulfilment of human needs and desires. *Power* is that relationship between human subjects which, on the basis of production and experience, imposes the will of some subjects upon others by the potential or actual use of violence, physical or symbolic. Institutions of society are built to enforce power relationships existing in each historical period, including the controls, limits, and social contracts achieved in the power struggles' (Castells, 1996, vol. I, 15). While we do not accept all aspects of Castell's remarkable analytical framework, particularly its undergirding historical materialism, his empirical analyses of the informational economy and the scope of his methodology are unmatched. As a counterpoint to Castells's notion of production, we espouse a right to productive agency; as a counterpoint to his notion of experience, we set forth a thicker philosophical anthropology and action-based human rights ethical theory; and as a counterpoint to his notion of power as the potential or actual use of physical or symbolic power, we advocate an understanding of struggle as a 'limit situation' of human existence, but we hold out the possibility of transforming violent and coercive

struggles into a mutualist and loving struggle as a key ethical challenge of the information age.

2 For the political economy of information, see Babe, 1995; Carnoy et al., 1993; Castells, 1996, 1997; Globerman, 1996; Howitt, 1996; Menzies, 1996; Mosco, 1995; Mosco and Wasko, 1988.

3 For emerging information technology practices and their privacy implications, see Agre and Rotenberg, 1998; Agre and Schuler, 1997; Bennet, 1992; Bennet and Grant, 1998; Cavoukian and Tapscott, 1995; Davies, 1992; Flaherty, 1989; Freedman, 1987; Gostin, 1995; Inness, 1992; Linowes, 1989; Regan, 1995; Westin, 1967; Westin and Baker, 1972.

4 For problems surrounding information warfare, see Abelson et al., 1998; Alexander, 1998; Arquilla and Ronfeldt, 1997a, b; Castells, 1996, Denning, 1998; Diffie and Landau, 1998; Henry and Peartree, 1998a, b; Molander et al., 1998; Schwartau,1994.

5 Raab's critique of the doctrine of 'balancing' in the name of 'steering' bears on a problem that dogs utilitarianism in general; namely, the impossibility of interpersonal comparisons of utility or well-being. We will discuss Raab's critique of the 'balancing' metaphor at greater length below in chapter 5 in the light of the 'criterion of degrees of needfulness for action' set forth in chapter 1. The objects that are compared by this criterion are not vague entities such as personal or social 'utilities' construed in terms of individual desires or preferences whose difficulties of comparison are severe. Instead, the objects compared in the degrees of needfulness for action are needs for agency. This criterion is restricted to general areas of agency and thus militates against absolutist interpretations of privacy rights without falling into the morass of trying to set up intricate calculi of the relative strength of desires or preferences.

6 This model of information has been referred to as the 'information pyramid' (Lucky, 1989).

7 In the words of AFL-CIO research analyst Chris Bohner, 'People are just beaten down, hearing year after year how good things are, seeing top leaders take home healthy increases, while they get little or nothing ... Whichever economist you listen to and whatever rationale – pro or con – you buy into, the facts are that the pay of chief executives is in the stratospheric range today, while the real, spendable earnings of the average worker are stagnant or sinking.' Cited in 'Pay Gap Becoming Grand Canyonesque.'

8 Mitcham (1994) distinguishes 'Engineering philosophy of technology,' which emphasizes the internal structure or nature of technology, from the 'Humanities philosophy of technology,' which is concerned with the exter-

nal relations and meaning of technology. The humanities philosophy of technology is the most philosophical tradition, but it has failed to pay sustained or detailed attention to the actual dynamics of engineering and technology. This book must be situated in the latter tradition, but we pay close attention to the empirical and technological dynamics involved in Canadian policy debates.

1. The Philosophical Framework

1 We read about a new pathology in Japan called *karoshi*, a dis-ease connected to new technological production techniques. Japanese doctors define *karoshi* as 'a condition in which psychologically unsound work practices are allowed to continue in such a way that [they] disrupt the worker's work and life rhythms leading to a build up of fatigue and a chronic condition of overwork accompanied by a worsening of pre-existing high blood pressure, and finally resulting in fatal breakdown' (McCarthy, 1996, 16). *Karoshi* is the human fallout from people being forced to adapt to a nanosecond culture.

2 For a developed historical overview of the western philosophical natural rights tradition see Walters (1995a).

3 According to Richard Rorty, 'the most philosophy can do is 'summarize our culturally influenced institutions about the right thing to do in various situations' (Rorty, 1993, 117). We reject Rorty's view of human rights as mere 'sentimental story.' The ethical intelligibility of human rights may reach epistemological limits, but Rorty never adequately argues against the ethical justification of rights in response to ethical rationalism.

4 We have addressed the debate between MacIntyre and Gewirth at length in Walters (2001). We shall also return to the philosophical issues at stake in this debate in the conclusion.

5 The words 'non-substractive' and 'additive' as applied to the goods that persons possess are second-order, relational, aggregative expressions. They refer 'to goods in a certain quantitative relation to other goods, the relation obtained by comparing different states or stages of someone's possession of goods. If at time t some person A had X units of goods, and at time t_1 he also has the same X units of goods, then he has not lost any units. The relation between these two states is nonsubstractive. But since not to lose units of good is better than to lose some units, A thereby has a nonsubstractive good. "Nonsubstractive" here refers both to the relation between the two states and to the X units of good A still has in the latter state. If, on the other hand, at time t_1 A has X + 1 units of good, then A has gained a unit, and the

relation between the two states is additive. Hence, A has an additive good, where "additive" refers both to the relation between the two states and to the added unit of good' (Gewirth, 1978, 55).

6 The full structure of the argument to the Principle of Generic Consistency is diagrammed by Beyleveld (1991, 14):

STAGE I (Gewirth, 1978, 22–63)

A PPA claims (by definition)

(1) I do (or intend to do) X voluntarily for some purpose E.
By virtue of making this claim, the PPA rationally must consider that (claim) in logical sequence
(2) E is good;
(3) My freedom and well-being are generically necessary conditions of my agency;
(4) My freedom and well-being are necessary goods.

STAGE II (Gewirth, 1978, 63–103)

By virtue of having to accept (4), the PPA must accept

(5) I (even if no one else) have a claim right (but not necessarily a moral one) to my freedom and well-being. [Gewirth speaks of generic rights as prudential rights, and not yet moral rights at Stage II, since in order to show that they are moral rights it has to be shown that each agent must admit that all other humans also have these rights.]

STAGE III (Gewirth, 1978, 104–98, esp. 104–28)

By virtue of having to accept (5) on the basis of (1), the PPA must accept

(9) Other PPAs have a (moral) claim right to their freedom and well being.
If this is the case, then every PPA rationally must claim, by virtue of claiming to be a PPA,
(13) Every PPA has a (moral) claim right to its freedom and well-being, which is a statement of the PGC [i.e., the Principle of Generic Consistency].

7 Readers should consult Gewirth's (1996, 1–105) important and extensive argument to show that rights and community have a relation of mutual support, rather than being antithetical to one another, as is often held by communitarian philosophers. We presuppose his argument both here and throughout further references to the 'community of rights.'

2. Information Highway Policy and E-Commerce Strategy

1 For the telegraph industry, see Babe, 1990, 1996; Borchardt, 1970; Innis, 1923; Nichols, 1948; Rutherford, 1982; Thompson, 1947; for the telephone industry, see Britnell, 1934; Canada, House of Commons, 1905; CRTC, 1992, 1994; Grindlay, 1975; Fetherstonaugh, 1944; Surtees, 1992; for the broadcasting industry, see Barnouw, 1978; Danielian, 1974 [1939]; Kern, 1983; Troyer, 1980.

2 Their economic supposition is that 'improved productivity increases competitiveness which enhances growth, wealth creation, higher value-added employment and increased standard of living' (Johnston et al., 1995, 218). Government should develop an environment in which the private sector can truly innovate and to help create wealth and jobs, address market imperfections, and be a model user of information and information technologies. The private sector ought to invest in technology and people, Canadian citizens must be real-time users of IT, take charge of their own education, and view the I-way as a great opportunity to enhance life, liberty, and property.

3 Clement and Shade (1996) note how a project sponsored by Status of Woman Canada investigated access issues to the Internet by women's organizations across Canada. The project found that the elimination of barriers towards access involves ameliorating the financial constraints of organizations. With minimal funds to purchase equipment and training and limited time to develop online content, many women's organizations simply do not have the economic wherewithal for truly effective access. The access triumvirate of 'equity, affordability, and ubiquity' requires examination of network literacy and the diverse social variables that affect geographic, linguistic, income, gender, and class-based barriers. The development of emerging social mores surrounding the creation and maintenance of Internet substance and content is thus profoundly influenced by gender. One need only look at the way Internet software development has been driven by the cyberporn industry.

4 IHAC had earlier recommended that by the end of 1997 a national access strategy be set up to ensure affordable access for all Canadians to essential communications services. In support of this policy goal, the 'Call for a National Task Force on Universal Access' was charged with accomplishing, among others, six key tasks: (1) conduct and commission research into current and proposed access models including the successes and failures of existing initiatives and the effects of changing network technologies and economics; (2) consult with stakeholders whose views have been marginal-

ized by the consultative process; (3) identify an initial basket of 'essential network services,' recommend a process for revising what is 'essential' over time, and validate a mechanism for monitoring Canadians' access to and participation in the evolving information and communications infrastructure; (4) communicate task force findings in a timely manner and educate, inform, and involve the Canadian public with the relevant government, industry, and non-profit organizations; (5) determine the most effective way for Canadian content creators and providers in the old and new media sectors to produce high-quality material; (6) recommend a structure and an ongoing process for research, consultation, and evaluation of universal access in order to achieve the government's objective of 'making Canada the most connected nation in the world' (CNTFUA, 1997).

5 In 1998 Canada was second only to the United States in telephone mainlines and Internet Host Density in G7 countries, according to the *World Telecommunication Development Report* of the International Telecommunication Union (CECS, 1998).

6 Readers may consult the Industry Canada Electronic Commerce in Canada Web site at http://strategis.ic.gc.ca. This is the web page of the Task Force on Electronic Commerce, which contains other important initiatives and documents related to e-commerce use, news, global initiatives, and numerous legal and other e-commerce links such as the *Connecting Canadians* strategy, which comprises the federal government's original vision of making Canada the most connected country in the world.

7 The *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies* is intended to provide a framework for addressing new security threats of the post–Cold War world. 'Canada's export control guidelines were adopted as a national regime consistent with our international obligations as specified by COCOM (the Coordinating Committee for Multilateral Strategic Export Controls) of which Canada had been a member since 1950. COCOM was originally intended to preserve Western technological superiority by reducing the flow of military, dual-use and nuclear technologies from Western industrial nations to the Soviet bloc and other Communist countries. COCOM was abolished on March 31, 1994, and has been replaced by a modified agreement. Named after the town of Wassenaar, outside The Hague, where five rounds of negotiations took place between 1993 and 1995' (IC, 1998a, 9, n.14).

8 The World Intellectual Property Organization (WIPO) is an intergovernmental organization with headquarters in Geneva, Switzerland, and is one of sixteen specialized agencies of the United Nations system of organizations. WIPO is responsible for the promotion of the protection of intellec-

tual property throughout the world through cooperation among states and for the administration of various multilateral treaties dealing with the legal and administrative aspects of intellectual property. The two treaties are the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty.

9 Who are these groups? They include, among others: Action Network Society, Canadian Health Coalition, Canadian Teachers Federation, B.C. Civil Liberties Association, Council on Aging, BC Coalition of People with Disabilities, B.C. Freedom of Information and Privacy, Community Networks Association, Coalition for Public Information, Canadian Federation of Nurses, Canadian Labour Congress, Canadian Federation, Canadian Union of Public Employees, Centre for Law and Social Change, Democracy Watch, CUSO, Electronic Frontier Canada, Freedom of Information and Privacy Committee, Hospital Employees Union, National Action on the Status of Women, National Privacy Coalition, Ontario Senior Citizens' Organizations, Public Interest Advocacy Centre, and Rural Dignity of Canada.

10 Garth Graham (1995), a leader in community network development in Ottawa, notes that the National Capital FreeNet budget is c. $400,000 and the membership base exceeds 50,000 people. The actual operating cost on a per-person-served basis is only $8.00 per year! By the time this book goes to press, most community FreeNets will have all but given way to paid access providers.

11 Corporate social responsibility will have to adjust to the evolving concerns of cyberspace accountability and public interest. The Canadian Association of Internet Providers' 'Draft Code of Conduct' may be a step in the right direction by committing CAIP members not to 'knowingly host illegal content' and to sharing 'information about illegal content for this purpose' (CAIP, 1997, art. 5). Electronic Frontier Canada offers a 'constructive criticism' of the draft code (Jones, 1996).

12 MacIntyre defines a virtue as *'an acquired human quality the possession and exercise of which tends to enable us to achieve those goods which are internal to practices and the lack of which effectively prevents us from achieving any such goods'* (1984, 191). While there are difficulties with his notion of 'practice,' this distinction between internal and external goods is helpful. Various human activities and vocational practices lead to either *internal goods*, such as playing a near-perfect performance of a Mendelssohn concerto, or the rearing of healthy and virtuous children in the practice of running a household. Practices may also be directed by *external goods*, such as money, prestige, and pleasures of the palate. When the goods internal to a practice like

scientific research are exchanged or usurped by external goods, we have a dangerous situation.

13 Home-based telework is common in the United States, United Kingdom, Canada, and Australia, where 5–7 per cent of the working population work from home with a link to the employer. In Scandinavia there are similar levels of telework, but the working conditions and culture are different. Those who work from home are trusted by their employers to work wherever it is most convenient for them. In southern Europe, levels of telework are much lower because of higher telecommunications costs, extended-family structures, and a work culture that places a premium on face-to-face communication. In developing countries, where the costs of IT are greatest and are out of reach for all but the rich, telework is for the privileged few. Telematics have made it possible to shift work to many parts of the world, such as data processing outsourced to the Caribbean, to the Philippines, or to the other low-wage regions using satellite links to retransmit results to a parent company. Call centres are being concentrated in declining industrial regions such as the north of England, New Brunswick (Canada), and Tasmania (Australasia). In Europe, operators in call centres work across national boundaries, automatically routing calls to an operator who speaks the appropriate language for the region where the call originated. A campaign to unionize the United Parcel Service call centre in Dublin, Ireland, actually originated among German speakers who had been recruited to work there. The Germans were used to collective bargaining or 'social dialogue' wherein every workplace has a work council with trade union representation. The Germans were apparently shocked by the lack of consultation with workers under the lax Irish system (Huws, 1999).

3. The Informational Economy, Work, and Productive Agency

1 Gewirth labels this strong disjustification of property rights the 'inegalitarian harm thesis.' The thesis acts as a proviso against the absolutization of claim-rights to property. While this is not meant as an argument from authority, there do exist numerous examples of the thesis in western political philosophy: 'Rousseau's assertion about "civil liberty": "in respect of riches, no citizen shall ever we wealthy enough to buy another, and none poor enough to be forced to sell himself." To "buy another" who is "forced to sell himself" implies that the person bought becomes the property of the buyer, and hence akin to a slave. That capitalism in the nineteenth century reduced its workers to a condition akin to slavery was maintained not only by Marx but also by J.S. Mill: "The generality of labourers in this and most

other countries have as little choice of occupation or freedom of locomotion, are practically as dependent on fixed rules and on the will of others, as they could be on any system short of actual slavery"' (Gewirth, 1996, 176–7). Obviously these drastic economic inequalities referred to by Rousseau and Mill have been mitigated by modern welfare states, now under pressure by the informational economy. When a pitcher for the New York Yankees makes more money than the gross domestic product of Belize, and the wage gap between CEOs and workers has exponentially increased, it is obvious that inequalities of power and wealth still exist with harmful consequences for the freedom and well-being of others. One might argue that such inequalities serve as incentives to young athletes or entrepreneurs, who, in turn, make productive innovations that benefit the poor in the long run. While the concern for incentives is important, the gross inequalities that keep millions of human beings in conditions of abject poverty and economic insecurity are not justified. So the consequentialist disjustification of property rights still holds.

2 J.S. Mill condemns the 'inverse ratio' between labour and reward and the non-mutualist contrast between the idle rich and the working poor in this way: 'the present [1852] state of society with all its sufferings and injustices ... the institution of private property necessarily carried with it, as a consequence, that the produce of labour should be apportioned as we now see it, almost in an inverse ration to the labour – the largest portions to those who have never worked at all, the next largest to those whose work is almost nominal, and so in a descending scale, the remuneration dwindling as the work grows harder and more disagreeable, until the most fatiguing and exhausting bodily labour cannot count with certainty on being able to earn even the necessaries of life' (Mill, 1915, 2.I.3, 208; cited in Gewirth, 1996, 208). Gewirth cites Mill in this context to argue that the antecedentalist justification and purposive-labour thesis run up against problems when the vast property rights that corporate employers of labour amass in capitalist societies are considered. He is not criticizing capitalism as such, but rather is making the point that when a true comparison of the contributions made by workers and capitalists (i.e., owners of great wealth who supply capital for the productive process) is made, a far more equal distribution of the proceeds is justified. The same may be said of the unequal distributions that are operative between the First World informational economy and the so-called 'losers' of the Fourth World.

3 'Pay Gap Becoming Grand Canyonesque.'

4 We use the terms 'globalization' and 'informational economy' synonymously in this chapter.

5 During the outward oriented development strategy period of the early 1980s the 'right to development' was often a catch-all right, ideologically loaded either for western concerned citizens or for world-ruling elites, who blamed underdevelopment exclusively on western colonialism (Howard, 1989, 216).

6 The new market dynamics resulting from the Information Technology Agreement (ITA) have affected the growth of networked production, the shift in power from integrated producers to major users, and the competition to set market standards. Borrus and Cohen (1997) argue that recent changes in the dynamics of IT industries – including extremely rapid productivity gains (thus supporting the first of the three hypotheses, below, on the productivity paradox) – demand open markets. They use the Chinese electronics industry as a case study. In their discussion of tariff policy and China's accession to the World Trade Organization, they note that developing areas, such as Hong Kong, Taiwan, and Singapore, which have had low or no duties on electronics components and systems over the past two decades, have strong, vibrant economies. In contrast, developing areas with high duties, such as Latin America (Brazil) and India, have not been successful in developing their domestic electronics industries. Thus, in the view of Borrus and Cohen, a sector-free IT trade zone will help the entire world to shift from second wave to a third wave information society (cf. Toffler and Toffler, 1993).

7 See Walters (1997a) and Shade (1998a) for Canadian perspectives on access.

8 The primary goal of strategic information systems (SIS), interorganizational systems (IOS), and information partnerships is to provide organizations with a sustainable competitive advantage or leverage over competitors. This is done by raising entry barriers for the industry, building in switching costs, changing the basis of competition, and changing the balance of power in supplier relationships. In fact, a popular IOS can lead to industry restructuring by compelling smaller players to exit the market if they cannot afford to link up with the industry-wide system (Johnston and Vitale, 1988). Empirical studies suggest that 50–80 per cent of all strategic business alliances fall apart because of poor communication across companies, where one company does not really know the other's structure or direction. Poor communication leads to a lack of trust, which translates into non-commital relationships (Shaw, 1997, 18).

9 The 'end of work' thesis has also been espoused by Aronowitz and DiFazio (1994).

10 These thirty occupations include cashiers, janitors and cleaners, retail sales-

persons, waiters and waitresses, registered nurses, general managers and top executives, systems analysts, home health aides, guards, nursing aides, orderlies, attendants, secondary-school teachers, marketing and sales supervisors, teacher aides and educational assistants, receptionists and information clerks, truck drivers, secretaries (except legal and medical), clerical supervisors and managers, childcare workers, general utility maintenance repairers, elementary teachers, personal and home care aides, special ed. teachers, licensed practical nurses, food service and lodging managers, food preparation workers, social workers, lawyers, financial managers, computer engineers, and hand packers and packagers (Source: *Monthy Labour Review,* November 1995; cited in Henwood, 1996).

11 Statistics Canada / Statistique Canada. 'Labour Force Characteristics for Both Sexes, Aged 15 and Over.' September 2000. Available at: http://http://www.statcan.ca.

12 Friedman (1968) argues that the natural rate of unemployment is the level of unemployment at which inflation indeed exists but is not accelerated. Unemployment below the 'natural' level accelerates inflation. Unemployment above that level accelerates deflation. The policy implication is that unemployment should be held at this 'natural' rate. In the United States this is about 4–7 per cent, each percentage point representing about 1 million workers.

13 Other proponents of the 'no-work thesis' include Bloch, 1984, 1990; Gorz, 1985; Jenkins and Sherman, 1979; Offe, 1995; and Van Parijs, 1991.

4. Privacy and Security Policy: The Historical Situation

1 Section 3 of the Privacy Act defines 'personal information' as information about an identifiable individual that is recorded in any form, including, without restricting the generality of

(a) information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual,
(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
(c) any identifying number, symbol or other particular assigned to the individual,
(d) the address, fingerprints or blood type of the individual,
(e) the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or

a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations,

(f) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual,

(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (e), but excluding the name of the other individual where it appears with the views or opinions of the other individual, and

(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual, but, for the purposes of sections 7, 8 and 26 and section 19 of the Access to Information Act, does not include

(j) information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual including,

  (i) the fact that the individual is or was an officer or employee of the government institution,

  (ii) the title, business address and telephone number of the individual,

  (iii) the classification, salary range and responsibilities of the position held by the individual,

  (iv) the name of the individual on a document prepared by the individual in the course of employment, and

  (v) the personal opinions or views of the individual given in the course of employment,

(k) information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, the name of the individual and the opinions or views of the individual given in the course of the performance of those services,

(l) information relating to any discretionary benefit of a financial nature, including the granting of a licence or permit, conferred on an individual, including the name of the individual and the exact nature of the benefit, and

(m) information about an individual who has been dead for more than twenty years (PCC, 1991, 2–3).

2 In mid-June 1999 the House rose for its summer break, with Bill C-54 on the Order Paper for Third Reading. On 20 September 1999 the House prorogued and, as a result, the bill died on the order paper. On 12 October 1999 Parliament began a new session, and on 15 October 1999 the government reintroduced Bill C-54 as Bill C-6 at report stage. The bill was passed by the House of Commons on 26 October 1999 and passed in the Senate on 9 December 1999. The amendments to define personal health information and to delay implementation of C-6 to such information for one year were adopted on 7 February 2000.

3 The Canadian Marketing Association, the Information Technology Association of Canada, and the banking industry have publicly supported Bill C-6. The B.C. Civil Liberties Association (BCCLA) and the Freedom of Information and Privacy Association (FIPA) are part of a larger coalition that supports the bill and includes the Canadian Health Coalition, Electronic Frontier Canada, the University of Ottawa's Human Rights Research and Education Centre, and the Ottawa-based Public Interest Advocacy Centre (PIAC).

4 The privacy commissioner is the officer of Parliament responsible for supervising the application of the Privacy Act regulating the collection, use, and disclosure of personal information by federal government institutions. The Privacy Commission investigates complaints by individuals about the handling of their personal information by government institutions, and conducts audits of government institutions to promote their compliance with the act. Although it has no formal research and education role, the commission has been at the forefront in exploring the panoply of privacy issues raised by advances in technology and shifts in public policy.

5 Of the 20,000 complaints handled by the privacy commissioner of Canada since 1983, fewer than twelve have required recourse to the courts. For this reason, the privacy commissioner of Canada, Bruce Phillips, sees his office less as a police department than a 'problem solver,' whose approach has been 'non-confrontational and non-adversarial' (Phillips, 1999). The commissioner's approach will be even more necessary in its dealings with the private sector, and it moves in the right direction in accordance with the norms of mutuality and social solidarity at the heart of the community of rights.

6 Section 4.3.6 of the CSA code states: 'The way in which an organization seeks consent may vary, depending on the circumstances and the type of

information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney)' (CSA, 1996).

7 McMurty (1998) chastises what he sees as our contemporary situation, in which the 'money-sequence of value' produces little use value between investment and profit moments. The name of the game in the informational economy is 'to maximize money or money-equivalent holdings *as a good in itself* as a condition in which life's requirements do not restrain choices by an recognized override of value' (31; emphasis in original). If this is true, then the negative implications for privacy rights and policy are obvious.

5. Privacy and Security: An Ethical Analysis

1 Fried (1984) argues that EM presents opportunities for malice and misunderstanding on the part of authorized personnel. The monitored subject is threatened by an unseen audience where intimate revelations could be heard by monitoring officials. EM undermines the parolee's capacity to enter relations of trust and is thus denied a sense of self-respect inherent in being trusted by the government that released him. The subject is unable to enter into true relations of trust with persons outside the prison. Fried also distinguishes the roles of privacy inside and outside the prison in response to the argument that prison life is surely more intrusive than being monitored outside the prison. In his view, the prison environment is overtly punitive and is not private, which changes the contexts for relations with others. Prisoners with a reasonably developed capacity for love, trust, and friendship are aware of this fact. With EM, by contrast, the subject merely appears free and cannot really be free, because he lacks autonomy and is forced to make at least a show of intimacy to others with whom he works or with would-be friends. If parolee tries to be intimate or 'give himself away,' he violates his own integrity by revealing his own most self to his official monitors, which his private most personality would reserve for others. Conversely, the subject might be forced to withdraw and thus seem cold or odd to others from who he craves esteem and affection. However, Fried's argument incurs difficulties. He presupposes that authorities have technological access to a parolee's intimate thoughts, not simply their movements, which is not the case in Ontario and Canadian EM practices. This fact weakens Fried's argument against EM on the basis of intimate trust. Authorities may know that Smith is in his girlfriend's house, but they need

not know intimate details of their actions. Second, what if the parolee freely consents and judges EM to be a preferable state of affairs to imprisonment? Fried cannot close off this alternative and still maintain his concern with liberty and the respect for persons.

2 One member of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities heard testimony from two pregnant women in New Brunswick who faced the possibility of delivering children with disabilities. They were instructed to submit to psychiatric evaluation when they refused to undergo genetic fetal testing. Another participant interviewed told of an American health insurer who refused to pay for the health care of a Down's Syndrome child because genetic tests prior to the birth indicated that the baby was at risk. 'The insurer hadn't been willing to assume that risk and had advised the mother to terminate the pregnancy. Once the baby was born, the insurer washed its hands of the matter' (Steeves, 1998, 3). The fact that this testimony is anecdotal, does not nullify the ethical concerns involved.

3 Bennett, 1992; Burnham, 1983; Cavoukian and Tapscott, 1995; Flaherty, 1989, 1991; Freedman, 1987; Linowes, 1989; Regan, 1993, 1995; Robertson, 1973; Schoeman, 1984; Westin, 1967; Westin and Baker, 1972.

4 The human rights framework we advocate must not be confused with a 'personalist' morality defined as consisting in counsels or precepts for living a good life that fulfils an individual's intellectual, esthetic, and other capacities in ways that contribute only to the individual's development and dignity. In this definition of morality, there is 'no direct or necessary reference to the goods or desires of persons other than the individual agent, and there is no necessary appeal from the agent's own desires to the desires or needs of other persons' (Gewirth, 1998, 54). Some extreme libertarian calls for freedom of speech on the Internet as well as views that the dominant role of the information highway is to provide for the autonomous and self-serving desires of the individual qualify as 'personalist' moralities as here defined.

5 Gewirth defines 'moral indeterminacy' in the context of his debate with MacIntyre on the question of the relation between human rights and the virtues, and the role of deontological and teleological approaches in ethical theory. A quality, rule, or judgment is morally indeterminate, according to Gewirth, 'when its content allows or provides outcomes which are mutually opposed to one another so far as concerns their moral status. Thus the content in question may be morally wrong as well as morally right.' When this definition is applied to the virtues, the problem is often that 'the criterion for a quality's being a virtue does not include the requirement that the

virtue reflect or conform to moral rules, [and thus] there is no assurance that the alleged virtue will be morally right or valid' (Gewirth, 1985, 752).

6 For human behaviours to be actions in a strict philosophical sense and at the same time be voluntary or free, certain causal conditions must be fulfilled. Stated negatively, the behaviours must not occur from one or more of the following kinds of cause: '(a) direct compulsion, physical or psychological, by someone or something external to the person; (b) causes internal to the person, such as reflexes, ignorance, or disease, that decisively contribute, in ways beyond his control, to the occurrence of the behavior; (c) indirect compulsion whereby the person's choice to emit the behavior is forced by someone else's coercion' (Gewirth, 1978, 31). Stated positively, the person must control her behaviour by her own unforced and informed choice.

7 Fair information practices pose their own set of ethical questions related to the principles upon which these practices are formed. For example, the principle of 'limiting collection' seeks to limit information 'to that which is necessary for the purposes identified by the organization' (IC, 1998b, 13). Neither the practices nor the principles themselves, however, are able to determine the meaning of 'necessity' and by which set of criteria necessity is to be defined and evaluated. If the determination of 'necessity' is defined by the 'purposes' of the organization, who, we must ask, will regulate the values of the organization? Who will guard the guardians? The set of questions that Marx (1999, 44–5) brings to the means, data collection context, and uses of information is exceedingly perceptive and helpful in this regard.

8 A Georgia Tech Internet Survey (1999) of 15,000 respondents cited this reason (70.15 per cent), as well as lack of trust in the collecting site (62 per cent), while a 1996 Equifax survey found that less than one-third of the respondents believed that the providers of Internet services should be able to track users on the Internet in order to send them targeted marketing offerings. Nearly half of the respondents (48 per cent) felt they should be able to use the Internet without disclosing their personal identity. Because young children are also online users, there was and is particular concern about the reuse of information disclosed by children about themselves and their families without parental consent (cited in Harris, 1996).

9 The difficulties of changing advertising and marketing habits should not be underestimated. As Burkert notes: 'Contrary to popular belief, advertising and direct marketing seem to be among the most conservative industries if judged by the amount of money these industries have spent so far on avoiding regulatory change' (1998, 134).

10 We agree with the intuitive reservations of Flaherty: 'Although I have a

congenital dislike for the notion that one should be allowed to sell one's privacy to the highest bidder, almost everything else is for sale in our capitalistic societies. In this case, in fact, we have been giving away our personal, private information for free, because we were not smart enough to insist on payments for its use at the outset' (1999, 34).

11 Burkert's definition of PETs starts from the observational supposition that personal information is being accumulated in transactions between individuals or by means of observing such transactions. This observation provides the basis for his differentiation of four types of PET concepts related to subject-object, object-oriented, action-oriented, and system-oriented concepts. Subject-oriented concepts seek to eliminate or reduce the ability to identify the acting subject(s) in transactions (using proxies). Object-oriented concepts build on the observation that transactions often involve exchange or barter. A given object in an exchange carries traces that allow for identification, so the aim is to free the exchanged object from all such traces (e.g., money in the form of cash). Transaction-oriented concepts seek to address the transaction process left behind, without directly addressing the objects being exchanged (e.g, videotaping of over-the-counter cash dealings at the bank). Systems-oriented concepts seek to integrate some or all of the former elements. Zones of interaction are created where the identity of subjects is hidden, the objects exchanged cannot be traced to those handling them, and no record of the interaction is created or maintained (e.g., Catholic confession, anonymous interactions with crisis intervention centres, anonymous e-mail subsequently destroyed by all parties and carriers). What is most fascinating about his detailed analysis is the conclusion that PETs actually force human beings to return to 'social innovation' and, specifically, *trust* as a 'conscious decision to interact *although* there is risk' (Burkert, 1998, 139; emphasis in original).

12 Cavoukian offers the following procedural and technical safeguards for encrypted finger scans: '1. Restricting the use of the biometric information to authentication of eligibility only, thereby ensuring that it is not used as an instrument of social control or surveillance; 2. Ensuring that a fingerprint cannot be reconstructed from the encrypted finger scan stored in the database; 3. Ensuring that a latent fingerprint (that is, picked up from a crime scene) cannot be matched to an encrypted finger scan stored in a database; 4. Ensuring that an encrypted finger scan cannot itself be sued as a unique identifier; 5. Ensuring that strict controls are in place as to who may access the information and what it is used for; 6. Requiring the production of a warrant or court order prior to permitting access by external agencies such as the police or other government departments; 7. Ensuring

that benefits data (personal information, for example, history of payments made) is stored separately from personal identifiers such as name or date of birth, etc.' (1999, 125–6).

13 Since the Nuremberg trials in Germany, the issue of informed consent has been at the forefront of bioethics, but the term did not appear until a decade after these trials. In recent years a shift has occurred from the physician's or the researcher's obligation to disclose information to the quality of a patient's or subject's understanding and consent. Some commentators reduce the meaning of informed consent to mutual decision making between doctor and patient. This is a good idea when consent involves ongoing exchanges of information between a doctor and a patient. In addition to what has been said earlier about the roles of disclosure, understanding, and voluntariness, we want to stress the temporal process, since a signed consent form is not the essence of consent in either the medical or the Internet context. Informed consent includes competence, disclosure, understanding, voluntariness, and consent. In the present context, end-user competence, full organizational or e-commerce business disclosure, and end-user understanding are vital if the ethical requirements of e-commerce and medical record informed consent are to be met properly.

6. Information Warfare

1 As one high-ranking Department of National Defence official put the matter to us during a conference on information warfare: What are officials supposed to do when transnational criminal groups have more money than the Canadian government has to spend on sophisticated encryption technologies put to use for criminal activity?

2 Much of the hype around the so-called RMA stems from analyses of the Gulf War, like Stephen Biddle's commentary on the Battle of 73 Easting. A small contingent of American forces composed of 9 M1 tanks and 12 M3 Bradleys defeated a much larger Iraqi force. The Iraqi's lost some 113 armoured vehicles, while the Americans lost 1 Bradley to enemy fire and another vehicle to 'friendly fire.' The synergy between RMA technology and skilful tactics led to the radical outcome of this battle (Biddle, 1996, 144–7).

3 Some argue that while the RMA is real, the feeding frenzy around IW security issues is mere hype, serving declining military budgets. The common view that the post–Cold War world is marked by 'chaos' is a myth about the collapse of Communism, bipolarity, and a nuclear stalemate. Thus, the world order created in the middle to late 1940s – including the commitment

to an open world economy and its multilateral management and the stabilization of socio-economic warfare – is alive and well (Ikenberry, 1996).

4 Christine A.R. MacNulty, chief operating officer of applied futures in the United States and the United Kingdom, maintains that while technological IW operations are important and should be pursued, they are not the most important aspect. IW is really about individuals' and organizations' objectives, priorities, vulnerabilities, and fears. Her psychological model, based on Maslow's hierarchy of needs, looks behind technology to understand human motivations in order to develop a 'vision' and a 'set of the principles' that form a basis for response in the whole IW field. Only by understanding the 'inner directed,' 'outer directed,' and 'sustenance driven' values of individuals are we able to observe and understand societal development and assess societal behaviour. Technological solutions alone are insufficient. Organizational composition, structure, training, and procedures formulated in the context of a potential threat are equally important. There is substantial gain to be realized through the exchange of ideas between organizations and across various boundaries (MacNulty, 1996).

5 In contrast, Constable Gil Puder of the Vancouver police force sees the RCMP's 'war on drugs' as a bust, which merely serves to legitimate police budgets. 'An effective method of evaluating the drug war is to examine its impact on the collective integrity of our calling. A renowned ethicist has found that "integrity in the context of police work should amount to the sum of the virtues required to bring about the general goals of protection and service to the public." If we examine drug enforcement practices, such virtues are sadly lacking, which raises uncomfortable issues of character and professionalism' (Puder, 1998, A15).

6 The American Electronic Privacy Information Center (EPIC) filed legal suit against the National Security Agency (NSA) in December 1999 on the grounds that the NSA has engaged in the indiscriminate acquisition and interception of domestic communications taking place on the Internet. The EPIC suit attempts to make available documents regarding the legal justification for any surveillance that NSA had performed on U.S. citizens. The same documents sought in the suit were requested earlier in the year by the House Intelligence Subcommittee, but NSA refused to provide them (Lemos, 1999).

7 STOA's five-volume report is a 'working document' commissioned by the European Parliament's Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (formerly the Committee on Civil Liberties and Internal Affairs). It is the logical continuation of an earlier study published

in September 1998, *An Appraisal of Technologies of Political Control*, drawn up by the Manchester, England, based OMEGA Foundation (STOA, 1998). The mandate of the STOA report complies with the earlier study in reporting on 'the impact of electronic surveillance in the European Union which will enable the institutions and, in particular, Members of the European Parliament to understand and comprehend the current state of the equipment used in and the use made of electronic surveillance so that they will have all the information they need to put in place legislation which will provide enhanced respect for the confidentiality of communications and also eliminate as far as possible the economic risks which may arise from such interceptions and from free competition' (EP, 1999, vol. 1/5). The original draft is published in French.

8 COMINT involves the 'covert interception of foreign communications [and] has been practised by almost every advanced nation since international telecommunications became available. Comint is a large-scale industrial activity providing consumers with intelligence on diplomatic, economic and scientific developments ... Globally, about 15–20 billion Euro is expended annually on Comint and related activities' (EP, 1999, vol. 2/5, 4).

9 The Peruvian and Ecuadorian governments, not particularly noted for their technological sophistication, were the first to bring international diplomacy on-line. Swett insinuates that groups such as the Institute for Global Communications (IGC) and the Association for Progressive Communications (APC) and its systems of networks, such as PeaceNet, EcoNet, ConflictNet and LaborNet, are 'left-wing' political organizations. They will play a significant, albeit slanted, role in filling gaps left in reporting done by the mainstream news media. Swett disapprovingly cites the mission statement of IGC News Service, which 'gathers and distributes alterative news and information to clients in the United States and abroad through a global network of distributed computers ... IGC News Service is part of a worldwide network connecting primarily non-governmental organizations, alterative press and community broadcasters and is dedicated to the free flow of information, human rights and environmental preservation. IGC's regional and issue-oriented conferences serve as a repository for news, analysis, *calls for action* and networking activities about that issue or region' (Swett, 1995; emphasis added). Is Swett's concern with IGC's dedication to the free flow of information, human rights, environmental preservation, and calls to action because it poses a threat to the Pentagon's Special Operations and the waging of Low-Intensity Conflict in the Third World? It is difficult to believe that the IGC News Service is a truly serious threat to Pentagon power, but one should not fault strategic bureaucrats for trying to do their jobs and pay off their mortgages in good faith.

7. Information Warfare and Deterrence

1 Key elements of the argument set forth in this section have been adapted to the present information age situation. We acknowledge our indebtedness, however, to Professor Gewirth (1986) for the structural elements of the argument.
2 For the difficulties incurred by these attempts and others at reconciling instrumental rationality and reasonableness, see Gewirth (1983).
3 'Is the epistemological end state to be reached all at once, everywhere, or are there interim states that need to be reached in specific geographical areas, in a specific sequence, or in specific sectors of information activity? ... Leaders at the operational level need to know when attacks will be terminated and the means by which the termination order will be communicated. These are important questions because information weapons, depending on the weapons used, may cause collateral damage to the attacker's knowledge and belief systems' (Szafranski, 1995, 56–65).
4 Prime Minister Pierre Elliott Trudeau's purchase of the German Leopard tanks for Canadian deployment is a case in point. It had very little to do with a putative rational assessment of Canadian Forces' needs, and everything to do with the Trudeau government's 'Third Option' policy. The Third Option was a process adopted in response to concern about growing Canadian economic dependence on the United States. The tank purchase sought to institutionalize an economic contractual link with the EC. It was only when Trudeau agreed to the tank purchase that the Europeans agreed to sign the contractual link in 1976. Canada's force posture, procurement of weapons systems, and alignments in international politics often are shaped not by defence requirements but by a large mix of motives and interests.
5 Why compete, for example, in expensive marketing contests when it is possible to disrupt R&D projects by means of well-placed computer viruses before production even begins (Denning, 1990)?
6 See above, chapter 1, for the definition of 'mutuality' that figures in our human rights framework.
7 When asked in 1974 whether he was sorry that the United States had developed MIRVs in 1969, Henry Kissinger replied: 'Well, that's a good question. And I think that is the same question people faced when the hydrogen bomb was developed. And it raises the issue whether your development of MIRVs or of a weapon produces the development on the other side, or whether by not going ahead you then simply give the advantage to the other side ... *I would say in retrospect that I wish I had thought through the implications of a MIRVed world more thoughtfully in 1969 and 1970 than I did*' (cited in Blacker and Duffy, 1984, 237–8; emphasis added).

This page intentionally left blank

References

Abelson, Hal, et al. 1998. *The Risks of Key Recovery, Key Escrow, & Third Party Encryption.* A Report by an Ad Hoc Group of Cryptographers and Computer Scientists. Updated version, 8 June. Available at http://www.crypto.com/key_study/report.shtml.

Agassi, Joseph. 1985. *Technology: Philosophical and Social Aspects.* Vol. 11, *Episteme*, ed. Mario Bunge. Dordrecht, Boston, Lancaster, Tokyo: D. Reidel.

Agre, Philip E., and Marc Rotenberg, eds. 1998. *Technology and Privacy: The New Landscape.* Cambridge, Mass., and London, England: MIT Press.

Agre, Philip E., and Douglas Schuler. 1997. *Reinventing Technology, Rediscovering Community: Critical Explorations of Computing as a Social Practice.* Greenwich, Conn., and London, England: Ablex Publishing.

Aldrich, Richard W., Maj., USAF. 1996. 'The International Legal Implications of Information Warfare.' INSS Occasional Paper 9 in the Information Warfare Series, April. USAF Academy, USAF Institute for National Security Studies, Colorado Springs, Colo. Available at: http://www.cdsar.af.mil/apj/aldricha.html.

Alexander, Catherine M. 1998. 'National Security Issues in a Wired World.' In *Digital Democracy: Policy and Politics in the Wired World*, ed. Cynthia J. Alexander and Leslie A. Pal. Toronto and New York: Oxford University Press.

Al-Khalil, Samir. 1990. *Republic of Fear: The Inside Story of Saddam's Iraq.* New York: Pantheon Books.

Alston, Philip. 1992. 'Peace as a Human Right.' In *Human Rights in the World Community: Issues and Action.* 2d ed. ed. Richard Pierre Claude and Burns H. Weston. Philadelphia: University of Pennsylvania Press.

Aly, Shala. 1997. 'Surfing for Dollars.' *Financial Post 2000: Report on the Nation-Internet Commerce*, 11 October, 8–9, 12.

Andrews, Rodney O. 1989. 'Computer Crime: The Worm in the Apple.' In *The Information Web: Ethical and Social Implications of Computers*, ed. Carol Gould. Boulder, Colo.: Westview Press.

Angus, Elizabeth, and Duncan McKie. 1994. *Canada's Information Highway: Services, Accessibility and Affordability.* A Policy Study prepared for the New Media Branch and Information Technologies Industry Branch, Industry Canada, May.

An-Na'im, Abdullahi Ahmed. 1992. 'Toward a Cross-Cultural Approach to Defining International Standards of Human Rights: The Meaning of Cruel, Inhuman, or Degrading Treatment or Punishment.' In *Human Rights in Cross-Cultural Perspectives: A Quest for Consensus*, ed. Abdullahi Ahmed An-Na'im. Philadelphia: University of Pennsylvania Press.

Arendt, Hannah. 1958. *The Human Condition.* Chicago: University of Chicago Press.

– 1963. *Eichmann in Jerusalem: A Report on the Banality of Evil.* New York: Penguin Books.

Aristotle. 1924. *Metaphysics.* Greek revised text with introduction and commentary by W.D. Ross. Oxford: Clarendon Press.

– 1980. *The Nichomachean Ethics.* Trans. David Ross; rev. J.L. Ackrill and J.O. Urmson. Oxford: Oxford University Press.

Arndt, H.W. 1949. 'The Cult of Privacy.' *Australian Quarterly* 21, 3 (Sept.): 69–71.

Aronowitz, Stanley, and William Difazio. 1994. *The Jobless Future: Sci-tech and the Dogma of Work.* Minneapolis: University of Minnesota Press.

Arquilla, John. 1999. 'Ethics and Information Warfare.' Forthcoming, *Strategic Assessment: Information Warfare.* Washington, D.C.: Government Printing Office.

Arquilla, John, and David Ronfeldt. 1997a. 'Cyberwar Is Coming!' In *In Athena's Camp: Preparing for Conflict in the Information Age.* Santa Monica, Ca: RAND. Also in *Comparative Strategy* 12, 2 (Spring 1993): 141–65.

– eds. 1997b. *In Athena's Camp: Preparing for Conflict in the Information Age.* Santa Monica, Calif.: RAND.

Arunachlam, Subbiah. 1998. 'Information Age Haves & Have-Nots.' *Educom Review* 33, 6 (Nov./Dec.): 40–5.

Babe, Robert. 1979. *Canadian Television Broadcasting Structure, Performance and Regulation.* Ottawa: Supply and Services for the Economic Council of Canada.

– 1990. *Telecommunications in Canada: Technology, Industry and Government.* Toronto: University of Toronto Press.

– 1995. *Communication and the Transformation of Economics: Essays in Information, Public Policy, and Political Economy.* Boulder, Colo.: Westview Press.

Ball, Patrick, Mark Girouard, and Audrey Chapman. 1997. 'Information Technology, Information Management, and Human Rights: A Response to Metzl.' *Human Rights Quarterly* 19:836–59.

Bambrough, Renford. 1984. 'The Roots of Moral Reason.' In Edward Regis Jr, *Gewirth's Ethical Rationalism*. Chicago: University of Chicago Press.

Banisar, David. 1996. 'Big Brother Goes High-Tech.' *Covert Action Quarterly* 56 (Spring) 6–10.

Barbour, Ian. 1993. *Ethics in an Age of Technology: The Gifford Lectures 1989–1991*. Volume 2. San Fransisco: HarperCollins.

Barlow, John Perry. 1996. 'A Declaration of The Independence of Cyberspace.' Available at: http://www.eff.org/homes/barlow.html.

Barnouw, E. 1978. *The Sponsor: Notes on a Modern Potentate*. New York: Oxford University Press.

Bayefsky, Anne F., and Mary Eberts, eds. 1985. 'The Canadian Bill of Rights.' In *Equality Rights and the Canadian Charter of Rights and Freedoms*. Toronto: Carswell.

Beauchesne, E. 1997. 'Economy Churns out Products, Not Jobs: Producers Increase Output Without Boosting Workforce.' *Ottawa Citizen*, 8 March, E3.

Beck, Nuala. 1992. *Shifting Gears: Thriving in the New Economy*. Toronto: HarperCollins.

Benn, Stanley I. 1984. 'Privacy, Freedom, and Respect for Persons.' In *Philosophical Dimensions of Privacy: An Anthology*, ed. Ferdinand D. Schoeman. Cambridge: Cambridge University Press.

Bennett, Colin. 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. New York: Cornell University Press.

– 1996. 'Rules of The Road and Level-playing Fields: The Politics of Data Protection In Canada's Private Sector.' *International Review of Administrative Sciences* 62 (Dec.): 481–2.

Bennett, Colin, and Rebecca Grant. 1999. *Visions of Privacy: Policy Choices for the Digital Age*. Toronto: University of Toronto Press.

Bentham, Jeremy. 1928. *Theory of Legislation*, ed. C.K. Ogden. London: Routledge and Kegan Paul.

Benzanson, K., and F. Sagasti. 1995. 'The Elusive Search: Development and Progress in the Transition to a New Century.' Mimeo. Ottawa: International Development Research Centre and Lima Peru: GRADE.

Beyleveld, Deryck. 1991. *The Dialectical Necessity of Morality: An Analysis and Defense of Alan Gewirth's Argument to the Principle of Generic Consistency*. Chicago: University of Chicago Press.

Biddle, Stephen. 1996. 'Victory Misunderstood: What the Gulf War Tells Us about the Future of Conflict.' *International Security* 21, 2 (Fall): 139–79.

'Bill of Rights and Responsibilities for the Electronic Community of Learners.' 1995. In *Human Rights in Theory and Practice: A Selected and Annotated Bibliography*, ed. Gregory J. Walters. Metuchen, N.J., London, England, Pasadena, Calif., and Englewood Cliffs, N.J.: Salem Press.

Blacker, Coit D. and Gloria Duffy, eds. 1984. *International Arms Control: Issues and Agreements*. 2d ed. Stanford, Calif. Stanford University Press.

Blaker, James R. 1997. *Understanding the Revolution in Military Affairs: A Guide to America's 21st Century Defense*. Washington, D.C.: Progressive Policy Institute, January.

Bloch, Fred. 1984. 'The Myth of Reindustrialization.' *Socialist Review* 14, 1 (Jan.–Feb.): 59–79.

– 1990. *Postindustrial Possibilities*. Berkeley and Los Angeles: University of California Press.

Bloustein, Edward J. 1984. 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser.' In *Philosophical Dimensions of Privacy*, ed. Ferdinand D. Schoeman. Cambridge: Cambridge University Press.

Blume, Lawrence E. 1998. 'On the Economic Impact of the Information Revolution.' In *The Information Revolution and International Security*, ed. Ryan Henry and C. Edward Peartree. Washington, D.C.: Center for Strategic & International Studies.

Borchardt, K. 1970. *Structure and Performance of the U.S. Communications Industry*. Boston, Mass.: Harvard University Press.

Borrus, Michael and Cohen, Stephen S. 1997. 'Building China's Information Technology Industry: Tariff Policy and China's Accession to the WTO.' Working Paper 105. Paper presented at the Third Meeting of the Trilateral Forum, Berkeley, Calif., 11–12 November. Available at: http:/brie.berkeley.edu/BRIE/pubs/wp/wp105.html#2.

Bowden, Brian P. 1991. 'Rights of Anonymity and Rights of Solitude: Ethical Information Management in the Private Sector.' *Canadian Public Administration* 34, 1:101–10.

Boylan, Michael, ed. 1999. *Gewirth: Critical Essays on Action, Rationality, and Community*. Lanham, Boulder, New York, Oxford: Rowman & Littlefield.

Britnell, G.E. 1934. Public Ownership of Telephones in the Praire Provinces. Master's thesis, University of Toronto.

Bronskill, Jim. 1999. 'CSIS Probes Cyber Warfare.' *Ottawa Citizen*, 25 January, A1–A2.

Brownlie, Ian. 1990. *Principles of Public International Law*. 4th ed. Oxford: Clarendon Press.

– ed. 1981. *Basic Documents on Human Rights*. 2d ed. Oxford: Clarendon Press.

Brunker, Mike. 2000. 'Vast Online Credit Card Theft Revealed: Hacker Hid

Data on 485,000 Cards on U.S. Agency's Web Site.' MSNBC. Available at: http://www.msnbc.com/news/382561.asp.

Brynjolfsson, Erik, and Lorin Hitt. 1993. 'Is Information Systems Spending Productive? New Evidence on the Returns to Information Systems.' Working Paper No. 3571–93. Cambridge, Mass.: Sloan School, MIT, 4 June.

Bunker, Robert J., ed. 1996. Nonlethal Weapons: Terms and References. INSS Occasional Paper 15. USAF Academy, Institute for National Security Studies, Colorado Springs, colo. Available at: http://www.infowar.com/RESOURCE/res_100997a.html.

Burkert, Herbert. 1998. 'Privacy-Enhancing Technologies: Typology, Critique, Vision.' In *Technology and Privacy: The New Landscape*, ed. Philip E. Agre and Marc Rotenberg. Cambridge, Mass. and London, England: MIT Press.

Burnham, David. 1983. *The Rise of the Computer State: The Threat to Our Freedom, Our Ethics and Our Democratic Process*. New York: Random House.

Burstein, Daniel, and David Kline. 1995. *Road Warriors: Dreams and Nightmares along the Information Highway*. New York and Toronto: Dutton Signet.

CAIP. 1997. Canadian Association of Internet Providers. 'Code of Conduct.' Available at: http://www.caip.ca/caipcode.html.

Campen, A.D., ed. 1992. *The First Information War: The Story of Communications, Computers, and Intelligence Systems*. Fairfax, Va.: AFCEA International Press.

Canada. *Charter of Rights and Freedoms: A Guide for Canadians, The*. 1982. Ottawa: Publications Canada.

- Department of Communications. 1971. *Instant World: A Report on Telecommunications in Canada*. Ottawa: Information Canada.
- HC. House of Commons. 1905. House of Commons Select Committee on Telephone Systems. *Proceedings*. Ottawa: King's Printer.
- HC. 1987. House of Commons Standing Committee on Justice and the Solicitor General. First Report, *Open and Shut: Enhancing the Right to Know and the Right to Privacy*. 2nd Session, 33rd Parliament, March.
- HC. 1997. Report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities / Comité Permanent des Droits de la Personne et de la Condition des Personnes Handicapées. *Privacy: Where Do We Draw the Line? La vie privée: où se situe la frontière?* Ottawa: Travaux publics et Services gouvernementaux, April.
- Senate. 2000. 'Senator Sheila Finestone Calls on Canadians to Support Rights-Based Privacy Charter/La Sénatrice Sheila Finestone demande à la population d'appuyer un projet de loi sur le respect de la vie privée.' Press Release. August 29.
- Senate. 1999. Proceedings of the Standing Senate Committee on Social Affairs, Science and Technology. Chairman: The Hon. Michael Kirby.

Subject matter: Bill C-6. Issues 1–6, Wednesday, 17 November to Monday, 6 December.

Cardoso, F.H. 1993. 'North-South Relations in the Present Context: A New Dependency?' In *The New Global Economy in the Information Age: Reflections on Our Changing World*, ed. Martin Carnoy et al. University Park: The Pennsylvania State University Press.

Carnoy, Martin, Manuel Castells, Stephen S. Cohen, and Fernando Henrique Cardosa. 1993. *The New Global Economy in the Information Age: Reflections on Our Changing World*. University Park: The Pennsylvania State University Press.

Castells, Manuel. 1993. 'The Informational Economy and the New International Division of Labor.' In *The New Global Economy in the Information Age: Reflections on Our Changing World*, ed. Martin Carnoy, Manuel Castells, Stephen S. Cohen, Fernando Henrique Cardosa. University Park: Pennsylvania State University Press.

– 1996. *The Information Age: Economy, Society and Culture*. Vol. I, *The Rise of the Network Society*. Oxford, England, and Malden, Mass.: Blackwell Publishers.

– 1997. *The Information Age: Economy, Society and Culture*. Vol. II, *The Power of Identity*. Oxford, England, and Malden, Mass.: Blackwell.

– 1998. *The Information Age: Economy, Society and Culture*. Vol. III, *End of Millennium*. Oxford, England, and Malden, Mass.: Blackwell Publishers.

Cavoukian, Ann. 1994. 'Genetic Privacy: The Right "Not to Know."' Paper presented at the 10th World Congress on Medical Law, Jerusalem, 28 Aug.–1 Sept.

– 1999. 'The Promise of Privacy-Enhancing Technologies: Applications in Health Information Networks.' In *Visions of Privacy: Policy Choices for a Digital Age*, ed. Colin J. Bennett and Rebecca Grant. Toronto, Buffalo, London: University of Toronto Press.

– 2000. 'Biometrics Backgrounder: Fingerprints vs. Finger Scans.' Available at: http://www.ipc.on.ca.

Cavoukian, Ann, and Don Tapscott. 1995. *Who Knows: Safeguarding Your Privacy in a Networked World*. Toronto: Random House of Canada.

CECS. 1998. *The Canadian Electronic Commerce Strategy*. Industry Canada/Industrie Canada. Electronic Commerce in Canada, the Web site of the Task Force on Electronic Commerce. Available at: http://e-com.ic.gc.ca.

Chataway, B., and A. Cooke, 1995. 'Measuring the Impact of Information on Development: Related Literature, 1993–1995.' In *Making a Difference: Measuring the Impact of Information on Development*, ed. Paul McConnell. Proceedings of a Workshop held in Ottawa, Canada, 10–12 July. Available at: http://www.idrc.ca/books/focus/783/.

Clarke, Roger. 1988. 'Information Technology and Dataveillance.' *Communications of the ACM* (May): 498–512.

– 1994. 'The Digital Persona and Its Application to Data Surveillance.' *Information Society* 10, 2: 77–92.

Clarke, Tony, and Maude Barlow. 1997. *MAI – The Multilateral Agreement on Investment and the Threat to Cultural Sovereignty.* Toronto: Stoddart.

Claude, Richard Pierre, and Burns H. Weston, eds. 1992. *Human Rights in the World Community: Issues and Action.* 2d ed. Philadelphia: University of Pennsylvania Press.

Cleaver, Barry, et al. 1992. *Handbook Exploring the Legal Context for Information Policy in Canada.* Toronto: Faxon Canada.

Clement, Andrew, and Leslie Regan Shade. 1996. 'What Do We Mean by "Universal Access"? Social Perspectives in a Canadian Context.' Proceedings of INET96, Montreal, 25–28 June. URL: http://info.isoc.org/isoc/whatis/conferences/inet/96/proceed ings/f2/f2_1.htm.

CMA. 1998. 'Canadian Medical Association (CMA) Privacy Code.' Approved by the Board of Directors, 15 August. Available at: http://www.cma.ca (Publications/Services).

CNN. 1998. 'Computer Crime Soars: Survey Reports Internet Break-ins, Security Breaches, Thefts Are On The Rise.' 4 March. Available at: http://www.cnnfn.com/digitaljam/wires/9803/04/survey_wg/.

CNTFUA. 1997. 'The Call for a National Task Force on Universal Access.' Available at: http://www.fis.utoronto.ca/research/iprp/ua/tfcall.htm.

Cohen, Eliot A. 1996. 'A Revolution in Military Warfare.' *Foreign Affairs* 75, 2 (March/April): 37–54.

Conley, M., and D. Livermore. 1996. 'Human Rights, Development and Democracy: The Linkage Between Theory and Practice.' *Canadian Journal of Development Studies,* Special Issue: 19–36.

Cooley, Dennis, and Scott De Vito. 1998. 'The Millennium Problem and the Marketplace of Ideas: Insights and Freedom, Responsibility, and Technological Development.' *Public Affairs Quarterly* 12, 3 (July): 244–86.

Courchene, Thomas J., ed. 1995. *Technology, Information and Public Policy.* Kingston, Ontario: Queen's University, John Deutsch Institute for the Study of Economic Policy.

CPI. 1994. Coalition for Public Information. *Towards a Public Policy on Universal Access and Participation for the Information Infrastructure.* Ottawa: CPI. Available from the author at: sskrzesz@julian.uwo.ca.

CRTC. 1979. Canadian Radio-television and Telecommunications Commission. 'CNCP Telecommunications: Interconnection With Bell Canada.' Telecom Decision CRTC 79-11, 17 May.

- 1992. Canadian Radio-television and Telecommunications Commission. 'Competition in the Provision of Public Long Distance Voice Telephone Services and Related Resale and Sharing Issues.' Telecom Decision CRTC 92-12, 12 June.
- 1994. Canadian Radio-television and Telecommunications Commission. 'Review of Regulatory Framework.' Telecom Decision CRTC 94-19, 16 September.
- 1995. Canadian Radio-television and Telecommunications Commission / Conseil de la radio diffusion et des téléommunications canadiennes. *Competition and Culture on Canada's Information Highway: Managing the Realities of Transition / Concurrence et culture sur l'autoroute canadienne de l'information.* Ottawa: Public Works and Government Services Canada, BC 92-53/1995, 19 May.

CSA. 1996. Canadian Standards Association. *Model Code for the Protection of Personal Information.* Etobicoke, Ont: Canadian Standards Association. Available at: http://www.efc.ca/pages/doc/csa-privacy-code.jun96.html.

CSE. 1998. Communications Security Establishment / Centre de la sécurité des télécommunications. *Government of Canada Public Key Infrastructure.* Available at: http://www.cse-cst.gc.ca/cse/english/Manuals/mg15a.html.

Council of Europe. 1981. *Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data.* Strasbourg: Council of Europe.

Culnan, Mary J., and Robert J. Bies. 1999. 'Managing Privacy Concerns Strategically: The Implications of Fair Information Practices for Marketing in the Twenty-First Century.' In *Visions of Privacy: Policy Choices for a Digital Age*, ed. Colin J. Bennett and Rebecca Grant. Toronto: University of Toronto Press.

Curtis, Terry. 1988. 'The Information Society: A Computer-Generated Caste System?' In *The Political Economy of Information*, ed. Vincent Mosco and Janet Wasko. Madison: University of Wisconsin Press.

Danielian, N.R. 1974 [1939]. *AT&T: The Story of Industrial Conquest.* New York: Arno Press.

Davenport, Paul. 1997. 'The Productivity Paradox and the Management of Information Technology.' Paper presented at Conference on Service Sector Productivity and the Productivity Paradox. Sponsored by the Centre for the Study of Living Standards, Chateau Laurier Hotel, Ottawa, 11–12 April. Unpublished manuscript.

David, Paul. 1990. 'The Dynamo and The Computer: An Historical Perspective On The Modern Productivity Paradox.' *American Economic Review* 80, 2:355–361.

Davies, Simon. 1992. *Big Brother: Australia's Growing Web of Surveillance.* East Roseville, N.S.W.: Simon and Schuster Australia.

– 1999. 'Spanners in the Works: How the Privacy Movement is Adapting to the Challenge of Big Brother.' In *Visions of Privacy: Policy Choices for a Digital Age*, ed. Colin J. Bennett and Rebecca Grant. Toronto: University of Toronto Press.

Davis, Frederick. 1959. 'What Do We Mean by "Right to Privacy"?' *South Dakota Law Review* 4 (Spring), 1–24.

Davis, Jim, and Michael Stack. 1997. 'Knowledge in Production.' In *Reinventing Technology, Rediscovering Community: Critical Explorations of Computing as a Social Practice*, ed. Philip E. Agre and Douglas Schuler. Greenwich, Conn. and London, England: Ablex Publishing.

Denning, Dorothy E. 1998. 'Encryption Policy: Global Challenges and Directions.' In *The Information Revolution and International Security*, ed. Ryan Henry and C. Edward Peartree. Washington, D.C.: Center for Strategic & International Studies.

Denning, Peter, ed. 1990. *Computers under Attack: Intruders, Worms, and Viruses*. New York: Addison-Wesley.

Der Derian, James. 1996. 'Speed Pollution.' An Interview with Paul Virilio. *Wired Magazine*, May. Available at: http://www.wired.com/collections/future_of_war/4.05_paul_vir ilio_pr.html

– 1998. 'Speed Bumps for the Information Revolution.' In *The Information Revolution and International Security*, ed. Ryan Henry and C. Edward Peartree. Washington, D.C.: Center for Strategic & International Studies.

Derlega, Valerian J., Sandra Metts, Sandra Petronio, and Stephen T. Margulis. 1993. *Self-Disclosure*. Newbury Park, Calif.: Sage.

Diffie, Whitfield, and Susan Landau. 1998. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge, Mass.: MIT Press.

Dillon, John. 1996. 'Are the Feds Sniffing Your Re-mail?' *CovertAction Quarterly*, 57 (Summer), 30–1. Available at: http://caq.com/CAQ57Sniff.html.

DOD. 1996a. Department of Defense. 'Department of Defense Directive 3600.1.' *Information Operations*. Washington, D.C.: DOD (9 December):1–1.

– 1996b. Joint Chiefs of Staff and Office of the Secretary of Defense. *Final Report of the Advanced Battlespace Information System (ABIS) Task Force*. Vols 1–6. Washington, D.C.: DOD (May).

Donnelly, Jack. 1985. *The Concept of Human Rights*. London: Croom Helm.

Donnelly, Jack, and Rhoda Howard. 1989. *Universal Human Rights in Theory and Practice*. Ithaca, N.Y.: Cornell University Press.

Douglass, James. 1983. *Lightning East to West: Jesus, Gandhi and the Nuclear Age*. New York: Crossroad.

Drake, William J., ed. 1995. *The New Information Infrastructure: Strategies for U.S. Policy*. New York: Twentieth Century Press.

Drucker, Peter. 1988. 'The Coming of the New Organization.' *Harvard Business Review* 66 (January/February), 45–53.

– 1994. 'The Age of Social Transformation.' *Atlantic Monthly* 274 (November), 53–80.

Dykeman, Winston. 1999. Senate Verbal Report: 'A Declaration of Concern from the College of Family Physicians of Canada.' Presented to The Senate Standing Committee on Social Affairs, Science and Technology – Re. Personal Information Protection and Electronic Documents Act, Bill C-6. 29 November. Issue No. 2.

– 2000. 'Protecting Privacy, Confidentiality, and Security of Personal Health Information in Canadian Healthcare: Studies in Public Policy.' Unpublished manuscript. Available from the author at: dykemar@nbnet.nb.ca.

EC. 1998. European Commission. Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. *Proposal for a European Parliament and Council Directive on a Common Framework for Electronic Signatures.* COM (1998) 297 final. 13 May. Available at: http://europa.eu.int/comm/dg15/en/media/infso/com297en.pdf.

– 2000. 'Commission Decision of pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce.' Available at: http://www.ita.doc.gov/td/ecom/DecisionSECGEN-EN.htm.

Edwards, Paul N. 1996. *The Closed World: Computers and the Politics of Discourse in Cold War America.* Cambridge, Mass. MIT Press.

Ehrlich, Leonard H. 1988. 'Tolerance and the Prospect of a World Philosophy.' In *Karl Jaspers Today: Philosophy at the Threshold of the Future*, ed. Leonard H. Ehrlich and Richard Wisser. Washington, DC: Center for Advanced Research in Phenomenology & University Press of America.

EKOS. 1993. *Privacy Revealed: The Canadian Privacy Survey.* Ottawa: EKOS Research Associates Inc.

– 1996. *Rethinking Government.* Ottawa: EKOS Research Associates, Inc.

– 1998. 'Information Highway and the Canadian Communication Household.' Draft Wave 1 Report, January. Ottawa: EKOS Research Associates, Inc.

Ellul, Jacques. 1980. 'The Power of Technique and the Ethics of Non-Power.' In *The Myths of Information: Technology and Post Industrial Culture*, ed. Kathleen Woodward. Madison, Wis.: Coda Press.

EP. 1999. European Parliament. Scientific and Technological Options Assessment (STOA). Working Documents for the STOA Panel. *Development of Surveillance Technology and Risk of Abuse of Economic Information.* Luxembourg: EP.

- Vol.1/5, *1) Presentation of the Four Studies 2) Analysis: Data Protection and Human Rights in the European Union and the Role of the European Parliament.* December. Luxembourg: EP.
- Vol. 2/5, *Interception Capabilities 2000.* October. Luxembourg: EP.
- Vol. 3/5, *Encryption and Cryptosystems in Electronic Surveillance: A Survey of the Technology Assessment Issues.* November. Luxembourg: EP.
- Vol. 4/5, *The Legality of the Interception of Electronic Communications: A Concise Survey of the Principal Legal Issues and Instruments under International, European and National Law.* October. Luxembourg: EP.
- Vol. 5/5, *The Perception of Economic Risks Arising from the Potential Vulnerability of Electronic Commercial Media to Interception.* October. Luxembourg: EP.

Ess, Charles, ed. 1996. *Philosophical Perspectives on Computer-Mediated Communication.* Albany: State University of New York Press.

EU. 1995. 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.' Available at: http://www2.echo.lu/legal/en/dataprot/directiv/directiv.html .

- 1997. European Union. 'Ministerial Declaration on Global Information Networks.' July. Available at: http://www2.echo.lu/bonn/final.html.

Ferguson, Mary, ed. 1994. *Canadian Federal Government Handbook. A Guide to Dealing with the Federal Government.* Toronto, Ont.: Globe Information Services.

Ferré, Frederick. 1988. *Philosophy of Technology.* Englewood Cliffs, N.J.: Prentice-Hall.

Fetherstonaugh, R.C. 1944. *Charles Fleetford Sise, 1938–1918.* Montreal: Gazette Publishing.

Flaherty, David H. 1989. *Protecting Privacy in Surveillance Societies.* Chapel Hill, N.C.: University of North Carolina Press.

- 1991. 'On the Utility of Constitutional Rights to Privacy and Data Protection.' *Case Western Reserve Law Review,* 41, 33: 831–55.
- 1999. 'Visions of Privacy: Past, Present, and Future.' In *Visions of Privacy: Policy Choices for a Digital Age,* ed. Colin J. Bennett and Rebecca Grant. Toronto: University of Toronto Press.

Foot, Richard. 1998. 'Computer Criminals Wave of the Future.' *Ottawa Citizen* 13 May, A12.

Foran, Brian. 1996a. *Privacy Framework For Smart Card Applications.* Ottawa: Privacy Commissioner. July. Available at: http://infoweb.magi.com/~privcan/pubs/smcard.html.

- 1996b. 'Information Warfare: Attacks on Personal Information.' Address to 91st Annual Canadian Association of Chiefs of Police Conference, Panel on

'Censorship and Privacy Issues for Law Enforcement,' Ottawa. Available: http: //infoweb.magi.com/~privcan/pubs/cacp91.html.

Forrester, Viviane. 1996. *L'horreur économique*. Paris: Fayard.

Frank, Robert H., and Philip J. Cook. 1996. *The Winner-Take-All Society: Why the Few at the Top Get So Much More Than the Rest of Us*. New York: Penguin Books.

Franklin, Ursula. 1994. *The Real World of Technology*. Concord, Ont.: Anansi.

Forsythe, David P. 1991. *The Internationalization of Human Rights*. Lexington, Mass.: Lexington Books.

Freedman, Warren. 1987. *The Right of Privacy in the Computer Age*. New York: Quorum Books.

Fried, Charles. 1984. 'Privacy [a moral analysis].' In *Philosophical Dimensions of Privacy: An Anthology*, ed. Ferdinand D. Schoeman. Cambridge: Cambridge University Press.

Friedman, Milton. 1968. 'The Role of Monetary Policy.' *American Economic Review* 58 (March): 1–17.

Fukuyama, Francis. 1995. *Trust*. New York: Free Press.

– 1999. 'The Great Disruption: Human Nature and the Reconstitution of Social Order.' *Atlantic Monthly* 283, 5 (May): 55–80.

GAO. 1996. U.S. Government Accounting Office. Report to Congressional Requesters. *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*. Chapter Report, GAO/AIMD-96-84, 05/22/96.

Gavison, Ruth. 1984. 'Privacy and the Limits of Law.' In *Philosophical Dimensions of Privacy*, ed. Ferdinand D. Schoeman. Cambridge: Cambridge University Press. Originally published in *Yale Law Journal* 89 (1980): 421–71.

Geertz, Clifford. 1973. *Interpretation of Culture*. New York: Basic Books.

Gellman, Robert. 1999. 'Personal, Legislative, and Technical Privacy Choices: The Case of Health Privacy Reform in the United States.' In *Visions of Privacy: Policy Choices for a Digital Age*, ed. Colin J. Bennett and Rebecca Grant. Toronto: University of Toronto Press.

Georgia Tech Research Corporation. 1999. Sixth WWW user Survey. (URL: http:// www.cc.gatech.edu/gvu/user_surveys).

Gera, Surendra, Wulong Gu, and Frank C. Lee. 1998. *Information Technology and Labour Productivity Growth: An Empirical Analysis for Canada and the United States*. Industry Canada Working Paper No. 20. Ottawa: Industry Canada, March.

German, P.M., Sgt. 1995. 'Information Technologies and Transborder Criminal Activities.' In Department of Foreign Affairs and International Trade, *Information Technologies and International Relations: Proceedings of a Symposium Held in Ottawa, January 13*. Policy Staff Paper No. 95/06. Ottawa: DFAIT.

Gewirth, Alan. 1978. *Reason and Morality.* Chicago: University of Chicago Press.
- 1981. 'Are There Any Absolute Rights?' *Philosophical Quarterly* 31:1–16.
- 1982. *Human Rights: Essays on Justification and Applications.* Chicago: University of Chicago Press.
- 1983. 'The Rationality of Reasonableness.' *Synthese* 57:225–247.
- 1984. 'The Epistemology of Human Rights.' *Social Philosophy and Policy* 2:1–24.
- 1985. 'Rights and Virtues.' *Review of Metaphysics* 38, 4:739–62.
- 1986. 'Reason and Nuclear Deterrence.' *Canadian Journal of Philosophy.* Supplementary Volume, 12:129–59.
- 1988. 'Human Rights and Conceptions of the Self.' *Philosophia: Philosophical Quarterly of Israel* 18, 2/3:129–49.
- 1992. 'Human Dignity as the Basis of Human Rights.' In *The Constitution of Rights: Human Dignity and American Values,* ed. Michael J. Meyer and William A. Parent. Ithaca, N.Y., and London: Cornell University Press.
- 1996. *The Community of Rights.* Chicago and London: University of Chicago Press.
- 1998. *Self-Fulfillment.* Princeton, N.J.: Princeton University Press.

Giddens, Anthony. 1991. *Modernity and Self-Identity: Self and Society in the Late Modern Age.* Stanford, Calif.: Stanford University Press.

GILC. Global Internet Liberty Campaign. 1996. *Resolution in Support of the Freedom to Use Cryptography.* September. Available at: http://www.gilc.org/crypto/oecd-resolution.html.
- 1998a. Crypto Survey. *Cryptography and Liberty: An International Survey of Encryption Policy.* February.. Available at: http://www.gilc.org/crypto/crypto-survey.html.
- 1998b. 'Statement on Canadian Crypto Policy.' 20 April. Available at: http://www.gilc.org.

Gilder, George. 1994. *Life After Television.* Rev. ed. New York: W.W. Norton.

Globerman, Steven. 1996. 'The Information Highway and the Economy.' In *The Implications of Knoweldge-Based Growth for Micro-Economic Policies/La croissance fondée sur le savoir et son incidence sur les politiques microéconomiques,* ed. Peter Howitt. Calgary, AL.: University of Calgary Press.

Goldman, Janlori. 1999. 'Privacy and Individual Empowerment in the Interactive Age.' In *Visions of Privacy: Policy Choices for a Digital Age,* ed. Colin J. Bennett and Rebecca Grant. Toronto: University of Toronto Press.

Goodspeed, Peter. 2000. 'New Space Invaders: In the Sky.' *National Post,* 19 February. Available at:http://www.nationalpost.com/news.

Gorz, André. 1985. *Paths to Paradise: On the Liberation from Work.* Boston: South End Press.

Gostin, Larry. 1991. 'Genetic Discrimination: The Use of Genetically Based

Diagnostic and Prognostic Tests by Employers and Insurers.' *American Journal of Law and Medicine* 17, 1&2:109–44.
– 1995. 'Genetic Privacy.' *Journal of Law, Medicine and Ethics* 23:320–30.
Grace, John. 1991. 'The Ethics of Information Management.' *Canadian Public Administration*, 34, 1: 95–100.
Graf, W.D. 1996. 'Democratization "for" the Third World: Critique of a Hegemonic Project.'*Canadian Journal of Development Studies*. Special Issue: 37–56.
Graham, Garth. 1995. 'A Domain Where Thought Is Free to Roam: The Social Purpose of Community Networks.' Prepared for Telecommunications Canada, 29 March. Available from author at: aa127@freenet.carleton.ca.
Gray, Chris Hables. 1997. *Postmodern War: The New Politics of Conflict*. New York and London: Guilford Press.
Grechko, Marshall A.A. 1977. 'Science and the Art of Victory.' In *Selected Soviet Military Writings, 1970–1975*. Colorado Springs, Colo.: United States Air Force.
Grindlay, Thomas. 1975. *A History of the Independent Telephone Industry in Ontario*. Toronto: Ontario Telephone Services Commission.
Gutstein, Donald. 1999. *E.con: How the Internet Undermines Democracy*. Toronto: Stoddart.
Habiger, General Eugene B. 1997. 'Deterrence in a New Security Environment.' National Defense University Institute for National Strategic Studies. *Strategic Forum* 109. Available at: www.ndu.edu/ndu/inss/strforum/forum109.html.
Hager, Nicky. 1996–97. 'Exposing the Global Surveillance System.' *Covert Action Quarterly* 59 (Winter), 11–17. Available at: http://caq.com/CAQ59GlobalSnoop.html.
– 1996. *Secret Power: New Zealand's Role in the International Spy Network*. Nelson, New Zealand: Craig Potton.
Haraway, Donna J. 1991. *Simians, Cyborgs, and Women: The Reinvention of Nature*. New York: Routledge.
– 1997. *Modest_Witness@Second_Millennium.FemaleMan©_Meets_Onco Mouse™: Feminism and Technoscience*. New York: Routledge.
Hardin, Russell, et al. 1985. *Nuclear Deterrence: Ethics and Strategy*. Chicago: University of Chicago Press.
Harknett, Richard J. 1996. 'Information Warfare and Deterrence.' Available at: http://carlisle-www.army....ers/96autumn/harknett.html. Also in *Parameters* (Autumn): 93–107.
Harris, Louis, and Associates. 1996. *Equifax Survey on Consumer Privacy*. Atlanta, Ga.: Equifax Inc.
Harris, N. 1986. *The End of the Third World*. London: Penguin Books.

Hart, H.L.A. 1955. 'Are There Any Natural Rights?' *Philosophical Review* 64: 178–81.

Harvey, Frank P. 1997. *The Future's Back: Nuclear Rivalry, Deterrence Theory, and Crisis Stability after the Cold War.* Montreal and Kingston: McGill-Queen's University Press.

Harvey, Philip. 1989. *Securing the Right to Employment.* Princeton, N.J.: Princeton University Press.

Hayes, Richard E., and Gary Wheatley. 1996. 'Information Warfare and Deterrence.' National Defense University, *Strategic Forum,* Institute for National Strategic Studies Report, No. 87. Available at: www.ndu.edu/ndu/inss/strforum/forum87.html.

Henry, Ryan and Peartree, C. Edward. 1998. 'Military Theory and Information Warfare.' In *The Information Revolution and International Security,* Ryan Henry and C. Edward Peartree, eds. 105–127. Washington, D.C.: Center for Strategic & International Studies.

– eds. 1998b. *The Information Revolution and International Security.* Washington, D.C.: Center for Strategic & International Studies.

Henwood, Doug. 1996. 'Work and Its Future.' *Left Business Observer* 72 (April). Available at: http://www.panix.com/~dhenwood/Work.html.

– 1998. 'Unemployment.' *Left Business Observer* (24 May). Available at: http://www.panix.com/~dhenwood/Stats_unempl.html

Herskovits, Melville J. 1964. *Cultural Dynamics.* New York: Knopf.

Hixson, Richard F. 1987. *Privacy in a Public Society: Human Rights in Conflict.* New York: Oxford University Press

Hobbes, Thomas. 1982 [1651]. *Leviathan,* ed. C.B. MacPherson. New York: Penguin Books.

Hoffman, Bruce. 1997. 'Responding to Terrorism across the Technological Spectrum.' In *In Athena's Camp: Preparing for Conflict in the Information Age,* ed. John Arquilla and David Ronfeldt. Santa Monica, Calif.: RAND.

Hohfeld, Wesley. 1966 [1919]. *Fundamental Legal Conceptions as Applied in Juridical Reasoning,* ed. Walter Wheeler Cook. New Haven, Conn.: Yale University Press.

Honeywood, A. 1997. 'Snapshots of Smart Card Applications.' *Intergovernmental Solutions Newsletter,* Smart Card Edition, Issue 1. Available at: http://policyworks.gov/org/main/mg/intergov/oisnews.htm.

Howard, Rhoda E. 1983. The Full-Belly Thesis: Should Economic Rights Take Priority over Civil and Political Rights? Evidence from Sub-Saharan Aftica.' *Human Rights Quarterly* 5:467–90.

– 1989. 'Human Rights, Development and Foreign Policy.' In *Human Rights and Development: International Views,* ed. D.P. Forsythe, London: Macmillan.

Howitt, Peter, ed. 1996. *The Implications of Knoweldge-Based Growth for Micro-Economic Policies / La croissance fondée sur le savoir et son incidence sur les politiques microéconomiques*. Alberta: University of Calgary Press.

Hundley, Richard O., and Robert H. Anderson. 1997. 'Emerging Challenge: Security and Safety in Cyberspace.' In *In Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt. Santa Monica, Calif.: RAND. Also published in *IEEE Technology and Society* (Winter 1995/96): 19–28.

Huws, Ursula. 1999. 'Teleworking & Telematics.' *Women'space* 4, 1:10–13.

IC Industry Canada. Many of Industry Canada's policy documents are available on line at http://strategis.ic.gc.ca.

- 1994a. *The Canadian Information Highway: Building Canada's Information and Communications Infrastructure / L'autoroute canadienne de l'information: Une nouvelle infrastructure de l'information et des communications au Canada*. Ottawa: Minister of Supply and Services Canada.
- 1994b. *Privacy and the Canadian Information Highway / La protection de la vie privée et l'autoroute canadienne de l'information*. Ottawa: Minister of Supply and Services Canada.
- 1994c. *Providing New Dimensions for Learning, Creativity and Entrepreneurship: Progress Report of the Information Highway Advisory Council / Source de nouvelles dimensions pour l'apprentissage, la créativité et l'esprit d'entreprise: Rapport d'étape du Comité consultatif sur l'autoroute de l'information*. Ottawa: Minister of Supply and Services Canada.
- 1995a. *Access, Affordability and Universal Service on the Canadian Information Highway / Acces, cout abordable et service universel sur l'autoroute canadienne de l'information*. Ottawa: Minister of Supply and Services Canada.
- 1995b. *Connection, Community, Content. The Challenge of the Information Highway. Final Report of the Information Highway Advisory Council / Contact, communauté contenu. Le défi de l'autoroute de l'information: Rapport final du Comité consultatif sur l'autoroute de l'information*. Ottawa: Minister of Supply and Services Canada.
- 1997a. *The Impact of the Information Highway on the Workplace: A Paper to Further the Discussion of Issues Related to the Introduction of Information Technology and its Effects on Canadians at Work / Les incidences de l'autoroute de l'information sur le milieu de travail: document visant à alimenter le débat sur les questions relatives à la mise en application de la technologie de l'information et à ses effets sur la main-d'oeuvre canadienne*. February/février. Ottawa: Industry Canada.
- 1997b. *Preparing Canada for a Digital World: Final Report of the Information Highway Advisory Council / Préparer le Canada au monde numérique: Rapport*

final du Comité consultatif sur l'autoroute de l'information. Ottawa: Industry Canada.
- 1998a. *A Cryptography Policy Framework for Electronic Commerce: Building Canada's Information Economy and Society / Politique cadre en matière de cryptographie aux fins du commerce électronique: Pour une économie et une société de l'information au Canada*. Ottawa: Industry Canada.
- 1998b. *The Protection of Personal Information: Building Canada's Information Economy and Society / La protection des renseignments personnels: Pour une économie et une société de l'information au Canada*. Ottawa: Industry Canada.

Ihde, Don. 1993. *Philosophy of Technology: An Introduction*. New York: Paragon Press.

Ikenberry, G. John. 1996. 'The Myth of Post-Cold War Chaos.' *Foreign Affairs* 75, 3:79–91.

ILO. 1984. International Labour Organization. Recommendation 169. 'Recommendation Concerning Employment Policy, XVIII–XXXV.' Adopted 26 June 1984. 70th Session. *Record of the Proceedings*. Geneva: ILO.
- 1991. 77th Session, 1990. *Record of Proceedings*. Geneva: ILO.
- 1996. 'World Employment Report: Global Unemployment Crisis Continues, Wage Inequalities Rising.' *World of Work* 18 (April). Available at: http://www.ilo.org/public/english/bureau/inf/magazine/18/global.htm.
- 1997. 'Will the Information Age Mean a Virtual Revolution in Employment? ILO Symposium on Multimedia Convergence. *World of Work* 19 (March). Available at: http://www.ilo.org/public/english/bureau/inf/magazine/19/multi.htm.
- 1998. *Consideration of a Possible Declaration of Principles of the International Labour Organization concerning Fundamental Fights and Its Appropriate Follow-up Mechanism*. 86th Session. Geneva: International Labour Office.

Inness, Julie C. 1992. *Privacy, Intimacy and Isolation*. New York: Oxford University Press.

Innis, Harold A. 1923. *A History of the Canadian Pacific Railway*. Toronto: University of Toronto Press.
- 1950. *Empire and Communications*. Oxford: Oxford University Press.

Islam, N., and D.R. Morrison 1996. 'Introduction: Governance, Democracy and Human Rights / Gouvernance, démocratie et droits de la personne,' *Canadian Journal of Development Studies*, Special Issue: 5–18.

ITAC. 1989. Information Technology Association of Canada. *The Enabling Effect: An ITAC Report on Using Information Technology for Strategic Advantage*, Sept. Available at: http://www.e-commerce.com/ITAC/frame.htm

IWCF. 1996. *Information Warfare and the Canadian Forces*. Prepared by Lt. Comdr. R. Garigue SITS/ADM(DIS) and Mr T. Romet DGInt/J2 Scientific and Tech-

nical. Document No. 1350-004-D001, Ver: 1. Contract No. W2213-4-4723/04-QE, Requisition No. 846495RAB93. National Defence Headquarters. Ottawa: Public Works and Government Services Canada.

Iyer, Raghavan, ed. 1991. *The Essential Writings of Mahatma Ghandi, 1869–1948.* Delhi: Oxford University Press.

Jaspers, Karl 1951 [1933]. *Man in the Modern Age*, trans. E. and C. Paul. 2d ed. Garden City, NY: Doubleday. London: Routledge & Kegan Paul.

– 1953. *The Origin and Goal of History*, trans. Michael Bullock. New Haven, Conn.: Yale University Press.

– 1958. *Die Atombombe und die Zukunft des Menschen: Politisches Bewusstsein unserer Zeit.* 4th ed. Munich: R. Piper.

– 1961. *The Atom Bomb and the Future of Man*, trans. E.B. Ashton. Chicago: University of Chicago Press.

– 1970. *Philosophy.* Vol. II: *Existential Elucidation*, trans. E.B. Ashton. Chicago: University of Chicago Press.

Jenkins, Clive, and Barrie Sherman. 1979. *The Collapse of Work.* London: Eyre Methuen.

Johnston, David, Deborah Johnston, and Sunny Handa. 1995. *Getting Canada Online: Understanding the Information Highway.* Toronto: Stoddart.

Johnston, Russell, and Michael Vitale. 1988. 'Creating Competitive Advantage with Interorganizational Information Systems.' *MIS Quarterly* (June): 153–65.

Jones, Capers. 1999. 'The Global Economic Impact of the Year 2000 Software Problem.' Burlington, Mass.: Software Productivity Research.

Jones, David. 1996. 'Critique of CAIP's Proposed Code of Conduct for Internet Service Providers.' Available at: http://insight.mcmaster.ca/org/efc/pages/isp/caip-code-critique-14nov96.html.

Kahin, Brian, and Ernest J. Wilson III, eds. 1997. *National Information Infrastructure Initiatives: Vision and Policy Design.* Cambridge, Mass.: MIT Press.

Kalshoven, Frits. 1991. *Constraints on the Waging of War.* 2d ed. Geneva: International Committee of the Red Cross.

Kant, Immanuel. 1971 [1795]. *Perpetual Peace: A Philosophical Sketch.* In *Kant's Political Writings*, ed. with intro. and notes Hans Reiss; trans. H.B. Nisbet. Cambridge: Cambridge University Press.

Kelly, Kathy. 1997. 'Iraq: The Massacre That Never Ended.' *Press for Conversion* 31 (December): 8–9.

Kenny, Martin. 1986. *Biotechnology: The University-Industrial Complex.* New Haven, Conn.: Yale University Press.

Kern, Stephen. 1983. *The Culture of Time and Space, 1880–1918.* Cambridge, Mass.: Harvard University Press.

Kipnis, David. 1990. *Technology and Power.* Berlin: Springer-Verlag.

Klapp, Orrin E. 1978. *Opening and Closing: Strategies of Information Adaptation in Society.* Cambridge: Cambridge University Press.

Klare, Michael T. 1991. 'Behind Desert Storm: The New Military Paradigm.' *Technology Review* (May-June): 28–36.

– 1995. 'The New "Rogue States" Doctrine.' *The Nation* 16, 1 (May): 625–8.

Kling, Rob. 1997. 'Reading "All About" Computerization: How Genre Conventions Shape Nonfiction Social Analysis.' In *Reinventing Technology, Rediscovering Community: Critical Explorations of Computing as a Social Practice,* ed. Philipe E. Agre and Douglas Schuler. Greenwich, Conn., and London, England: Ablex.

Koontz, Sidney H. 1965. *Productive Labour and Effective Demand.* London: Routledge & Kegan Paul.

Kranzberg, Melvin. 1985. 'The Information Age: Evolution or Revolution?' In *Information Technologies and Social Transformation,* ed. Bruce R. Guile. Washington, D.C.: National Academy of Engineering.

– ed. 1980. *Ethics in an Age of Pervasive Technology.* Boulder, Colo.: Westview Press.

Krepinevich, Andrew. 1992. *The Military Technical Revolution: A Preliminary Assessment.* Washington, D.C.: Office of the Secretary of Defense, Office of Net Assessment.

– 1994. 'Calvary to Computer: The Pattern of Military Revolutions.' *The National Interest* 37 (Fall): 37–43.

Kroker, Arthur. 1984. *Technology and the Canadian Mind: Innis/McLuhan/Grant.* Montreal: New World Perspectives.

Kuehl, Dan. 1999. 'The Ethics of Information Warfare and Statecraft.' NDU/School of Information Warfare & Strategy. Available at: http://www.infowar.com.

Lafleur, Brenda, and Peter Lok. 1997. *Jobs in the Knowledge-Based Economy: Information Technology and the Impact on Employment.* Ottawa: Conference Board of Canada.

Lamarche, Lucie. 1995. *Perspectives du droit international des droits économiques de la personne.* Brussels: Bruylant.

Lanvin, Bruno. 1995. 'Why the Global Village Cannot Afford Information Slums.' In *The New Information Infrastructure: Strategies for U.S. Policy,* ed. Drake, William J. New York: Twentieth Century Press.

Laperrière, René. 1999. 'The "Quebec Model" of Data Protection: A Compromise between *Laissez-faire* and Public Control in a Technological Era.' In *Visions of Privacy: Policy Choices for a Digital Age,* ed. Colin J. Bennett and Rebecca Grant. Toronto: University of Toronto Press.

Lawson, Philippa. 1999. 'Bill C-54: A Primer on Its Privacy Provisions' and 'Q&A's, Bill C-54: Protection of Personal Information Act.' Ottawa: Public Interest Advocacy Centre.

Lebacqz, Karen. 1994. 'Genetic Privacy: No Deal for the Poor.' *Dialog* 33 (Winter): 39–48.

Lemos, Robert. 1999. 'Privacy Group Sues NSA over Spy Net.' 4 Dec. Electronic post available at: http:// news.excite.com/news/zd

Levinas, Emmanuel. 1969. *Totality and Infinity: An Essay on Exteriority,* trans. Alphonso Lingis. Pittsburgh, Pa. Duquesne University Press.

Levy, Steven. 1984. *Hackers: Heroes of the Computer Revolution.* New York: Dell.

Libicki, Martin C. 1995. 'What is Information Warfare?' National Defense University. Institute for National Strategic Studies. *Strategic Forum* 28. Available at: http://www.ndu.edu/ndu/inss/strforum/forum28.html.

– 1996. 'Information & Nuclear RMA's Compared.' National Defense University. Institute for National Strategic Studies. *Strategic Forum* 82. Available at: http://www.ndu.edu.

– 1998. 'Halfway to the System of Systems.' In *The Information Revolution and International Security* ed. Ryan Henry and C. Edward Peartree, Washington, D.C.: Center for Strategic & International Studies.

Lifton, Robert Jay. 1986. *The Nazi Doctors: Medical Killing and the Psychology of Genocide.* New York: Basic Books.

Linowes, David F. 1989. *Privacy in America: Is Your Private Life in the Public Eye?* Champaign, Ill.: University of Illinois Press.

Lockard, Joseph. 1997. 'Progressive Politics, Electronic Individualism and the Myth of Virtual Community.' In *Internet Culture,* ed. David Porter. New York and London: Routledge.

Locke, John. 1965 [1690]. *Two Treatises of Government,* ed. Peter Laslett. Rev. ed. New York and Scarborough, Ont.: Mentor.

Lucky, Robert. 1989. *Silicon Dreams: Information, Man and Machine.* New York: St Martin's Press.

Lyon, David, and Elia Zureik, eds. 1996. *Computers, Surveillance, and Privacy.* Minneapolis: University of Minnesota Press.

Machlup, Fritz. 1980. *Knowledge: Its Creation, Distribution and Economic Significance.* Vol. 1: *Knowledge and Knowledge Production.* Princeton, N.J.: Princeton University Press.

MacIntyre, Alasdair. 1984. *After Virtue: A Study in Moral Theory.* 2d ed. Notre Dame, Ind.: University of Notre Dame Press.

MacLean, Douglas, ed. 1984. *The Security Gamble : Deterrence Dilemmas in the Nuclear Age.* Totowa, N.J: Rowman & Allanheld.

MacNeill, Heather. 1991. 'Defining the Limits of Freedom of Inquiry: The

Ethics of Disclosing Personal Information Held in Government Archives.' *Archivaria* 32 (Summer): 138–51.

MacNulty, Christine A.R. 1996. 'Changing Social Values and Their Implications for the Ethics of Information Warfare.' Available at: http://www.infowar.com/class_1/class1_b.html-ssi.

Malik, Om. 1998. 'Computer Security: The Next Big Thing? Available at: http://www.forbes.com/asp/redir.asp?/tool/html/98/may/0520/side1.htm.

Manishin, Glenn B. 1998. 'Domain Names and Internet Governance.' *Computer Professionals for Social Responsibility Newsletter* 16, 2 (Spring): 1, 7–9.

Mann, Edward, Col. USAF. 1994. 'Desert Storm: The First Information War?' *Air Power Journal* 8, 4: 4–14. Available at: http://www.airpower.maxwell.af.mil/airchronicles/apj/apj94/w in94.html.

Mansell, R. and U. Wehn, eds. 1998. *Knowledge Societies: Information Technology for Sustainable Development*. Oxford and New York: Oxford University Press.

Margherio, Lynn, David Henry, Sandra Cook, and Sabrina Montes. 1998. *The Emerging Digital Economy*. Washington, D.C.: United States Department of Commerce, April.

Maritain, Jacques. 1951. *The Rights of Man and Natural Law*, trans. D. Anson. New York: Charles Scribner's Sons.

Marx, Gary T. 1999. 'Ethics for the New Surveillance.' In *Visions of Privacy: Policy Choices for a Digital Age*, ed. Colin J. Bennett and Rebecca Grant. Toronto: University of Toronto Press

Marx, Karl. 1978 [1859]. 'Preface to *A Contribution to the Critique of Political Economy*.' In *The Marx-Engels Reader*, ed. Robert C. Tucker. 2d ed. New York: W.W. Norton.

Maslow, Abraham H. 1954. *Motivation and Personality*. New York: Harper and Brothers.

Mason, Richard O., Florence M. Mason, and Mary J. Culnan. 1995. *Ethics of Information Management*. Thousand Oaks, Calif.: Sage.

McCarthy, Gerry. 1996. 'The End of Work.' *Literary Review of Canada* (May): 16–18.

McCarthy, Shawn. 2000. 'Ottawa Pulls Plug on Big Brother Database.' *Globe and Mail*, 30 May, A1.

McChesney, Robert W. 1999. *Rich Media, Poor Democracy: Communication Politics in Dubious Times*. Urbana and Chicago: University of Illinois Press.

McLuhan, Marshall. 1994 [1964]. *Understanding Media: The Extensions of Man*. Boston: MIT Press.

McMurty, John. 1998. *Unequal Freedoms: The Global Market as an Ethical System*. Toronto: Garamond Press.

Mendes, Errol P. 1997a. 'Human Rights and the New Information Technologies: The Law and Justice of Proportionality and Consensual Alliances.' *Human Rights Research and Education Bulletin* 34 (December): 1–9.

– 1997b. 'The Five Generations of Corporate Codes of Conduct and Their Impact on Corporate Social Responsibility.' *Human Rights Research and Education Bulletin* 33 (July): 1–7.

Menzies, Heather. 1996. *Whose Brave New World? The Information Highway and the New Economy.* Toronto: Between the Lines.

Metzl, Jamie F. 1996. 'Information Technology and Human Rights.' *Human Rights Quarterly* 18, 4: 705–46.

– 1997. 'Metzl Response to Ball, Girouard, and Chapman.' *Human Rights Quarterly* 19, 4: 860–3.

Meyer, William H. 1998. *Human Rights and International Political Economy in Third World Nations: Multinational Corporations, Foreign Aid, and Repression.* Westport, Conn., and London: Praeger.

Mill, John Stuart. 1915. *Principles of Political Economy,* ed. W.J. Ashley. London: Longmans, Green.

– 1969 [1861]. *Utilitarianism.* In *Collected Works,* vol. 10. Toronto: University of Toronto Press.

– 1972 [1859]. *On Liberty in J.S. Mill: Utilitarianism, On Liberty and Considerations on Representative Government,* ed. H.B. Acton. London: J.M. Dent.

Miller, Judith, and Laurie Mylroie. 1990. 'Human Rights in Iraq.' In *Saddam Hussein and the Crisis in the Gulf.* New York: Random House.

Mitcham, Carl. 1994. *Thinking through Technology: The Path between Engineering and Philosophy.* Chicago: University of Chicago Press.

Mitcham, Carl, and Robert Mackey, eds. 1983 [1972]. *Philosophy & Technology: Readings in the Philosophical Problems of Technology.* New York: Free Press.

Molander, Roger C., Andrew S. Riddile, and Peter A. Wilson. 1996. *Strategic Information Warfare: A New Face of War.* Santa Monica, Calif.: RAND, MR-661-OSD. Available at: http://www.rand.org/publications/MR/MR661/MR661.html.

Molander, Roger, Peter Wilson, David Mussington, and Richard Mesic. 1998. *Strategic Information Warfare Rising.* Prepared for the Office of the Secretary of Defense. Santa Monica, Calif.: RAND, MR-964-OSD.

Moll, Marita. 1997. 'Canadian Classrooms on the Information Highway: Making the Connections.' In *Tech High, Globalization and the Future of Canadian Education: A Collection of Critical Perspectives on Social, Cultural and Political Diemmas.* Ottawa: Canadian Centre for Policy Alternatives; Halifax, N.S.: Fernwood.

Moll, Marita, and Leslie Regan Shade, eds. 2001. *E-commerce vs. e-commons:*

Communications in the Public Interest. Ottawa: Canadian Centre for Policy Alternatives.

Monkhouse, Duncan. 1997. 'Smart Card Technology Threats.' *IT Security / Sécurité des IT* 43 (February): 16–17. Available at: http://www.rcmp-grc.gc.ca/html/bull43-e.htm.

Morth, Todd A. 1998. 'Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter.' *Case Western Reserve Journal of International Law* 30, 2–3 (Spring/Summer): 567–600.

Morton, Bruce. 1996. 'Canadian Federal Government Policy and Canada's Electronic Information Industry.' *Government Information Quarterly* 12, 3 (Winter/hiver): 251–95. Available at: Http://www.usask.ca/library/gic/.

Mosco, Vincent. 1989. *The Pay-Per Society: Computers and Communication in the Information Age. Essays in Critical Theory and Public Policy*. Toronto: Garamond Press.

– 1995. *The Political Economy of Communication: Rethinking and Renewal*. London: Sage.

Mosco, Vincent, and Janet Wasko, eds. 1988. *The Political Economy of Information*. Madison: University of Wisconsin Press.

Mulgan, G. J. 1991. *Communication and Control: Networks and the New Economies of Communication*. New York: Guilford Press.

Mulinen, Frederic de. 1987. *Handbook on the Law of War for Armed Forces*. Geneva: International Committee of the Red Cross.

Murphy, Robert F. 1984. 'Social Distance and the Veil.' In *Philosophical Dimensions of Privacy: An Anthology*, ed. Ferdinand D. Schoeman. Cambridge: Cambridge University Press.

Murray, Philip. 1998. 'Mounties Target "The Big Players."' *Ottawa Citizen*, 26 June, A4.

Mussington, David A., Peter A. Wilson, and Roger C. Molander. 1998. *Exploring Money Laundering Vulnerabilities through Emerging Cyberspace Technologies: A Caribbean-Based Exercise*. Prepared for the Office of Science and Technology Policy and the Financial Crimes Enforcement Network. Santa Monica, Calif.: RAND.

Mytelka, Lynn Krieger. 1995. 'Information Technologies and the Restructuring of Production.' In Department of Foreign Affairs and International Trade, *Information Technologies and International Relations: Proceedings of a Symposium Held in Ottawa, January 13, 1995*. Policy Staff Paper No. 95/06. Ottawa: DFAIT.

National Defence / Défense Nationale. 1997. *The Many Faces of Ethics in Defence / Les multiples faces éthiques de la de défense*: Proceedings of the Conference on Ethics in Canadian Defence, Ottawa, 24–25 October 1996. Sponsored

by the Defence Ethics Program, Chief Review Services, National Defence Headquarters. Ottawa: Minister of Public Works and Government Services.

Naumetz, Tim. 1999. 'PM Must Reverse Child-Porn Ruling, Backbenchers Say.' *Ottawa Citizen*, 26 January, A1, A6.

NEPSSG. 1998. National Electronic Public Space Steering Group. 'Proposed Model for Consultation and Comment on Public Space Community Networks.' Available at: http://www.fis.utoronto.ca/research/iprp/ua/eps.html.

Neutel, C. Ineke. 1997. 'Privacy Issues in Research Using Record Linkage.' *Pharmacoepidemiology and Drug Safety* 6:367–9.

Nichiporuk, Brian, and Carl H. Builder. 1997. 'Societal Implications.' In *In Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt. Santa Monica, Calif.: RAND.

Nichols, M.E. 1948. *(CP): The Story of the Canadian Press*. Toronto: Ryerson Press.

Nickel, James W. 1978/9. 'Is There a Human Right to Employment?' *Philosophical Forum* 10 (Winter-Summer): 149–70.

– 1987. *Making Sense of Human Rights: Philosophical Reflections on the Universal Declaration of Human Rights*. Berkeley and Los Angeles: University of California Press.

Nielsen, Kai. 1985. 'Commentary: Doing the Morally Unthinkable.' In *Nuclear War: Philosophical Perspectives*, ed. Michael A. Fox and Leo Groarke. New York, Berne, Frankfurt am Main: Peter Lang.

Nilsen, Kirsti. 1997. 'The Canadian Information Policy Bibliography.' Working Paper No. 7. Faculty of Information Studies, University of Toronto, September. Available at: http://www.fis.utoronto.ca/research/iprp/dipcii/workpap7.htm .

Nietzsche, Friedrich. 1967 [1887]. *On the Geneology of Morals*, trans. Walter Kaufmann and R.J. Hollingdale. New York: Vintage.

Noble, David F. 1995. *Progress without People: New Technology, Unemployment, and the Message of Resistance*. Toronto: Between the Lines.

– 1996. 'Selling the Schools a Bill of Goods: The Marketing of Computer-Based Education.' *AfterImage* (March/April): 13–19.

– 1998. 'Digital Diploma Mills, Part I: The Automation of Higher Education.' *First Monday: Peer-Reviewed Journal on the Internet* 3, 1 (5 January). Available at: http://www.firstmonday.dk/issues/issue3_1/index.html

Nossal, Kim Richard. 1995. 'Rationality and Non-Rationality in Canadian Defence Policy.' In *Canada's International Security Policy*, ed. David B. Dewitt and David Leyton-Brown. Scarborough, Ont.: Prentice-Hall.

Nozick, Robert. 1974. *Anarchy, State and Utopia*. New York: Basic Books.

Nye, Joseph S., Jr, and William A. Owens. 1996. 'America's Information Age.' *Foreign Affairs* 75, 2 (March): 20–36.

O'Berry, Carl G. 1998. 'Information Technology: Convergence and Connective Potential.' In *The Information Revolution and International Security*, ed. Ryan Henry and C. Edward Peartree. Washington, D.C.: Center for Strategic & International Studies.

OECD. 1980. Organization for Economic Cooperation and Development. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Available at: http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM.

– 1996. *Technology, Productivity and Job Creation*. Paris: OECD.

– 1997a. *Cryptography Policy: The Guidelines and the Issues: The OECD Cryptography Policy Guidelines and the Report on Background and Issues of Cryptography Policy*, March. Available at: http://www.oecd.org/dsti/sti/it/secur/index.htm.

– 1997b. *Employment Outlook*. July. Available at: http://www.oecd.org/els/publicatio/labour/eoblurb.htm

– 1998. Ministerial Conference. 'A Borderless World: Realizing The Potential of Global Electronic Commerce.' Ottawa, Canada, 7–9 October.

Offe, Claus. 1995. 'Full Employment: Asking the Wrong Question?' *Dissent* (Winter): 77–81.

Ohmae, K. 1985. *Triad Power: The Coming Shape of Global Competition*. New York: Free Press.

OMSGCS. 1995a. Ontario Ministry of the Solicitor General and Correctional Services / Ministère du Soliciteur général et des Services correctionnels. *Facts About Electronic Monitoring*. Toronto: Operational Support and Coordination Branch Correctional Services Division.

– 1995b. *Electronic Monitoring Program: Interim Policy and Procedures*. Toronto: Operational Support and Coordination Branch Correctional Services Division.

Osberg, Lars, and Andrew Sharpe. 1998. 'An Index of Economic Well-Being for Canada.' Paper presented at the CSLS Conference on the State of Living Standards and Quality of Life in Canada, 30–31 October 1998, Chateau Laurier Hotel, Ottawa.

Osberg, Lars, Fred Wien, and Jan Grude. 1995. *Vanishing Jobs: Canada's Changing Workplaces*. Toronto: James Lorimer.

Owens, Admiral William A. 1996. 'The Emerging U.S. System-of-Systems.' *Strategic Forum* 63 (February). National Defense University, Institute for National Strategic Studies. Available at: http://www.ndu.edu/ndu/inss/strforum/forum63.html.

Owens, Richard. 1999. 'Bill [C-54] Would Wreak Havoc on Business.' *National Post*, 13 May, C1.

Paine, Thomas. 1969 [1791/2] *Rights of Man*, ed. Henry Collins. Baltimore, Md.: Penguin Books.

Pannikar, Raimundo. 1982. 'Is the Notion of Human Rights a Western Concept?' *Diogenes* 120 (Winter): 75–102.

Paust, Jordan J., and Albert P. Blaustein. 1974. 'The Arab Oil Weapon – a Threat to International Peace.' *American Journal of International Law* 68:410–17.

'Pay Gap Becoming Grand Canyonesque.' 1999. *International Operating Engineer* 142, 5 (October-November): 8.

PCC. 1989. Privacy Commissioner of Canada /Commissaire à la protection de la vie privée du Canada. *AIDS and the Privacy Act / Le SIDA et la loi sur la protection des renseignements personnels*. Ottawa: Privacy Commissioner of Canada.

– 1991. *The Privacy Act / La loi sur la protection des renseignements*. Ottawa: Privacy Commissioner of Canada.

– 1992. *Genetic Testing and Privacy / Le dépistage génétique et la vie privée*. Ottawa: Privacy Commissioner of Canada.

1997. 'A Day in the Life ... Or How to Help Build Your Super File.' Extract from the 1995–96 *Annual Report* of the Privacy Commissioner. Available at: http://magi.com/~privcan/pubs/dayen.html.

PCCIP. 1997. President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures*. October. Available: http://www.info-sec.com/pccip/web/index.html.

Phillips, Bruce. 1999. 'Remarks to the Senate Standing Committee on Social Affairs, Science & Technology: Bill C-6.' 1 December. Ottawa: Privacy Commissioner of Canada. Available at: http://www.privcom.gc.ca.htm.

– 1999–2000. *Annual Report*. Available at: http://www.privcom.gc.ca/english/02_04_08_e.htm.

PIAC. 1995. Public Interest Advocacy Centre. *Surveying Boundaries: Canadians and their Personal Information*. Ottawa: Public Interest Advocacy Centre (PIAC) and the Fédération nationale des associations de consommateurs du Québec (FNACQ).

Piamonte, Ed. 1997. 'Cookies.' *IT Security / Sécurité des IT* 43 (February): 9–15. Available at:http://www.rcmp-grc.gc.ca/html/bull43-e.htm.

Pine, Evelyn, and Jeff Johnson. 'Cyber-Responsibilities.' *Computer Professionals for Social Responsibility Newsletter* 16, 3 (Summer): 1.

Poirier, Roger. 1997/8. *'A Wireless World.' Canadian Technology* (Fall/Winter): 11.

Pokempner, Dinah. 1997. 'Briefing Paper: Encryption in the Service of Human Rights.' Deputy General Counsel, Human Rights Watch, 1 August. Available at: http://www.aaas.org/SPP/DSPP/CSTC/briefings/crypto/dinah.htm .

Pollis, Adamantia, and Peter Schwab. 1979. 'Human Rights: A Western Construct with Limited Applicability.' In *Human Rights: Cultural and Ideological Perspectives*, ed. Adamantia Pollis and Peter Schwab. New York: Praeger.

Porteous, Holly. 1997. 'Analysts Advise Caution on Pentagon's Use of Info Warfare.' *Inside the Pentagon* 13, 40 (2 October): 20.

Porteous, Samuel D. 1998. *Organized Crime Impact Study.* Ottawa: Public Works and Government Services of Canada.

Porter, David, ed., 1997. *Internet Culture.* New York and London: Routledge.

Potter, Ralph B. 1969. *War and Moral Discourse.* Richmond, Va.: John Knox Press.

Powell, Johanna. 1997. 'Flight to Tax Havens.' *Financial Post, Tax Planning: A Special Report*, 22 November, 48.

PRC. 1998. Privacy Rights Clearinghouse. 'Fact Sheet #8: How Private Is My Medical Information?' May. Available at: http://www.privacyrights.org.

Privacy Act. Available at: http://canada.justice.gc.ca/stable/EN/Laws/Chap/P/P-21.html and http://canada.justice.gc.ca/FTP/FR/Lois/Chap/P/P-21.html.

Prosser, William L. 1984. 'Privacy [a legal analysis].' In *Philosophical Dimensions of Privacy*, ed. Ferdinand D. Schoeman. Cambridge: Cambridge University Press.

Protocol I. 1977. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June. In *Human Rights: A Compilation of International Instruments*, vol. 1, 2d. pt. New York and Geneva: United Nations, 1994.

Protocol II. 1977. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June. In *Human Rights: A Compilation of International Instruments*, vol. 1, 2d pt. New York and Geneva: United Nations, 1994.

Puder, Gil. 1998. 'A Pointless Civil War.' *Ottawa Citizen*, 26 June, A15.

Quebec. Loi sur la protection des renseignements personnels dans le secteur privé / Act Respecting the Protection of Personal Information in the Private Sector. Available at: http://canada.justice.gc.ca.

Quittner, Joshua. 1997. 'The Death of Privacy.' *Time*, 25 August, 53–9.

Raab, Charles D. 1999. 'From Balancing to Steering: New Directions for Data Protection.' In *Visions of Privacy: Policy Choices for a Digital Age*, ed. Colin J. Bennett and Rebecca Grant. Toronto: University of Toronto Press.

Raboy, Marc. 1997. 'Cultural Sovereignty, Public Participation, and Democratization of the Public Sphere: The Canadian Debate on the New Information Infrastructure.' In *National Information Infrastructure Initiatives: Vision and*

Policy Design, ed. Brian Kahin and Ernest J. Wilson, III. Cambridge, Mass.: MIT Press.

Rapoport, Anatol. 1986. 'The Technological Imperative.' In *Man-Environment Systems* 16:2–3.

Rawls, John. 1971. *A Theory of Justice.* Cambridge, Mass.: Harvard University Press.

– 1993. 'The Law of Peoples.' In *On Human Rights: The Oxford Amnesty Lectures 1993*, ed. Stephen Shute and Susan Hurley. NewYork: Basic Books.

Regan, Priscilla M. 1993. 'The Globalization of Privacy: Implications of Recent Changes in Europe.' *American Journal of Economics and Society* 257: 264–5.

– 1995. *Legislating Privacy: Technology, Social Values, and Public Policy.* Chapel Hill, N.C.: University of North Carolina Press.

– 1999. 'American Business and the European Data Protection Directive: Lobbying Strategies and Tactics.' In *Visions of Privacy: Policy Choices for a Digital Age*, ed. Colin J. Bennett and Rebecca Grant. Toronto: University of Toronto Press.

Regis, Edward, Jr, ed. 1984. *Gewirth's Ethical Rationalism: Critical Essays with a Reply by Alan Gewirth.* Chicago: University of Chicago Press.

Reid, Angus. 1996. *Workplace 2000: Under Construction. Survey of Canadian Employees.* Toronto: Royal Bank of Canada.

Reidenberg, Joel R. 1999. 'The Globalization of Privacy Solutions: The Movement towards Obligatory Standards for Fair Information Practices.' In *Visions of Privacy: Policy Choices for a Digital Age*, ed. Colin J. Bennett and Rebecca Grant. Toronto: University of Toronto Press.

Rheingold, Howard. 1993. *The Virtual Community: Homesteading on the Electronic Frontier.* Reading, Mass.: Addison-Wesley.

Rifkin, Jeremy. 1995. *The End of Work: The Decline of the Global Labor Force and the Dawn of the Post-Market Era.* New York: G.P. Putnam's Sons.

Rivière, Phillipe. 1999. 'All Europe Is Listening.' *Le Monde diplomatique.* March.

Robertson, A.H., ed. 1973. *Privacy and Human Rights: Reports and Communications Presented at the Third International Colloquy about the European Convention on Human Rights, Organised by the Belgian Universities and the Council of Europe, with the Support of the Belgian Government, Brussels, 30 September – 3 October 1970.* Manchester, England: University of Manchester Press.

Rogerson, Simon. 1998. 'The Social Impact of Smart Card Technology.' Unpublished paper presented at the Round Table on 'Human Rights and New Technologies,' Twentieth World Congress of Philosophy: PAIDEIA. Philosophy Educating Humanity / XXe Congrès Mondial de Philosophie: La philosophie dans l'éducation de l'humanité, Boston, Mass., 10–16 August.

Rorty, Richard. 1993. 'Human Rights, Rationality, and Sentimentality.' In *On*

Human Rights: The Oxford Amnesty Lectures 1993, ed. Stephen Shute and Susan Hurley. New York: Basic Books.

Rosenau, James N. 1998. 'Global Affairs in an Epochal Transformation.' In *The Information Revolution and International Security*, ed. Ryan Henry and C. Edward Peartree. Washington, D.C.: Center for Strategic & International Studies.

Rosenblueth, Arturo, Norbert Wiener, and Julian Bigelow. 1943. 'Behavior, Purpose and Teleology.' *Philosophy of Science* 10:18–24.

Rothrock, John. 1997. 'Information Warfare: Time for Some Constructive Skepticism?' In *In Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt. Santa Monica, Calif.: RAND. First published in *American Intelligence Journal* (Spring/Summer 1994): 71–6.

Rule, James, and Lawrence Hunter. 1999. 'Toward Property Rights in Personal Data.' In *Visions of Privacy: Policy Choices for a Digital Age*, ed. Colin J. Bennett and Rebecca Grant. Toronto: University of Toronto Press.

Rutherford, Paul. 1982. *A Victorian Authority: The Daily Press in Late Nineteenth-Century Canada*. Toronto: University of Toronto Press.

Salamun, Kurt, 1991. 'Die liberal-aufklärerische Dimension in Jaspers' Denken – ein Beispiel moderner Aufklärung.' In *Karl Jaspers: Zur Aktualität seines Denkens*, ed. Kurt Salamun. Munich: R. Piper.

SCEPSP. 1997. Steering Committee for the Electronic Public Space Project. 'Community/Communications: A Model for Electronic Public Space.' Available at: http://www.fis.utoronto.ca/research/iprp/ua/eps.html

Schell, Jonathan. 1982. *The Fate of the Earth*. New York: Avon Books.

Schiller, Dan. 1999. *Digital Capitalism: Networking the Global Market System*. Cambridge, Mass., and London, England: MIT Press.

Schindler, Dietrich, and Jiri Toman, eds. 1973. *The Law of Armed Conflicts: A Collection of Conventions, Resolutions and Other Documents*. Leiden: A.W. Sijthoff.

Schneider, Benjamin, and David E. Bowen. 1995. *Winning the Service Game*. Boston: Harvard Business School Press.

Schoeman, Ferdinand D., ed. 1984. *Philosophical Dimensions of Privacy: An Anthology*. Cambridge: Cambridge University Press.

Schwartau, Winn. 1994. *Information Warfare: Chaos on the Electronic Superhighway*. New York: Thunders Mouth Press.

Schweizer, Peter. 1993. *Friendly Spies: How America's Allies Are Using Economic Espionage to Steal Our Secrets*. New York: Atlantic Monthly Press.

Shade, Leslie Regan. 1997. 'Access to the Internet for Women's Groups Across Canada.' In *Women, Work and Computerization: Spinning a Web from Past to Future*, ed. A.F. Grundy et al. Proceedings of the 6th International IFIP-Conference, Bonn, Germany, 24–27 May. Bonn: Springer.

– 1998a. 'A Gendered Perspective on Access to the Information Infrastructure.' *The Information Society* 14:33–44.
– 1998b. 'Developing Guidelines with the Canadian "Knowledge-Based Economy/Society."' *Proceedings of the Ethics and Social Impact Component, ACM Policy '98, Shaping Policy in the Information Age*, ed. Tom Jewett and Keith Miller. *Computers and Society*, Special Issue (June): 14–16.
Sharp, Gene. 1965. *The Political Equivalent of War: Civil Defense.* New York: Carniege Endowment for International Peace.
Sharpe, Andrew. 1998. 'Solving the Productivity Paradox: The Mysterious Link between Computers and Productivity.' Centre for the Study of Living Standards. Available at: http://www.csls.ca/finpost2.pdf.
Shaw, Andy. 1997. 'Myths and Realities of Partnerships.' *Computing Canada* 23, 23 (November): 17–18.
Shelton, Denise. 1996. 'Banks Appease Online Terrorists.' (3 June). Available at: http://news.cnet.com/news.
Shniad, Sid. 1998. 'An Excerpt from Comments Made by IBM President Louis Gerstner, Jr, at the OECD Ministerial Conference on Electronic Commerce, Ottawa, Ontario. Canada,' Universal Access Canada, 8 October.
Sidorsky, D. 1979. 'Contemporary Reinterpretations of the Concept of Human Rights.' In *Essays on Human Rights: Contemporary Issues and Jewish Perspectives*, ed. D. Sidorsky. Philadelphia, Pa.: Jewish Publication Society of America.
Siegel, Richard Lewis. 1994. *Employment and Human Rights: The International Dimension.* Philadelphia: University of Pennsylvania Press.
Sieghart, Paul. 1983. 'Information, Technology, Law and Human Rights.' *IDOC International* 1-2:20–27.
Simmel, Georg. 1978. *The Philosophy of Money.* London: Routledge.
Sivard, Ruth Leger. 1991. *World Military and Social Expenditures 1991.* 14th ed. Washington, D.C.: World Priorities.
Solow, Robert M.. 1987. 'We'd Better Watch Out.' *New York Times Book Review,* 12 July, 36.
Sopinka, John. 1994. 'Freedom of Speech and Privacy in the Information Age.' Unpublished manuscript. University of Waterloo Symposium on Free Speech and Privacy in the Information Age, 26 November.
– 1997. 'Sopinka on Cyberspace.' *Ottawa Citizen* 18 Sept. A19–20.
Sottas, E. 1990. *The Least Developed Countries: Development and Human Rights.* Geneva: OMCT/SOS-Torutre.
Spafford, Eugene. 1992. 'Are Computer Hacker Break-ins Ethical?' *Journal of Systems Software* (January): 41–7.
Spinello, Richard A. 1995. *Ethical Aspects of Information Technology.* Englewood Cliffs, N.J.: Prentice-Hall.

Stanbury, W.T., and Ilan B. Vertinsky. 1995. 'Assessing the Impact of New Information Technologies on Interest Group Behaviour and Policymaking.' In *Technology, Information and Public Policy*, ed. Thomas J. Courchene. Kingston, Ont.: John Deutsch Institute for the Study of Economic Policy, Queen's University.

Steeves, Valerie. 1995. 'Humanizing Cyberspace: Privacy, Freedom of Speech, and the Information Highway.' *Human Rights Research and Education Bulletin* 28 (June): 1–5.

– 1998. 'A Response to Professor Walters's Paper Entitled "Dignitizing Technology, Transforming Ourselves."' Presented at *Building a Human Rights Agenda for the 21st Century: A Practical Celebration of the 50th Anniversary of the Universal Declaration of Human Rights*, October 1–3.

Stentor Telecom Policy, Inc. 1993. *The Information Highway: Canada's Road to Economic and Social Recovery*. Ottawa: Stentor.

STOA. 1998. Scientific and Technical Options Assessment (European Parliament). 'An Appraisal of Technologies of Political Control.' Unpublished paper. Manchester, England: OMEGA Foundation.

Strawson, J.M. 1980. 'Future Methods and Techniques.' In *The Future of the Printed Word*, ed. Philip Hills. London: Pinter.

Surtees, Lawrence. 1992. *Pa Bell: A. Jean de Grandpré & The Meteoric Rise of Bell Canada Enterprises*. Toronto: Random House of Canada.

Swett, Charles. 1995. 'Strategic Assessment: The Internet.' Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (Policy Planning), Room 2B525, the Pentagon 703-693-5208. Available at http://www.fas.org/cp/swett.html.

Szafranski, Richard, Col. 1995. 'A Theory of Information Warfare: Preparing for 2020.' *Air Power Journal* 1 (Spring): 56–65. Available at: www.airpower.maxwell.af.mil/airchronicles/apj/spr95.html

Taylor, Alison. 1997. 'Visioning Education in the Information Economy.' In *Tech High, Globalization and the Future of Canadian Education: A Collection of Critical Perspectives on Social, Cultural and Political Diemmas*, ed. Marita Moll. Ottawa: Canadian Centre for Policy Alterantives; Halifax, N.S.: Fernwood.

Thomas, Tim. 1996. 'Russian Views on Information-Based Warfare.' Fort Leavenworth, Kans.: Foreign Military Studies Office. Available at: http://leav-www.army.mil/fmso.

Thompson, W.L. 1947. *Wiring a Continent: The History of the Telegraph in the United States, 1832–1866*. Princeton, N.J.: Princeton University Press.

Thomson, Judith Jarvis. 1984. 'The Right to Privacy.' In *Philosophical Dimensions of Privacy*, ed. Ferdinand D. Schoeman. Cambridge: Cambridge University Press.

– 1990. *The Realm of Rights*. Cambridge, Mass.: Harvard University Press.
Toffler, Alvin, and Heidi Toffler. 1993. *War and Anti-war: Survival at the Dawn of the Twenty-first Century*. Boston: Little, Brown.
Troyer, W.L. 1980. *The Sound and the Fury: An Anecdotal History of Canadian Broadcasting*. Toronto: Personal.
Trudel, Pierre, France Abran, Karim Benyekhleff, Sophie Hein, et al. 1997. *Droit du cyberespace*. Montreal: Éditions Thémis.
Tuck, Richard. 1979. *Natural Rights Theories: Their Origin and Development*. Cambridge: Cambridge University Press.
Turkle, Sherry. 1984. *The Second Self: Computers and the Human Spirit*. London, Toronto, Sydney, New York: Granada.
– 1996. 'Who Am We?' *Wired* 4, 1 (Jan.) http://www.wired.com/wired/archive/4.01/turkle.html.
Ullman, Ellen. 1997. *Close to the Machine: Technophilia and Its Discontents*. San Francisco: City Lights Books.
UNCESCR. 1998. United Nations. Committee on Economic, Social and Cultural Rights. 'Concluding Observations of the Committee on Economic, Social and Cultural Rights: Canada. 04/12/98. E/C12/1/Add.31.
UNDP. 1997. United Nations Development Program. Human Development Report 1997: Overview. Available: http://www.undp.org/undp/hdro/overview.htm.
– 1998. 'Achievements in Poverty Eradication.' Available at: http://www.undp.org/toppages/poverty/povframe.htm
USAF. 1974. United States Air Force. *Scientific-Technical Progress and the Revolution in Military Affairs (A Soviet View)*. Colorado Springs, Colo.: U.S. Air Force.
– 1977. *Selected Soviet Military Writings 1970–1975: A Soviet View*. Colorado Springs, Colo.: U.S. Air Force.
USAP. 1994. U.S. Army Pamphlet 5255. *Force XXI Operations*. Fort Monroe, Va.: U.S. Army Training and Doctrine Command, 1 August.
USCC. 1983. United States Catholic Conference. *The Challenge of Peace: God's Promise and Our Response*. Washington, D.C.: USCC.
USOTA. 1991. U.S. Congress, Office of Technology Assessment, *Medical Monitoring and Screening in the Workplace: Results of a Survey – Background Paper*. OTA-BP-BA-67. Washington, D.C.: U.S. Government Printing Office, October.
U.S. National Information Infrastructure Task Force. 1997. 'Options for Promoting Privacy on the National Information Infrastructure' (April). Available at: http://www.iitf.nist.gov/ipc/privacy.htm.
Van Creveld, Martin. 1989. *Technology and War: From 2000 B.C. to the Present*. New York: Free Press.
Van Parijs, Phillippe. 1991. 'Why Surfers Should Be Fed: The Liberal Case for

an Unconditional Base Income.' *Philosophy and Public Affairs* 20 (Spring): 101–31.

Varian, Hal R. 1995. 'The Information Economy.' *Scientific American* 273, 3 (Sept.): 200–2.

Vlahos, Michael. 1998. 'Entering the Infosphere.' *Journal of International Affairs* 51, 2 (Spring): 497–525.

Vuono, Carl E. 1991. 'Desert Storm and the Future of Conventional Forces.' *Foreign Affairs* 70 (Spring):58–64.

Wajcman, Judy, ed. 1991. *Feminism Confronts Technology.* University Park: Pennsylvania State University Press.

Waldron, Jeremy. 1993. *Liberal Rights.* Cambridge: Cambridge University Press.

Waldrop, M. Mitchell. 1998. 'Is There an Information Revolution? In *The Information Revolution and International Security,* ed. Ryan Henry and C. Edward Peartree. Washington, D.C.: Center for Strategic & International Studies.

Waller, Douglas. 1995. 'Onward Cyber Soldier.' *Time,* 21 August, 30–6.

Walters, Gregory J. 1988. *Karl Jaspers and the Role of "Conversion" in the Nuclear Age.* Lanham, Md.: University Press of America.

– 1990. 'Nuclear Deterrence, Strategic Defense and Caesar's Coin: Looking Back, Looking Ahead.' *Église et Théologie* 21:329–48.

– 1995a. *Human Rights in Theory and Practice: A Selected and Annotated Bibliography.* Metuchen, N.J., London, Pasadena, Calif., Englewood Cliffs, N.J.: Salem Press.

– 1995b. 'Just-War Casuistry, the Gulf War, and the Conditions of Human Coexistence.' In *Violence and Human Coexistence,* ed. Venant Cauchy, 195–205. Montréal: Éditions Montmorency.

– 1997a. 'Canadian Information Highway Policy, the Right of Access to Information, and the Conditions of Human Action.' *Science et esprit* 49, 2:193–229.

– 1997b. 'Human Rights, World Philosophy, and the Quest for Global Solidarity: Karl Jaspers's Abiding Contribution.' *Jahrbuch der Österreichischen Karl Jaspers Gesellschaft / Yearbook of the Austrian Karl Jaspers Society,* Studien Verlag Innsbruck-Wien, Herausgegeben von Elisabeth Salamun-Hybašek und Kurt Salamun Jahrgang / Annual 10:127–50.

– 1998a. 'Information Technology, Human Rights and Community / Technologie de l'information, des droits de la personne et de la communauté.' *Human Rights Research and Eduction Centre Bulletin / Droits de la personne Bulletin d'information sur la recherche et l'enseignement* 36 (Nov.): 1–11.

– 1998b. 'A New Way of War in the Information Age.' Argument & Observation Section, *Ottawa Citizen,* 14 March, B7.

– 1999a. 'Information Technology, Work and Human Development: A Human Rights Perspective.' *Canadian Journal of Development Studies* 20, 2:225–54.

– 1999b. 'Is a Global Human Rights Community Possible? On *Confucianism and Human Rights*, edited by Wm. Theodore de Bary and Tu Weiming.' *International Philosophical Quarterly* 39, 2 (June): 209–15.
– 2001. 'MacIntyre or Gewirth? Virtue, Rights and the Problem of Moral Indeterminacy.' In *Philosophical Approaches to Human Rights*, ed. Will Sweet. Amsterdam and Atlanta: Rodolpi Press.
– ed. 1996. *The Tasks of Truth: Essays on Karl Jaspers's Idea of the University.* Frankfurt am Main: Peter Lang.
Walzer, Michael. 1977. *Just and Unjust Wars*. New York: Basic Books.
Warren, Samuel, and Louis Brandeis. 1890. 'The Right to Privacy.' *Harvard Law Review* 4:193–220. Reprinted as 'The Right to Privacy [The implicit made Explicit].' In *Philosophical Dimensions of Privacy: An Anthology*, ed. Ferdinand D. Schoeman. Cambridge: Cambridge University Press, 1984.
Wayner, Peter. 1998a. 'Cypercash's Less in Web Survival.' *New York Times*, 10 August, D1.
– 1998b. 'Code Breaker Cracks Smart Cards' Digital Safe.' *New York Times*, 22 June, C1.
Web Review. 1996. 'What Smells? Is the NSA [National Security Agency] Sniffing Your E-mail?' Available at: http://webreview.com/96/01/12/features/nsa.sniff.html.
Wehling, Jason. 1995. 'Netwars and Activists: Power on the Internet.' March. Available at: http://www.teleport.com/~jwehling/Netwars.html.
Welch, Claude E., Jr., and Ronald I. Meltzer, eds. 1984. *Human Rights and Development in Africa*. Albany: State University of New York Press.
Westin, Alan F. 1967. *Privacy and Freedom*. New York: Atheneum.
– 1984. 'The Origins of Modern Claims to Privacy.' In *Philosophical Dimensions of Privacy: An Anthology*, ed. Ferdinand D. Schoeman. Cambridge: Cambridge University Press.
– Westin, Alan F., and Michael A. Baker. 1972. *Databanks in a Free Society: Computers, Record-Keeping and Privacy*. New York: Quadrangle Books.
Wheelwright, Geoff. 1997. 'Survey Finds Telecommuting Brings Benefits.' *IT Monthly: A Special Report on Information Technology*, 15 November, IT27.
Whitaker, Randall. 1995. 'The Revolution in Military Affairs (RMA).' November. Available at: http://www/informatik.umu.se/~rwhit/RMA.html
Wiener, Norbert. 1967 [1950]. *The Human Use of Human Beings: Cybernetics and Society*. New York: Avon Books.
Wilbur, Shawn P. 1997. 'An Archaeology of Cyberspaces: Virtuality, Community, Identity.' In *Internet Culture*, ed. David Porter. New York and London: Routledge.
Williams, Phil. 1997. 'Transnational Criminal Organizations and International

Security.' In *In Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt. Santa Monica, Calif.: RAND.

Williamson, Michael. 1995. 'SchoolNet and the Community Access Project.' *Network Notes* 11. Ottawa: Information Technology Services, National Library of Canada.

Wilson, Ernest J., III. 1997. 'Introduction: The What, Why, Where, and How of National Information Initiatives.' In *National Information Infrastructure Initiatives*, ed. Brian Kahin and Ernest J. Wilson III. Cambridge, Mass.: MIT Press.

Winner, Langdon. 1997. 'Cyberlibertarian Myths and the Prospects for Community,' *Computers and Society* 27, 3 (Sept.): 14–19.

Winnecott, D.W. 1965. *The Maturational Processes and the Facilitating Environment*. London: Hogarth.

Winston, Morton E. 1989. *The Philosophy of Human Rights*. Belmont, Calif.: Wadsworth.

– 1996. 'Privacy Protection Models for the Private Sector.' Available at: http://www.ipc.on.ca/web_site.eng/matters/sum_pap/papers/mod els-e.htm

Wright, Tom. 1993. Information and Privacy Commissioner, Ontario. 'Smart Cards.' April. Available at: http://www.ipc.on.ca.

Yerxa, Shawn W., and Marita Moll. 1995. 'Commodification, Communication, and Culture: Democracy's Dead End on the Infobahn.' *Government Information in Canada / Information gouvernementale au Canada* 1, 3 (Winter/hiver).

Zahn, Gordon C., ed. 1980. *Thomas Merton on Peace*. New York: Farrar, Straus, Giroux.

This page intentionally left blank

Index