

Privacy and Human Rights 2002

An International Survey of Privacy Laws and Developments

**Electronic Privacy Information Center
Washington, DC, USA**

**Privacy International
London, United Kingdom**

Copyright © 2002 by the Electronic Privacy Information Center and
Privacy International

First edition 2002
Printed in the United States of America
All Rights Reserved

ISBN: 1-893044-16-5

About the Electronic Privacy Information Center

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC is a project of the Fund for Constitutional Government. EPIC is a member of the Transatlantic Consumer Dialog, Global Internet Liberty Campaign, the Internet Free Expression Alliance and the Internet Privacy Coalition.

The EPIC Bookstore provides a comprehensive selection of books and reports on computer security, cryptography, the First Amendment and free speech, open government, and privacy. Visit the EPIC Bookstore at www.epic.org/bookstore/.

About Privacy International

Privacy International (PI) is a human rights group formed in 1990 as a watchdog on surveillance by governments and corporations. PI is based in London, England, and has an office in Washington, D.C. PI has conducted campaigns throughout the world on issues ranging from wiretapping and national security activities, to ID cards, video surveillance, data matching, police information systems, and medical privacy.

An electronic version of this report and updates is available from the Privacy International web page at <http://www.privacyinternational.org/>.

EPIC Staff

Marc Rotenberg, Executive Director
David L. Sobel, General Counsel
Sarah Andrews, Research Director
Chris Hoofnagle, Legislative Counsel
Mikal Condon, Staff Counsel
Kate Rears, Editorial Director
Cédric Laurant, Policy Fellow
Mihir Kshirsagar, Policy Analyst
Wayne Madsen, Senior Fellow

Acknowledgments

This study was first written by David Banisar, Deputy Director of Privacy International in 1998 and has been updated on an annual basis since then. The 2002 updates were conducted by Sarah Andrews, Research Director at EPIC, and Gus Hosein, Senior Fellow at Privacy International. Substantial writing and research for this edition was provided by EPIC staff, and the law students who participated in the EPIC 2002 Internet Public Interest Opportunities Program (IPIOP): Nicole Anastasopoulos, Will DeVries, Marcia Hofmann, Dwayne Nelson, Carla Meninsky, Greg Pemberton, Sara Rose and Jason Young.

To gather information for this study and previous editions, knowledgeable individuals from academia, government, human rights groups and other fields were asked to submit reports and information. Their reports were supplemented with information gathered from Constitutions, laws, international and national government documents, news reports, human rights reports and other sources.

EPIC and Privacy International would like to thank the following people for providing invaluable reports, information and advice: Jason Abrams, EPIC; Andrzej Adamski, Nicolas Copernicus University, Poland; Yaman Akdeniz, Cyber-Rights & Cyber-Liberties; Andrej D. Bartosiewicz, Citizen's Initiative for a Good Law on Access To Information, Slovakia; Diana Alonso Blas, Registratiekamer, Netherlands; Joze Bogataj, Data Protection Inspector, Republic of Slovenia; Mads Bryde Andersen, University of Copenhagen, Denmark; Jacques Berleur, Facultes Universitaires N.D. de la Paix, Belgium; Colin Bennett, University of Victoria, Canada; Mark Berthold, Office of the Ombudsman, New Zealand; Ian Brown, University of London; Herbert Burkert,

GMD, Germany; Heiner Busch, Switzerland; Lee Bygrave, Norwegian Research Centre for Computers & Law; Rafael Fernandez Calvo, CLI, Spain; Anne Carblanc, OECD, France; Pavel Cerny, EPS, Czech Republic; David Casacuberta, Spain; Dmitry Chereskin, Russian Academy of Natural Sciences; Tyng-Ruey Chuang, Taiwan Association of Human Rights; Kira Kolby Christensen, Legal Adviser, Datatilsynet, Denmark; Dr. Richard Claude, Washington, D.C.; Tracy Cohen, Link Centre, University of the Witwatersrand, South Africa; Ulrich Dammann, Bundesbeauftragte für den Datenschutz, Germany; Ravi Dhar, India; Alexander Dix, Commissioner for Data Protection and Access to Information, Brandenburg, Germany; Ronnie Downes, Irish Data Protection Agency; Bo Elkjaer, Denmark; Jón Erlendsson, Iceland; Emilio Aced Féllez, Agencia De Protección De Datos, Spain; William G. Ferroggiard, National Security Archive, USA; Anne-Marije Fontein, College bescherming persoonsgegevens, Netherlands; Maurice Frankel, Campaign for Freedom of Information, United Kingdom; Miguel Angel Garcia, Estudios de Consumo, Spain; Marie Georges, CNIL, France; Rishab Aiyer Ghosh, India; Ann Goldsmith Office of the Privacy Commissioner, Canada; Eric Goldstein, Human Rights Watch Middle East/North Africa; Graham Greenleaf, University of New South Wales, Australia; Marina Gromova, Russia; Alex Hamilton, Liberty, United Kingdom; Pétur Hauksson, Mannvernd, Iceland; Hordur Helgi Helgason, Deputy Commissioner, Icelandic Data Protection Authority (Persónuvernd); Bénédicte Havelange, Commission de la Protection de la Vie Privée, Belgium; Helmut. Heil, Bundesbeauftragte für den Datenschutz, Germany; Jan Holvast, Holvast and Partners, Netherlands; Deborah Hurley, Harvard Information Infrastructure Project; Pavol Husar, Commissioner for the Protection of Personal Data in Information Systems, Slovak Republic; Joichi Ito, Japan; Joel Jaakkola, Finland; Ms. Ona Jakstaite, State Data Protection Inspection, Lithuania; Sigrún Jóhannesdóttir, The Icelandic Data Protection Commission; Barbara Jurgeleviciene, Senior inspector, State Data Protection Inspectorate of the Republic of Lithuania; Marina Karakonova, Access to Information Programme, Bulgaria; Alexander Kashamov, Access to Information Programme, Bulgaria; Michael Kassner, EPIC; Yeoh Beng Keat, Ministry of Energy, Communications and Multimedia, Malaysia; Maija Kleemola, Office of Data Protection Ombudsman, Finland; Igor Kowalewski, The Bureau of the Inspector General of Poland for Personal Data Protection; Natalia Krajcovicova, Head of Commissioner's Secretariat, Inspection Unit for the Protection of Personal Data, Slovak Republic; Dieter Kronegger, Arge Daten, Austria; Jorma Kuopus, Office of the Parliamentary Ombudsman, Finland; Margarita Lacabe, Derechos Human Rights; Anne-Christine Lacoste, Belgian Privacy Data Protection Commission; Steven Lau, Hong Kong Privacy Commissioner; Pippa Lawson, Public Interest Advocacy Centre, Canada; Georg Lechner, Austrian Data Protection

Commission; Anatoly Levenchuk, Russia; Vaida Linartaite, Chief Inspector, State Data Protection Inspectorate, Lithuania; László Majtényi, Hungarian Information and Privacy Commissioner; Veni Markovski, Internet Society Bulgaria; Joe Meade, Data Protection Commissioner, Ireland; Meryem.Marzouki, IRIS, France; Viktor Mayer-Schönberger, Harvard University; Robin McLeish, Hong Kong; Erich Moechel, Quintessenz, Austria; Andrea Monti, Studio Legale Monti, Italy; Dinesh Nair; Victor Naumov, St.Petersburg Institute for Informatics, Russia; Dr. Karel Neuwirt, Office for Personal Data Protection, Czech Republic; Detlef Nogala, Max-Planck-Institut, Germany; Nelly Ognyanova, Bulgarian Institute for Legal Development; Toshimaru Ogura, Professor of Toyama University, Japan; Kaidi Oone, Estonian State Chancellery, Department of State Information Systems; Maxim Otstavnov, Computerra, Russia; Pablo A. Palazzi, Argentina; Hugues Parasie, Commission de la Protection de la Vie Privée, Belgium; Stephanie Perrin, Zero Knowledge Systems, Canada; Alberto Escudero-Pascual, Royal Institute of Technology, Sweden; Andriy Pazyuk, Privacy Ukraine; Charlotte Edholm Petersen, Datatilsynet, Denmark; Signe Plumina, Director of State Data Inspection, Latvia; Erki Podra, Data Protection Inspectorate, Ukraine; Yves Poulet, Centre de Recherches Informatique et Droit, Belgium; Andrei Pribylov, Human Rights Network, Russia; Felix Rauch, President, Swiss Internet User Group; Joel Reidenberg, Fordham University Law School, USA; Katitza Rodriguez, Director, Privaterra, Peru; Dovota Rowicka, Bureau of Inspector General for the Protection of Personal Data, Poland; Felipe Rodriquez, Electronic Frontiers Australia; Roman Romanov, Sebastopol Group for Human Rights Protection, Ukraine; Anneliese Roos, University of South Africa; Dr Paul Roth, University of Otago, New Zealand; Dag Wiese Schartum, University of Oslo, Norway; Anat Scolnicov, Association for Civil Rights in Israel; Jin Wan Seo, Department of Public Administration, University of Incheon, South Korea; Per Helge Sørensen, Digital Rights, Denmark; Antonino Serra Cambaceres, Consumers International; Justyna Seweryoska, Bureau of the Inspector General for the Protection of Personal Data, Poland; Bernard Silva, Office of the Federal Privacy Commissioner, Australia; Sergei Smirnov, Human Rights Network, Russia; Robert Ellis Smith, Privacy Journal; Christoph Sobotta, University of Frankfurt, Germany; Per Helge Sørensen, Digital Rights, Denmark; Barry Steinhardt, ACLU; Blair Stewart, New Zealand Privacy Commission; Bettina Stomper, Quintessenz, Austria; Ivan Szekely, Central European University, Hungary; Jerome Thorel, France; Kosmas Tsiraktopoulos, Swiss Data Protection Commission; Marie Vallée, Videotron, Canada; Shauna Van Dongen, Privacy Journal, USA; Geetha Veloo Malaysia; Nigel Waters, Australia; Raymond Wacks, The University of Hong Kong; Elisabeth Wallin, The Data Inspection Board, Sweden; Elizabeth Jane Walsh, University College Cork, Ireland;

Maurice Wessling, Bits of Freedom, Netherlands; Ingrid Wilson; Australian Privacy Commission; Niti Wirudchawong, Official Information Commission, Thailand; Bobson Wong, Digital Freedom Network; Ko Youngkyoung, Social Information Networking Group, South Korea.

Financial assistance was provided by the Open Society Institute and the EPIC Trust.

Foreword

The events of September 11, 2001 brought new challenges to the protection of privacy in the modern era. In the rush to strengthen national security and to reduce the risk of future terrorist acts, governments around the world turned to legal authority and new technology to extend control over individuals. Many of these proposals have had far-reaching consequences for the protection of privacy.

But many of these same proposals were not new. Prior to September 11, law enforcement agencies sought expanded communications surveillance authority. Trade groups for the entertainment industry urged national governments to create new categories of computer crime that included copyright infringements. Sellers of computer database systems had pressed governments to buy more database systems. Developers of identification technologies had pushed for increased use of their own identification techniques. Pundits had called for greater transparency about private life. All of them found support in the events of September 11 to argue for greater surveillance of people who had committed no crime.

Still, September 11 has not yet signaled the end of privacy. Constitutional authority remained in place as a barrier against the proposals that most threatened democratic self-governance. Government institutions established to safeguard privacy turned their attention to the challenges posed by the response to September 11. Political leaders spoke out against the most egregious plans. Technical experts found flaws in facial recognition systems and constitutional scholars excised provisions in legislative proposals introduced in national parliaments. NGOs around the world rallied in support of campaigns to block and even repeal invasive proposals. In Great Britain, privacy advocates pushed back the expansive and unjustified Regulation of Investigatory Powers Act. Big Brother is not yet welcome in most countries.

The annual Privacy and Human Rights survey continues to document the ebb and flow of efforts to safeguard privacy in the modern era. EPIC Research Director Sarah Andrews edited the 2002 edition of Privacy and Human Rights building on the earlier work of Simon Davies and David Banisar. Gus Hosein provided his expertise for several critical sections. The students participating in the EPIC Internet Public Interest Opportunities Program (IPIOP), national data protection authorities, and more than one hundred experts, scholars, and advocates have all lent their support to this effort.

It continues to be our hope that a careful examination of how countries around the world respond to new challenges, even those as horrific as September 11, will enable the safeguarding of privacy in the years ahead.

Marc Rotenberg
Executive Director
EPIC
July 2002

Privacy and Human Rights 2002

Executive Summary

This annual report by EPIC and Privacy International reviews the state of privacy in over fifty countries around the world. It outlines legal protections for privacy, and summarizes important issues and events relating to privacy and surveillance.

A major focus of the 2002 report has been to document the effects of September 11, 2001 on privacy and civil liberties. In response to the events of that day, specific anti-terrorism measures have been introduced in Australia, Austria, Canada, Denmark, France, Germany, India, Singapore, Sweden, the United Kingdom and the United States. Another significant development was the adoption, in June 2002, of the European Union's Electronic Communications Privacy Directive. This Directive allows European Union member states to enact laws requiring Internet Service Providers, and other telecommunications operators, to retain the traffic and location data of all people using mobile phones, text messaging, land-line telephones, faxes, e-mails, chatrooms, the Internet, or any other electronic communication devices, to communicate. Such data retention schemes are already in place in Belgium, France, Spain and the United Kingdom and have been proposed in the Netherlands. In New Zealand a law granting significant new interception authority to law enforcement is also pending. Among all of these measures, it is possible to identify a number of trends including: increased communications surveillance and search and seizure powers; weakening of data protection regimes; increased data sharing; and increased profiling and identification. While none of the above trends are necessarily new; the novelty is the speed in which these policies gained acceptance, and in many cases, became law.

On the other hand, the report finds that efforts to pass new data protection laws or to strengthen existing laws are continuing in Eastern Europe, Asia and Latin America. In August 2001, Peru enacted a data protection law covering credit reporting agencies and, in March 2002, created a Commission to draft a more comprehensive law. In Bulgaria, a new Personal Data Protection Act came into effect in January 2002. In Estonia, the Government is currently working on an amendment bill to the Data Protection Act to bring it into full compliance with the 1995 European Union Data Protection Directive. Poland ratified the Convention for the Protection of Individuals with Regard to Automatic

Processing of Personal Data (ETS No. 108) in May 2002. In Slovakia, an amended data protection law has been introduced and is expected to take place in September 2002. In 2001, Slovenia amended its Data Protection Act in order to establish an independent supervisory authority. A Personal Data Protection Act is pending in Malaysia. In Japan, two new anti-spam laws were adopted in 2002. In Singapore a National Internet Advisory Committee issued a Model Data Protection Code for the Private Sector in February 2002.

In addition, laws or codes to protect privacy in the workplace are gaining more prominence. In Finland, a new law on Data Protection in Working Life entered into force in October 2001. In December 2001, the President of the Russian Federation, signed into law the new Labor Code which includes protection of personal data. The United Kingdom Privacy Commissioner has drafted a four-part code on data protection in the workplace. The first of these, relating to privacy in the recruitment and selection process was issued in March 2002. The second, on employee monitoring, was released for public comment in April 2002. In Sweden, a national committee issued a proposal in March 2002 recommending specific legislation to protect the personal information of current employees, former employees and employment applicants in both the private and public sectors. In May 2002, the European Union Article 29 Data Protection Working Party issued a working paper on monitoring and surveillance of electronic communications in the workplace. In June 2002, the Hong Kong Data Protection Commission issued a draft a code of practice on workplace for public consultation. The new European Union Electronic Communications Directive, while leaving open the possibility of data retention in the members states, has also established important safeguards for information transmitted across the Internet. It prohibits unsolicited commercial marketing by e-mail (spam) without consent, and protects mobile phone users from precise location tracking and surveillance.

During the year new Freedom of Information Laws were passed in Peru and Mexico and went into effect in Poland.

Table of Contents

TABLE OF CONTENTS	v
OVERVIEW	1
DEFINING PRIVACY	1
<i>Aspects of Privacy</i>	3
MODELS OF PRIVACY PROTECTION	3
<i>Comprehensive laws</i>	3
<i>Sectoral Laws</i>	4
<i>Self-Regulation</i>	4
<i>Technologies of Privacy</i>	4
THE RIGHT TO PRIVACY.....	5
THE EVOLUTION OF DATA PROTECTION	8
<i>Rationales for Adopting Comprehensive Laws</i>	9
<i>The European Union Data Protection Directives</i>	10
OVERSIGHT AND PRIVACY AND DATA PROTECTION COMMISSIONERS	13
TRANSBORDER DATA FLOWS AND DATA HAVENS.....	14
<i>European Union-United States “Safe Harbor” Agreement</i>	16
THREATS TO PRIVACY	20
THE RESPONSE TO SEPTEMBER 11, 2001	20
<i>Increased Communications Surveillance and Search and Seizure Powers</i>	22
<i>Weakening of Data Protection Regimes</i>	23
<i>Increased Data Sharing</i>	24
<i>Increased Profiling and Identification</i>	26
IDENTITY SYSTEMS.....	27
<i>Identity (ID) cards</i>	27
<i>Biometrics</i>	29
SURVEILLANCE OF COMMUNICATIONS.....	30
<i>Legal Protections and Human Rights</i>	31
<i>Legal and Technical Standards for Surveillance: Building in Big Brother</i>	33
<i>Internet Surveillance: Black Boxes and Key Loggers</i>	37
<i>Transactional and Location Data: Surveillance and New Communications Technologies</i>	40
<i>Retention of Traffic and Location Data</i>	43
<i>‘Cybercrime’: International Initiatives in Harmonizing Surveillance</i>	45
<i>National Security, Intelligence Agencies and the “Echelon system”</i>	50
AUDIO BUGGING	53
VIDEO SURVEILLANCE.....	53
<i>Face Recognition</i>	56
SATELLITE SURVEILLANCE.....	57
ELECTRONIC COMMERCE.....	58
<i>Spam</i>	59
<i>Profiling</i>	59
<i>Security Breaches</i>	63
<i>Information Brokers and Seal Programs</i>	63
<i>Privacy Enhancing Techniques</i>	64
<i>Electronic Numbering</i>	66

PUBLIC RECORDS AND PRIVACY, PUBLIC-PRIVATE VENTURES	66
DIGITAL RIGHTS MANAGEMENT	68
AUTHENTICATION AND IDENTITY DISCLOSURE	69
<i>Defining Identity Disclosure</i>	69
<i>Inscribing Identity into Policy</i>	71
<i>Inscribing Identity into Infrastructure</i>	72
<i>Inscribing Identity into Technology</i>	72
<i>Authentication without Identification</i>	73
SPY TV: INTERACTIVE TELEVISION & “T-COMMERCE”	74
GENETIC PRIVACY	76
<i>Genetic Identification</i>	78
<i>Genetic Testing</i>	81
<i>Right Not to Know</i>	81
<i>In the Workplace</i>	82
<i>Insurance</i>	84
<i>Legal Safeguards</i>	84
WORKPLACE PRIVACY	86
<i>Legal Background</i>	87
<i>Performance Monitoring</i>	90
<i>Telephone Monitoring</i>	91
<i>E-mail and Internet Use Monitoring</i>	92
<i>Drug Testing</i>	94
COUNTRY REPORTS.....	97
ARGENTINE REPUBLIC	97
COMMONWEALTH OF AUSTRALIA	102
<i>State and Territory Laws</i>	112
REPUBLIC OF AUSTRIA	114
KINGDOM OF BELGIUM	119
FEDERATIVE REPUBLIC OF BRAZIL.....	125
REPUBLIC OF BULGARIA	129
CANADA	133
<i>Provinces</i>	143
REPUBLIC OF CHILE	144
PEOPLE’S REPUBLIC OF CHINA	146
CZECH REPUBLIC	158
KINGDOM OF DENMARK	162
<i>Greenland</i>	166
REPUBLIC OF ESTONIA	166
REPUBLIC OF FINLAND.....	171
<i>Aland Islands</i>	175
FRENCH REPUBLIC	175
FEDERAL REPUBLIC OF GERMANY	182
HELLENIC REPUBLIC (GREECE).....	190
SPECIAL ADMINISTRATIVE REGION OF HONG KONG.....	196
REPUBLIC OF HUNGARY.....	205
REPUBLIC OF ICELAND	210
REPUBLIC OF INDIA	215
REPUBLIC OF IRELAND.....	219

STATE OF ISRAEL	225
ITALIAN REPUBLIC	230
JAPAN	234
JORDAN.....	241
REPUBLIC OF (SOUTH) KOREA	243
REPUBLIC OF LATVIA.....	252
REPUBLIC OF LITHUANIA	256
GRAND DUCHY OF LUXEMBOURG.....	261
MALAYSIA.....	264
UNITED MEXICAN STATES.....	268
KINGDOM OF THE NETHERLANDS.....	271
NEW ZEALAND.....	277
<i>Self-governing territories</i>	285
KINGDOM OF NORWAY	285
REPUBLIC OF PERU.....	290
REPUBLIC OF THE PHILIPPINES	295
REPUBLIC OF POLAND.....	303
REPUBLIC OF PORTUGAL.....	308
RUSSIAN FEDERATION	312
<i>Autonomous Russian Republics</i>	317
REPUBLIC OF SAN MARINO.....	317
REPUBLIC OF SINGAPORE.....	318
SLOVAK REPUBLIC.....	324
REPUBLIC OF SLOVENIA.....	329
REPUBLIC OF SOUTH AFRICA.....	331
KINGDOM OF SPAIN.....	338
KINGDOM OF SWEDEN	342
SWISS CONFEDERATION (SWITZERLAND)	348
REPUBLIC OF CHINA (TAIWAN)	354
KINGDOM OF THAILAND	358
REPUBLIC OF TURKEY	363
REPUBLIC OF UKRAINE	367
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND.....	375
<i>Territories</i>	381
UNITED STATES OF AMERICA	382

Overview

Privacy is a fundamental human right. It underpins human dignity and other values such as freedom of association and freedom of speech. It has become one of the most important human rights of the modern age.

Privacy is recognized around the world in diverse regions and cultures. It is protected in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and in many other international and regional human rights treaties. Nearly every country in the world includes a right of privacy in its constitution. At a minimum, these provisions include rights of inviolability of the home and secrecy of communications. Most recently written constitutions include specific rights to access and control one's personal information. In many of the countries where privacy is not explicitly recognized in the constitution, the courts have found that right in other provisions. In many countries, international agreements that recognize privacy rights such as the International Covenant on Civil and Political Rights or the European Convention on Human Rights have been adopted into law.

Defining Privacy

Of all the human rights in the international catalogue, privacy is perhaps the most difficult to define.¹ Definitions of privacy vary widely according to context and environment. In many countries, the concept has been fused with data protection, which interprets privacy in terms of management of personal information.

Outside this rather strict context, privacy protection is frequently seen as a way of drawing the line at how far society can intrude into a person's affairs.² The lack of a single definition should not imply that the issue lacks importance. As one writer observed, "in one sense, all human rights are aspects of the right to privacy."³

Some viewpoints on privacy:

¹ James Michael, *Privacy and Human Rights 1* (UNESCO 1994).

² Simon Davies, *Big Brother: Britain's Web of Surveillance and the New Technological Order 23* (Pan 1996).

³ Volio, Fernando, "Legal personality, privacy and the family" in Henkin (ed), *The International Bill of Rights* (Columbia University Press 1981).

In the 1890s, future United States Supreme Court Justice Louis Brandeis articulated a concept of privacy that urged that it was the individual's "right to be left alone." Brandeis argued that privacy was the most cherished of freedoms in a democracy, and he was concerned that it should be reflected in the Constitution.⁴

Robert Ellis Smith, editor of the *Privacy Journal*, defined privacy as "the desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves."⁵

According to Edward Bloustein, privacy is an interest of the human personality. It protects the inviolate personality, the individual's independence, dignity and integrity.⁶

According to Ruth Gavison, there are three elements in privacy: secrecy, anonymity and solitude. It is a state which can be lost, whether through the choice of the person in that state or through the action of another person.⁷

The Calcutt Committee in the United Kingdom said that, "nowhere have we found a wholly satisfactory statutory definition of privacy." But the committee was satisfied that it would be possible to define it legally and adopted this definition in its first report on privacy:

The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information.⁸

The Preamble to the Australian Privacy Charter provides that, "A free and democratic society requires respect for the autonomy of individuals, and limits on the power of both state and private organizations to intrude on that autonomy . . . Privacy is a key value which underpins human dignity and other key values such

⁴ Samuel Warren and Louis Brandeis, "The Right to Privacy," 4 *Harvard Law Review* 193–220 (1890).

⁵ Robert Ellis Smith, *Ben Franklin's Web Site* 6 (Sheridan Books 2000).

⁶ "Privacy as an Aspect of Human Dignity," 39 *New York University Law Review* 971 (1964).

⁷ "Privacy and the Limits of Law," 89 *Yale Law Journal* 421, 428 (1980).

⁸ Report of the Committee on Privacy and Related Matters, Chairman David Calcutt QC, 1990, Cmnd. 1102, London: HMSO, page 7.

as freedom of association and freedom of speech. . . . Privacy is a basic human right and the reasonable expectation of every person.”⁹

Aspects of Privacy

Privacy can be divided into the following separate but related concepts:

Information privacy, which involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. It is also known as “data protection”;

Bodily privacy, which concerns the protection of people’s physical selves against invasive procedures such as genetic tests, drug testing and cavity searches;

Privacy of communications, which covers the security and privacy of mail, telephones, e-mail and other forms of communication; and

Territorial privacy, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks.

Models of Privacy Protection

There are four major models for privacy protection. Depending on their application, these models can be complementary or contradictory. In most countries reviewed in the survey, several are used simultaneously. In the countries that protect privacy most effectively, all of the models are used together to ensure privacy protection.

Comprehensive laws

In many countries around the world, there is a general law that governs the collection, use and dissemination of personal information by both the public and

⁹“The Australian Privacy Charter,” published by the Australian Privacy Charter Group, Law School, University of New South Wales, Sydney 1994.

private sectors. An oversight body then ensures compliance. This is the preferred model for most countries adopting data protection laws and was adopted by the European Union to ensure compliance with its data protection regime. A variation of these laws, which is described as a *co-regulatory model*, was adopted in Canada and Australia. Under this approach, industry develops rules for the protection of privacy that are enforced by the industry and overseen by the privacy agency.

Sectoral Laws

Some countries, such as the United States, have avoided enacting general data protection rules in favor of specific sectoral laws governing, for example, video rental records and financial privacy. In such cases, enforcement is achieved through a range of mechanisms. A major drawback with this approach is that it requires that new legislation be introduced with each new technology so protections frequently lag behind. The lack of legal protections for individual's privacy on the Internet in the United States is a striking example of its limitations. There is also the problem of a lack of an oversight agency. In many countries, sectoral laws are used to complement comprehensive legislation by providing more detailed protections for certain categories of information, such as telecommunications, police files or consumer credit records.

Self-Regulation

Data protection can also be achieved - at least in theory - through various forms of self-regulation, in which companies and industry bodies establish codes of practice and engage in self-policing. However, in many countries, especially the United States, these efforts have been disappointing, with little evidence that the aims of the codes are regularly fulfilled. Adequacy and enforcement are the major problem with these approaches. Industry codes in many countries have tended to provide only weak protections and lack enforcement. This is currently the policy promoted by the governments of the United States and Singapore.

Technologies of Privacy

With the recent development of commercially available technology-based systems, privacy protection has also moved into the hands of individual users. Users of the Internet and of some physical applications can employ a range of programs and systems that provide varying degrees of privacy and security of

communications. These include encryption, anonymous remailers, proxy servers and digital cash.¹⁰ Users should be aware that not all tools are effective of protecting privacy. Some are poorly designed while others may be designed to facilitate law enforcement access. (For more discussion of this subject see the section on *Privacy Enhancing Techniques* at 64).

The Right to Privacy

The recognition of privacy is deeply rooted in history. There is recognition of privacy in the Qur'an¹¹ and in the sayings of Mohammed. ¹² The Bible has numerous references to privacy.¹³ Jewish law has long recognized the concept of being free from being watched.¹⁴ There were also protections in Classical Greece and ancient China.¹⁵

Legal protections have existed in Western countries for hundreds of years. In 1361, the Justices of the Peace Act in England provided for the arrest of peeping toms and eavesdroppers.¹⁶ In 1765, British Lord Camden, striking down a warrant to enter a house and seize papers wrote, “We can safely say there is no law in this country to justify the defendants in what they have done; if there was, it would destroy all the comforts of society, for papers are often the dearest property any man can have.”¹⁷ Parliamentarian William Pitt wrote, “The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow though it; the storms may enter; the rain may enter – but the King of England cannot enter; all his forces dare not cross the threshold of the ruined tenement.”¹⁸

Various countries developed specific protections for privacy in the centuries that followed. In 1776, the Swedish Parliament enacted the Access to Public Records Act that required that all government-held information be used for legitimate

¹⁰ EPIC maintains a list of privacy tools at <<http://www.epic.org/privacy/tools.htm>>.

¹¹ an-Noor 24:27-28 (Yusufali); al-Hujraat 49:11-12 (Yusufali).

¹² Volume 1, Book 10, Number 509 (Sahih Bukhari); Book 020, Number 4727 (Sahih Muslim); Book 31, Number 4003 (Sunan Abu Dawud).

¹³ Richard Hixson, *Privacy in a Public Society: Human Rights in Conflict* 3 (1987). See also, Barrington Moore, *Privacy: Studies in Social and Cultural History* (1984).

¹⁴ See Jeffrey Rosen, *The Unwanted Gaze* (Random House 2000).

¹⁵ *Id.* at 5.

¹⁶ James Michael, *supra* n.1, at 15. Justices of the Peace Act, 1361 (Eng.), 34 Edw. 3, c. 1.

¹⁷ *Entick v. Carrington*, 1558-1774 All E.R. Rep. 45.

¹⁸ Speech on the Excise Bill, 1763.

purposes. France prohibited the publication of private facts and set stiff fines for violators in 1858.¹⁹ The Norwegian criminal code prohibited the publication of information relating to “personal or domestic affairs” in 1889.²⁰

In 1890, American lawyers Samuel Warren and Louis Brandeis wrote a seminal piece on the right to privacy as a tort action, describing privacy as “the right to be left alone.”²¹ Following the publication, this concept of the privacy tort was gradually picked up across the United States as part of the common law.

The modern privacy benchmark at an international level can be found in the 1948 Universal Declaration of Human Rights, which specifically protects territorial and communications privacy.²² Article 12 states:

No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks.

Numerous international human rights treaties specifically recognize privacy as a right.²³ The International Covenant on Civil and Political Rights (ICCPR), Article 17,²⁴ the UN Convention on Migrant Workers, Article 14,²⁵ and the UN Convention on Protection of the Child, Article 16²⁶ adopt the same language.

¹⁹ The Rachel affaire. Judgment of June 16, 1858, Trib. pr. inst. de la Seine, 1858 D.P. III 62. See Jeanne M. Hauch, Protecting Private Facts in France: The Warren & Brandeis Tort is Alive and Well and Flourishing in Paris, 68 Tulane Law Review 1219 (May 1994).

²⁰ See Prof. Dr. Juris Jon Bing, Data Protection in Norway, 1996, available at <http://www.jus.uio.no/iri/rettsinfo/lib/papers/dp_norway/dp_norway.html>.

²¹ Warren and Brandeis, *supra* n.4.

²² Universal Declaration of Human Rights, adopted and proclaimed by General Assembly resolution 217 A (III) of December 10, 1948, available at <<http://www.un.org/Overview/rights.html>>.

²³ See generally, Marc Rotenberg, ed., *The Privacy Law Sourcebook: United States Law, International Law and Recent Developments* (EPIC 2001).

²⁴ International Covenant on Civil and Political Rights, adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of December 16, 1966, entry into force March 23 1976, available at <http://www.unhchr.ch/html/menu3/b/a_ccpr.htm>.

²⁵ International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, adopted by General Assembly resolution 45/158 of December 18, 1990, available at <http://www.unhchr.ch/html/menu3/b/m_mwctoc.htm>.

²⁶ Convention on the Rights of the Child, adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of November 20, 1989, entry into force September 2, 1990, available at <<http://www.unhchr.ch/html/menu3/b/k2crc.htm>>.

On the regional level, various treaties make these rights legally enforceable. Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms 1950²⁷ states:

(1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health of morals, or for the protection of the rights and freedoms of others.

The Convention created the European Commission of Human Rights and the European Court of Human Rights to oversee enforcement. Both have been active in the enforcement of privacy rights and have consistently viewed Article 8's protections expansively and interpreted the restrictions narrowly.²⁸ The Commission found in 1976:

For numerous Anglo-Saxon and French authors, the right to respect "private life" is the right to privacy, the right to live, as far as one wishes, protected from publicity . . . In the opinion of the Commission, however, the right to respect for private life does not end there. It comprises also, to a certain degree, the right to establish and develop relationships with other human beings, especially in the emotional field for the development and fulfillment of one's own personality.²⁹

The Court has reviewed member states' laws and imposed sanctions on numerous countries for failing to regulate wiretapping by governments and private individuals.³⁰ It has also reviewed cases of individuals' access to their personal information in government files to ensure that adequate procedures exist.³¹ It has expanded the protections of Article 8 beyond government actions

²⁷ Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, (ETS no: 005) open for signature November 4, 1950, entry into force September 3, 1950, available at <<http://conventions.coe.int/Treaty/EN/cadreprincipal.htm>>.

²⁸ Nadine Strossen, Recent United States and Intl. Judicial Protection of Individual Rights: A comparative Legal Process Analysis and Proposed Synthesis, 41 *Hastings Law Journal* 805 (1990).

²⁹ *X v. Iceland*, 5 *Eur. Comm'n H.R.* 86.87 (1976).

³⁰ European Court of Human Rights, *Case of Klass and Others: Judgement of 6 September 1978*, Series A No. 28 (1979). *Malone v. Commissioner of Police*, 2 *All E.R.* 620 (1979). See Note, *Secret Surveillance and the European Convention on Human Rights*, 33 *Stanford Law Review* 1113, 1122 (1981).

³¹ *Judgement of 26 March 1987 (Leander Case)*.

to those of private persons where it appears that the government should have prohibited those actions.³²

Other regional treaties are also beginning to be used to protect privacy. Article 11 of the American Convention on Human Rights sets out the right to privacy in terms similar to the Universal Declaration.³³ In 1965, the Organization of American States proclaimed the American Declaration of the Rights and Duties of Man, which called for the protection of numerous human rights, including privacy.³⁴ The Inter-American Court of Human Rights has begun to address privacy issues in its cases.

The Evolution of Data Protection

Interest in the right of privacy increased in the 1960s and 1970s with the advent of information technology. The surveillance potential of powerful computer systems prompted demands for specific rules governing the collection and handling of personal information. The genesis of modern legislation in this area can be traced to the first data protection law in the world enacted in the Land of Hesse in Germany in 1970. This was followed by national laws in Sweden (1973), the United States (1974), Germany (1977), and France (1978).³⁵

Two crucial international instruments evolved from these laws. The Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data³⁶ and the Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data³⁷ set out specific rules covering the handling of electronic data. These rules describe personal information as data that are afforded protection at every step from collection to storage and dissemination.

³² Id. at 848-49.

³³ Signed November 22, 1969, entered into force July 18, 1978, O.A.S. Treaty Series No. 36, at 1, O.A.S. Off. Rec. OEA/Ser. L/V/II.23 dec rev. 2, available at <<http://www.oas.org/juridico/english/Treaties/b-32.htm>>.

³⁴ O.A.S. Res XXX, adopted by the Ninth Conference of American States, 1948 OEA/Ser. L./V/I.4 Rev (1965).

³⁵ An excellent analysis of these laws is found in David Flaherty, *Protecting Privacy in Surveillance Societies* (University of North Carolina Press 1989).

³⁶ Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data Convention, ETS No. 108, Strasbourg, 1981, available at <<http://www.coe.fr/eng/legaltxt/108e.htm>>.

³⁷ OECD, "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data" Paris, 1981, available at <<http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM>>.

The expression of data protection in various declarations and laws varies. All require that personal information must be:

- obtained fairly and lawfully;
- used only for the original specified purpose;
- adequate, relevant and not excessive to purpose;
- accurate and up to date;
- accessible to the subject;
- kept secure; and
- destroyed after its purpose is completed.

These two agreements have had a profound effect on the enactment of laws around the world. Nearly thirty countries have signed the COE convention and several others are planning to do so shortly. The OECD guidelines have also been widely used in national legislation, even outside the OECD member countries.

Rationales for Adopting Comprehensive Laws

There are three major reasons for the movement towards comprehensive privacy and data protection laws. Many countries are adopting these laws for one or more reasons.

To remedy past injustices. Many countries, especially in Central Europe, South America and South Africa, are adopting laws to remedy privacy violations that occurred under previous authoritarian regimes.

To promote electronic commerce. Many countries, especially in Asia, have developed or are currently developing laws in an effort to promote electronic commerce. These countries recognize that consumers are uneasy with the increased availability of their personal data, particularly with new means of identification and forms of transactions. These countries recognize consumers are uneasy with their personal information being sent worldwide. Privacy laws are being introduced as part of a package of laws intended to facilitate electronic commerce by setting up uniform rules.

To ensure laws are consistent with Pan-European laws. Most countries in Central and Eastern Europe are adopting new laws based on the Council of Europe Convention and the European Union Data

Protection Directive. Many of these countries hope to join the European Union in the near future. Countries in other regions are adopting new laws or updating older laws to ensure that trade will not be affected by the requirements of the European Union Directive.

The European Union Data Protection Directives

In 1995, the European Union enacted the Data Protection Directive in order to harmonize member states' laws in providing consistent levels of protections for citizens and ensuring the free flow of personal data within the European Union. The directive sets a baseline common level of privacy that not only reinforces current data protection law, but also establishes a range of new rights. It applies to the processing of personal information in electronic and manual files.³⁸

A key concept in the European data protection model is “enforceability.” Data subjects have rights established in explicit rules. Every European Union country has a data protection commissioner or agency that enforces the rules. It is expected that the countries with which Europe does business will need to provide a similar level of oversight.

The basic principles established by the Directive are: the right to know where the data originated; the right to have inaccurate data rectified; a right of recourse in the event of unlawful processing; and the right to withhold permission to use data in some circumstances. For example, individuals have the right to opt-out free of charge from being sent direct marketing material. The Directive contains strengthened protections over the use of sensitive personal data relating, for example, to health, sex life or religious or philosophical beliefs. In the future, the commercial and government use of such information will generally require “explicit and unambiguous” consent of the data subject.

The 1995 Directive imposes an obligation on member states to ensure that the personal information relating to European citizens has the same level of protection when it is exported to, and processed in, countries outside the European Union. This requirement has resulted in growing pressure outside Europe for the passage of privacy laws. Those countries that refuse to adopt adequate privacy laws may find themselves unable to conduct certain types of

³⁸ 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://europa.eu.int/comm/internal_market/en/media/dataprot/law/index.htm>.

information flows with Europe, particularly if they involve sensitive data. (See below.)

In 1997, the European Union supplemented the 1995 directive by introducing the Telecommunications Privacy Directive.³⁹ This directive established specific protections covering telephone, digital television, mobile networks and other telecommunications systems.⁴⁰ It imposed wide-ranging obligations on carriers and service providers to ensure the privacy of users' communications, including Internet-related activities. It covered areas that, until then, had fallen between the cracks of data protection laws. Access to billing data was severely restricted, as was marketing activity. Caller ID technology was required to incorporate an option for per-line blocking of number transmission. Information collected in the delivery of a communication was required to be purged once the call is completed.

In July 2000, the European Commission issued a proposal for a new directive on privacy in the electronic communications sector.⁴¹ The proposal was introduced as a part of a larger package of telecommunications directives aimed at strengthening competition within the European electronic communications markets. As originally proposed, the new directive would have strengthened privacy rights for individuals by extending the protections that were already in place for telecommunications to a broader, more technology-neutral category of "electronic communications." During the process, however, the Council of Ministers began to push for the inclusion of data retention provisions, requiring Internet Service Providers and telecommunications operators to store logs of all telephone calls, e-mails, faxes, and Internet activity for law enforcement purposes. These proposals were strongly opposed by most members of the Parliament. In July 2001, the European Parliament's Civil Liberties Committee approved the draft directive without data retention stating:

The Civil Liberties Committee ("LIBE Committee") expressed itself in favour of a strict regulation of law enforcement authorities' access to personal data of citizens, such as communication traffic and location data. This decision is fundamental because in this way the EP blocks

³⁹ Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector (Directive), available at <<http://www.ispo.cec.be/legal/en/dataprot/protection.html>>.

⁴⁰ European Union member countries were required to enact implementing legislation by October 1998. As of the summer 2002, however, several are still pending.

⁴¹ European Commission, Proposal for a directive of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, available at <http://europa.eu.int/comm/information_society/policy/framework/pdf/com2000385_en.pdf>.

European Union States' efforts underway in the Council to put their citizens under generalised and pervasive surveillance, following the Echelon model.

Following the events of September 11, however, the political climate changed and the Parliament came under increasing pressure from member states to adopt the Council's proposal for data retention. The United Kingdom and the Netherlands, in particular, questioned whether the proposed privacy rules still struck "the right balance between privacy and the needs of the law enforcement agencies in the light of the battle against terrorism."⁴² The Parliament stood firm and up to a few weeks before the final vote on May 30, 2002, the majority of MEPs opposed any form of data retention. Finally, after much pressure by the European Council and European Union governments, and well organized lobbying by two Spanish MEPs,⁴³ the two main political parties (PPE and PSE, the center-left and center-right parties) reached a deal to vote in favor of the Council's position.

On June 25, 2002 the European Union Council adopted the new Electronic Communications Privacy Directive as voted in the Parliament.⁴⁴ Under the terms of the new Directive member states may now pass laws mandating the retention of the traffic and location data of all communications taking place over mobile phones, SMS, landline telephones, faxes, e-mails, chatrooms, the Internet, or any other electronic communication device. Such requirements can be implemented for purposes varying from national security to the prevention, investigation and prosecution of criminal offences.

In other areas, the Electronic Communications Privacy Directive had a more favorable outcome. For example, it adds new definitions and protections for "calls," "communications," "traffic data" and "location data" in order to enhance the consumer's right to privacy and control in all kinds of data processing. These new provisions ensure the protection of all information ("traffic") transmitted across the Internet, prohibit unsolicited commercial marketing by e-mail (spam) without consent, and protect mobile phone users from precise location tracking and surveillance. The directive also gives subscribers to all electronic

⁴² Jelle van Buuren, "Telecommunication Council Wants New Investigation Into Privacy Rules," Heise Online, October 17, 2001.

⁴³ Respectively, MEPs Ana Palacio Vallelersundi and Elena Paciotti, members of the PPE (European Peoples' Party/Christian Democrats) and PSE (Social Democrats) political parties.

⁴⁴ 2439th Council meeting, Luxembourg, June 25, 2002. Transcripts of proceedings available at <http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=PRES/02/180/0|AGED&lg=EN>.

communications services (such as GSM and e-mail) the right to choose whether they are listed in a public directory.

The Directive will enter into force from date of publication in the official journal. After that time member states will have fifteen months to implement its provisions.

Oversight and Privacy and Data Protection Commissioners

An essential aspect of any privacy protection regime is oversight. In most countries with an omnibus data protection or privacy act, there is an official or agency that oversees enforcement of the act. The powers of these officials - Commissioner, Ombudsman or Registrar - vary widely by country. A number of countries including Germany and Canada also have officials or offices on a state or provincial level.

Under Article 28 of the European Union Data Protection Directive, all European Union countries must have an independent enforcement body. Under the Directive, these agencies are given considerable power: governments must consult the body when the government draws up legislation relating to the processing of personal information; the bodies also have the power to conduct investigations and have a right to access information relevant to their investigations; impose remedies such as ordering the destruction of information or ban processing, and start legal proceedings, hear complaints and issue reports. The official is also generally responsible for public education and international liaison in data protection and data transfer. Many authorities also maintain the register of data controllers and databases. They must approve licensing for data controllers.

A number of countries that do not have a comprehensive act still have a commissioner. A major power of these officials is to focus public attention on problem areas, even when they do not have any authority to fix the problem. They can do this by promoting codes of practice and encouraging industry associations to adopt them. They also can use their annual reports to point out problems. For example, in Canada, the Federal Privacy Commissioner announced in his 2000 report the existence of an extensive database maintained by the federal government. Once the issue became public, the Ministry disbanded the database.

In a number of countries, this official also serves as the enforcer of the jurisdiction's Freedom of Information Act. These include Hungary, Estonia, Thailand and the United Kingdom. On the sub-national level, many of the German Land Commissioners have recently been given the power of information commissioner, and most of the Canadian provincial agencies handle both data protection and freedom of information.

A major problem with many agencies around the world is a lack of resources to adequately conduct oversight and enforcement. Many are burdened with licensing systems, which use much of their resources. Others have large backlogs of complaints or are unable to conduct significant number of investigations. Many that started out with adequate funding find their budgets cut a few years later.

Independence is also a problem. In many countries, the agency is under the control of the political arm of the government or part of the Ministry of Justice and lacks the power or will to advance privacy or criticize privacy invasive proposals. In Japan and Thailand, the oversight agency is under the control of the Prime Ministers Office. In Thailand, the director was transferred in 2000 after conflicts with the Prime Ministers' Office. In 2001, Slovenia amended its Data Protection Act in order to establish an independent supervisory authority and thereby ensure compliance with the Data Protection Directive. This was previously the responsibility of the Ministry of Justice.

Finally, in some countries that do not have a separate office, the role of investigating and enforcing the laws is done by a human rights ombudsman or by a parliamentary official.

Transborder Data Flows and Data Havens

The ease with which electronic data flows across borders leads to a concern that data protection laws could be circumvented by simply transferring personal information to third countries, where the national law of the country of origin doesn't apply. This data could then be processed in those countries, frequently called a "data havens," without any limitations.

For this reason, most data protection laws include restrictions on the transfer of information to third countries unless the information is protected in the destination country. For example, Article 12 of the Council of Europe's 1981

Convention places restrictions on the transborder flows of personal data.⁴⁵ Similarly, Article 25 of the European Directive imposes an obligation on member States to ensure that any personal information relating to European citizens is protected by law when it is exported to, and processed in, countries outside Europe. It states:

The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if the third country in question ensures an adequate level of protection.

This requirement has resulted in growing pressure outside Europe for the passage of strong data protection laws. Those countries that refuse to adopt meaningful privacy laws may find themselves unable to conduct certain types of information flows with Europe, particularly if they involve sensitive data. Determination of a third country's system for protecting privacy is made by the European Commission. The overarching principle in this determination process is that the level of protection in the receiving country must be "adequate" rather than "equivalent." Therefore, a reasonably high standard of protection is expected from the third party, although the precise dictates of the Directive need not be followed.

On July 26, 2000 the European Commission ruled that both Switzerland and Hungary provide "adequate" protection for personal information and therefore that all transfers of personal data to these countries could continue.⁴⁶ In January 2002, the European Commission recognized that the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) provides adequate protection for certain personal data transferred from the European Union to Canada. The Commission's decision of adequacy does not cover any personal data held by federal sector or provincial bodies or information held by personal organizations and used for non-commercial purposes, such as data handled by charities or collected in the context of an employment relationship.⁴⁷ The Commission is currently looking into the privacy protection schemes in

⁴⁵ Council of Europe, Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, 1981, available at <<http://www.coe.fr/eng/legaltxt/108e.htm>>.

⁴⁶ See European Commission Press Release, "Data protection: Commission adopts decisions recognising adequacy of regimes in United States, Switzerland and Hungary," July 27, 2000, available at <http://europa.eu.int/comm/internal_market/en/media/dataprot/news/safeharbor.htm>.

⁴⁷ Commission Decision of December 20, 2001, Official Journal of the European Communities L 2/13, available at <http://www.europa.eu.int/comm/internal_market/dataprot/adequacy/canada-faq_en.htm>

several other non-European Union countries, including New Zealand, Australia, and Hong-Kong.

Another possible way to protect the privacy of information transferred to countries that do not provide “adequate protection” is to rely on a private contract containing standard data protection clauses. This kind of contract would bind the data processor to respect fair information practices such as the right to notice, consent, access and legal remedies. In the case of data transferred from the European Union, the contract would have to meet the standard “adequacy” test, in order to satisfy the Data Protection Directive.⁴⁸ A number of model clauses that could be included in such a contract were outlined in a 1992 joint study by the Council of Europe, the European Commission and the International Chamber of Commerce.⁴⁹ In a June 2000 report (see below), the European Parliament accused the European Commission of a “serious omission” in failing to draft standard contractual clauses that European citizens could invoke in the courts of third countries before the Data Directive came into force.⁵⁰ It recommended that they do so before September 30, 2000.⁵¹ In July 2001, the Commission issued a final decision approving the standard contractual clauses.⁵² During the drafting process, the United States criticized the standard contracts as “unduly burdensome” and “incompatible with real world operations.”⁵³

European Union-United States “Safe Harbor” Agreement

Although the Commission never issued a formal opinion on the adequacy of privacy protection in the United States, there were serious doubts whether the

⁴⁸ See European Union, Internal Market Directorate, Background Information: Transfer of data to non-European Union countries – FAQ, available at <http://europa.eu.int/comm/internal_market/en/media/dataprot/backinfo/info.htm>.

⁴⁹ Joint Study of the Council of Europe and the Commission of the European Communities (1992), available at <http://www.coe.fr/dataprotection/Etudes_Rapports/ectype.htm>.

⁵⁰ European Parliament Resolution on the Draft Commission Decision on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the United States Department of Commerce, available at <http://www.epic.org/privacy/intl/EP_SH_resolution_0700.html>.

⁵¹ For general guidance on the role of contracts see European Union Article 29 Data Protection Working Group, “Transfers of personal data to third countries: Applying Articles 25 and 26 of the European Union data protection directive” July 24, 1998, available at <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp12en.htm>.

⁵² Commission Approves Standard Contractual Clauses For Data Transfers To Non-European Union Countries, Press Release of the Internal Market Directorate, July 18, 2001, available at <http://europa.eu.int/comm/internal_market/en/dataprot/news/clauses2.htm>.

⁵³ “Bush Administration Criticizes European Union Privacy Rules,” EPIC Alert 8.06, March 29, 2001 <http://www.epic.org/alert/EPIC_Alert_8.06.html>.

United States' sectoral and self-regulatory approach to privacy protection would pass the adequacy standard set out in the Directive. The European Union commissioned two prominent United States law professors, who wrote a detailed report on the state of United States privacy protections and pointed out the many gaps in United States protection.⁵⁴

The United States strongly lobbied the European Union and its member countries to find the United States system adequate. In 1998, the United States began negotiating a "Safe Harbor" agreement with the European Union in order to ensure the continued transborder flows of personal data. The idea of the "Safe Harbor" was that United States companies would voluntarily self-certify to adhere to a set of privacy principles worked out by the United States Department of Commerce and the Internal Market Directorate of the European Commission. These companies would then have a presumption of adequacy and they could continue to receive personal data from the European Union. Negotiations on the drafting of the principles lasted nearly two years and were the subject of bitter criticism by privacy and consumer advocates.⁵⁵ In early July, the European Parliament approved a forceful resolution that the agreement needed to be re-negotiated in order to provide adequate protection.⁵⁶

On July 26, 2000, the Commission approved the agreement.⁵⁷ The Commission did, however, promise to re-open negotiations on the arrangement if the remedies available to European citizens prove inadequate. European Union member states were given 90 days to put the Commission's decision into effect and United States companies began joining Safe Harbor in November 2000. There is an open-ended grace period for United States signatory companies to implement the principles.

The principles require all signatory organizations to provide individuals with "clear and conspicuous" notice of the kind of information they collect, the purposes for which it may be used, and any third parties to whom it may be disclosed. This notice must be given at the time of the collection of any personal information or "as soon thereafter as is practicable." Individuals must be given the ability to choose (opt-out of) the collection of data where the information is

⁵⁴ Paul M. Schwartz and Joel R. Reidenberg, *Data Privacy Law* (Michie 1996).

⁵⁵ See e.g., Public Comments Received by the United States Department of Commerce in Response to the Safe Harbor Documents April 5, 2000, available at <<http://www.ita.doc.gov/td/ecom/Comments400/publiccomments0400.html>>.

⁵⁶ European Parliament Resolution, *supra*, n.50.

⁵⁷ Commission Decision on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the United States Department of Commerce, available at <http://europa.eu.int/comm/internal_market/en/media/dataprot/news/decision.pdf>.

either going to be disclosed to a third party or used for an incompatible purpose. In the case of sensitive information, individuals must expressly consent (opt-in) to the collection. Organizations wishing to transfer data to a third party may do so if the third party subscribes to Safe Harbor or if that third party signs an agreement to protect the data. Organizations must take reasonable precautions to protect the security of information against loss, misuse and unauthorized access, disclosure, alteration and destruction. Organizations must provide individuals with access to any personal information held about them, and with the opportunity to correct, amend, or delete that information where it is inaccurate. This right is to be granted only if the burden or expense of providing access would not be disproportionate to the risks to the individual's privacy or where the rights of persons other than the individual would not be violated. In terms of enforcement, organizations must provide access to readily available and affordable independent recourse mechanisms that may investigate complaints and award damages. They must issue follow up compliance procedures and must adhere to sanctions for failing to comply with the Principles.

Privacy advocates and consumer groups both in the United States and Europe are highly critical of the European Commission's decision to approve the agreement, which they say will fail to provide European citizens with adequate protection for their personal data.⁵⁸ The agreement rests on a self-regulatory system whereby companies merely promise not to violate their declared privacy practices. There is little enforcement or systematic review of compliance. The Safe Harbor status is granted at the time of self-certification. There is no individual right to appeal or right to compensation for privacy infringements. There is an open-ended grace period for United States signatory companies to implement the principles. The agreement will only apply to companies overseen by the Federal Trade Commission and Department of Transportation (excluding the financial and telecommunications sectors) and there are special exceptions granted for public records information protected by European Union law.

In February 2002, the European Commission issued a report on the practical operation of the European Union-United States Safe Harbor Agreement.⁵⁹ This was the first report to evaluate the success of the agreement. It concluded that all the essential elements of the agreement are in place and that a structure exists for individuals to lodge complaints if they feel their rights have been infringed. It did

⁵⁸ See, e.g. the earlier Statement of the Transatlantic Consumer Protection Dialogue on United States Department of Commerce Draft International Safe Harbor Privacy Principles and FAQs March 30, 2000, available at <<http://www.tacd.org/ecommercef.html#usdraft>>.

⁵⁹ European Commission Staff Working Paper, February 2002, available at <http://europa.eu.int/comm/internal_market/en/dataprot/news/02-196_en.pdf>

find, however, that there is not sufficient transparency among the organizations that have signed up to Safe Harbor and that not all dispute resolution providers relied on to enforce Safe Harbor actually comply with the privacy principles in the agreement itself. The Commission will issue a full evaluation of the agreement in 2003.

In July 2002, the Article 29 Data Protection Working Party issued a working paper on the functioning of the agreement. In it, the Working Party expressed its intention to study the agreement in further detail with particular regard to “possible gaps between the principles...and the implementing practices” and also “the transparency requirements to be met by organizations.” The Working Party called on all authorities, organizations and companies concerned to enhance compliance and awareness of the Agreement.⁶⁰

⁶⁰ “Working Document on the Functioning of the Safe Harbor Agreement,” Article 29 Data Protection Working Party, 11194/02/EN, July 2, 2002, available at <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp62_en.pdf>

Threats to Privacy

The Response to September 11, 2001

Even with the adoption of legal and other protections, violations of privacy remain a concern. In many countries, laws have not kept up with the technology, leaving significant gaps in protections. In other countries, law enforcement and intelligence agencies have been given significant exemptions. Without adequate oversight and enforcement, the mere presence of a law may not provide adequate protection. Finally, with recent transformations to data protection regimes, further gaps, exemptions, and inadequacies are arising.

It may take some years to fully evaluate the effects of September 11th 2001 on privacy and civil liberties. Shortly after the events of that day, previous proposals were re-introduced, and new policies with similar objectives were drafted to extend police surveillance authority.

The policy changes were not limited to the United States, as a large number of countries responded to the threat of terrorism. The country reports in this survey outline, in more detail, the many legislative shifts that took place around the world.

It was a time of fear, flux and uncertainty. The United Nations responded with Resolution 1368 calling on increased cooperation between countries to prevent and suppress terrorism.⁶¹ NATO invoked Article 5, claiming an attack on any NATO member country is an attack on all of NATO; legislatures responded accordingly. The Council of Europe condemned the attacks, called for solidarity, and also called for increased cooperation in criminal matters.⁶² Later the Council of Europe Parliamentary Assembly called on countries to ratify conventions combating terrorism, lift any reservations in these agreements, extend the mandate of police working groups to include “terrorist messages and the

⁶¹ United Nations Resolution 1368 (2001), adopted by the Security Council at its 4370th meeting, September 12, 2001.

⁶² Council of Europe Committee of Ministers, Declaration of the Committee of Ministers on the fight against international terrorism, adopted by the Committee of Ministers at the 763rd meeting of the Ministers’ Deputies, September 12, 2001.

decoding thereof.”⁶³ The European Union responded similarly, pushing for a European arrest warrant, common legislative frameworks for terrorism, increasing intelligence and police cooperation, freezing assets and ensuring passage of the Money Laundering Directive.⁶⁴ The OECD furthered its support for the Financial Action Task Force on Money Laundering and, along with the G-7⁶⁵ and the European Commission, called for the extension of its mandate to combat terrorist financing.⁶⁶ These calls for international cooperation were perceived by many as impetus to create new laws.

The European Commission considered requiring every member state of the European Union to make cyber-attacks punishable as a terrorist offence. New Zealand minimized public consultation on a proposed law to freeze the financial assets of suspected terrorists because the government felt it was bound by United Nations Security Council resolutions. France expanded police powers to search private property without warrants. Germany reduced authorization restraints on interception of communications, and increased data sharing between law enforcement and national security agencies.

Australia and Canada both introduced laws to redefine *terrorist activity* and to grant powers of surveillance to national security agencies (*ASIO* and *CSIS* respectively) for domestic purposes if terrorist activity or a terrorist affiliation is suspected. India passed a law to allow authorities to detain suspects without trial, conduct increased wiretapping, and seize funds and property. The United Kingdom passed a law permitting the retention of data for law enforcement purposes in contravention to existing data protection rules. The United States passed a number of laws, including the USA-PATRIOT Act, which increases surveillance powers and minimizes oversight and due process requirements.

The above list of international and national initiatives is not exhaustive. New policies are being proposed every week with the goal of investigating, preventing, and suppressing terrorist activity. However, within this deluge of new policy proposals, a number of trends may be identified.

⁶³ Council of Europe Parliamentary Assembly, Recommendation 1534 (2001), Democracies Facing Terrorism, September 26, 2001 (28th Sitting), available at <<http://assembly.coe.int/>>.

⁶⁴ Commission of the European Communities, Brussels, Report From The Commission, Overview of European Union action in response to the events of the 11 September and assessment of their likely economic impact, 17.10.2001, COM(2001) 611 final.

⁶⁵ Statement of G-7 Finance Ministers and Central Bank Governors, Action Plan to Combat the Financing of Terrorism, October 6, 2001.

⁶⁶ See generally, <<http://www1.oecd.org/fatf/>>.

Increased Communications Surveillance and Search and Seizure Powers

Almost every country that changed its laws to reflect the environment following September 2001 increased the ability of law enforcement and national security agencies to perform interception of communications, and transformed the powers of search and seizure, and an increase in the type of data that can be accessed.

The novelty in these initiatives tends to arise in the reduced authorization requirements and oversight. This includes initiatives to weaken due process requirements; as occurred in Canada where the first anti-terrorism bill proposed that law enforcement agencies will no longer be required to justify the need for the wiretap. That is, in existing law, the judge authorizing the interception would need to be satisfied that “other investigative procedures have been tried and have failed, other investigative procedures are unlikely to succeed or the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures.”⁶⁷ In the law, an exception is established for all offences that fall under the broad category of “terrorist activity.” Other parts of the law allow for interception authorization by the Minister of Defence instead of requiring judicial authorization.

There is also a general increase in the breadth of application of these powers, by incorporating and including new technologies and communications infrastructures, permitting additional government agencies to use these powers, and formalize roving powers. The USA-PATRIOT Act codified the use of Carnivore-style Internet surveillance technology, granting access to sensitive traffic data with only a court order rather than a judicial warrant. Moreover, the reporting regime in the United States was weakened with amendments to the Foreign Intelligence Surveillance Act so that fewer warrants would have to be requested and reported because the expiration time period was increased, and ‘generic’ orders could be requested allowing one warrant to be served on multiple service providers.

Attempts to differentiate the authorization and oversight requirements based on the communications-technology also occurred. The Australian government proposed in its Telecommunications Interception Legislation Amendment Bill 2002 to grant powers to intercept and read email, SMS and voice mail messages without a warrant because these communications were considered access to ‘stored’ data rather than ‘intercepted’ in real-time. This proposed act was

⁶⁷ Criminal Code of Canada, (CC 186(1b)), 2000.

rejected in the Senate in June 2002;⁶⁸ however, the Government claims that it “remains of the view that the approach adopted in the bill with respect to stored information is appropriate. However, to avoid holding up this important package of legislation, the government has agreed to remove these provisions from the bill and to deal with the issue at a later date.”⁶⁹

Weakening of Data Protection Regimes

In 2000, the United Kingdom proposed a policy to require the retention of communications traffic data for up to 7 years by a central government authority.⁷⁰ While the proposal faced significant resistance in the public discourse at that time, in December 2001 a similar policy was introduced and passed under the United Kingdom’s anti-terrorism law in response to the events of September 2001. The new European Union directive on data protection in electronic services also supports the creation of such data retention laws within the European community and is consistent with international pressure to weaken data protection. In October 2001, President Bush sent a letter to the President of the European Commission requesting that the European Union “[c]onsider data protection issues in the context of law enforcement and counterterrorism imperatives,” and as a result to “[r]evise draft privacy directives that call for mandatory destruction to permit the retention of critical data for a reasonable period.”⁷¹ Building from previously articulated concerns that “[d]ata protection procedures in the sharing of law enforcement information must be formulated in ways that do not undercut international cooperation,”⁷² the United States Department of Justice submitted a number of recommendations to the European Commission working group on cybercrime, including the recommendation that

Any data protection regime should strike an appropriate balance between the protection of personal privacy, the legitimate needs of service

⁶⁸ Electronic Frontiers Australia, Media Release: Senate Rejects Email Snooping Law - Victory For Online Privacy, June 28, 2002.

⁶⁹ Statement of Senator Ellison, Minister of Justice and Customs, Senate Official Hansard No.6 2002, June 27, 2002, available at <<http://www.aph.gov.au/hansard/senate/dailys/ds270602.pdf>>.

⁷⁰ Roger Gaspar (NCIS), “Looking to the Future : Clarity on Communications Data Retention Law,” August 21, 2000, ACPO, ACPO(S), HM Customs & Excise, Security Service, Secret Intelligence Service, and GCHQ.

⁷¹ Letter from President George W. Bush to Mr Romano Prodi, President, Commission of the European Communities, Brussels, October 16, 2001, forwarded by the Deputy Chief of Mission, United States Mission to the European Union, available at <<http://www.statewatchchapterorg/news/2001/nov/06Ausalet.htm>>

⁷² Comments of the United States Government on the European Commission Communication on Combating Computer Crime, December 2001, available at <http://www.cybercrime.gov/intl/USComments_CyberCom_final.pdf>.

providers to secure their networks and prevent fraud, and the promotion of public safety.⁷³

This perspective was reiterated in May 2002, this time by the Group of 8 Justice and Interior Ministers, requesting that countries

Ensure data protection legislation, as implemented, takes into account public safety and other social values, in particular by allowing retention and preservation of data important for network security requirements or law enforcement investigations or prosecutions, and particularly with respect to the Internet and other emerging technologies.⁷⁴

Further discussion regarding the reduction of the protections of privacy afforded by data protection law will likely arise in September when the European Commission continues discussion of the implementation of the 1995 directive (95/46/EC).

Individuals and citizens are at the same time losing subject access rights under data protection and freedom of information regimes. In the interests of critical infrastructure protection, access to information is being reduced, limiting government accountability. Meanwhile, in order to protect sensitive investigative and intelligence data, subject access requests are restricted as some data banks are being exempted from both data protection and freedom of information laws.

Increased Data Sharing

A number of policies were introduced to enable and promote increased data sharing, both within and across government agencies, and with the private sector. The sharing of data between agencies introduces purpose-creep where data collected for one purpose is used for another, but also introduces highly sensitive data to arms of government that can not be expected to protect the data adequately.

⁷³ Prepared statement of the United States of America, presented at European Union Forum on Cybercrime, Brussels, 27 November 2001, available at <http://www.cybercrime.gov/intl/MMR_Nov01_Forum.doc>.

⁷⁴ Statement of the G8 Justice and Interior Ministers: Recommendations for Tracing Networked Communications Across National Borders in Terrorist and Criminal Investigations, May 14 2002, Mont Tremblant, Quebec, available at <<http://www.g8j-i.ca/english/doc2.html>>.

There are significant shifts in the policies and practices in the United States with changes to the Attorney General Guidelines regulating the actions and capabilities of the Department of Justice and FBI, increased sharing of information between the FBI and CIA supported by the USA-PATRIOT Act, and proposed policies to increase sharing with local law enforcement agencies. The United States is not alone in introducing such policies. The United Kingdom is proposing “joined-up government” within its consultation paper on modernizing government and public services⁷⁵ to create “data-sharing gateways” and provide “seamless” services. It also tried unsuccessfully to allow practically any government agency to gain access to the traffic data of individuals under the Regulation of Investigatory Powers Act, including local councils and parishes.⁷⁶

The increased flow of data is also coming from the private sector. The United Kingdom and Canada proposed laws to grant law enforcement agencies access to travelers’ information. The United Kingdom Home Office has recommended that it gain access to information from every passenger before international flights.⁷⁷ The Canadian policy proposes to grant both the federal law enforcement and the intelligence agencies access to air passenger information, regardless of domestic or international travel, and to match this data with other personal information,⁷⁸ for a wide number of purposes and investigations, not limited only to terrorism.⁷⁹

Similarly, the European Union is considering granting Europol access to the Schengen Information System, including privileges to change the information held on travelers.⁸⁰ Germany has recommended to the European Union the creation of a database of “known trouble-makers,” to be used “for criminal prosecution purposes and in order to avert dangers constitute a proper and necessary tool in the fight against international terrorism. However, in view of the fact that members and supporters of terrorist groups are known to roam

⁷⁵ The Performance and Innovation Unit of the Cabinet Office, “Privacy and data-sharing: The way forward for public services,” April 2002, available at <<http://www.cabinet-office.gov.uk/innovation/2002/privacy/report/>>.

⁷⁶ “FIPR appalled by Huge Increase in Government Snooping,” Foundation for Information Policy Research Press Release, June 10, 2002, available at <<http://www.fipr.org/press/020610snooping.html>>.

⁷⁷ “Chaos’ warning over airport security plan,” BBC News Online, July 6, 2002, available at <http://news.bbc.co.uk/1/hi/english/uk/newsid_2104000/2104280.stm>.

⁷⁸ Solicitor General of Canada, RCMP and CSIS Access to Airline Passenger Information, available at <<http://www.sgc.gc.ca/EPub/Pol/eAirPassInfo.htm>>.

⁷⁹ Letter to Honourable David Collenette, Minister of Transport, on the subject of Bill C-55, from the Privacy Commissioner of Canada, George Radwanski, June 18, 2002. available at <http://www.privcom.gc.ca/media/nr-c/02_05_b_020618_e.asp>.

⁸⁰ “Europol to be given access to the S.I.S., then custody?” Statewatch, March 27, 2002.

across Europe, the measure would be much more effective if it were applied by all European Union Member States.”

Data sharing between financial institutions and with government agencies has also increased. New money laundering agreements and regulations have been introduced to increase surveillance of transactions, and even expanded to include hedge funds and money transfer firms.⁸¹ Donations to charities are receiving further scrutiny as both the charities and the donors are monitored to investigate links with terrorist groups.⁸² Some financial institutions are also sharing personal information between themselves in order to minimize risk of clients being terrorists, or “undesirables.”⁸³

Increased Profiling and Identification

Following from data sharing, there are a number of proposals to create profiles or increase the existing profiles of individuals. This occurs in a number of ways; the most immediate appears to be the profile of travelers. There are proposals for a *next generation* computer-assisted passenger prescreening system that will bring in data from credit-reporting agencies and other companies,⁸⁴ and even previous flights and registries, set for data mining.⁸⁵ Other proposals include trusted-traveler programs involving biometrics in both the United States and Germany,⁸⁶ similar to schemes used at Ben Gurion Airport in Tel Aviv. ⁸⁷ Some airports have also installed face-recognition technologies, while similar technologies are being implemented at national monuments, and even beaches.

In the longer term there are a number of proposals to increase profiling of citizens and non-citizens. These proposals are typically enhanced and complemented by national identification schemes, enhanced with biometrics.

⁸¹ Glenn R. Simpson and Jathon Sapsford, “New Rules for Money-Laundering,” *The Wall Street Journal*, April 23, 2002.

⁸² “Financial Action Task Force on Money Laundering Special Recommendations on Terrorist Financing,” available at <http://www.fatf-gafi.org/SReecsTF_en.htm>.

⁸³ Robert O’Harrow Jr., “Financial Database To Screen Accounts: Joint Effort Targets Suspicious Activities,” *Washington Post*, May 30, 2002; at E01.

⁸⁴ “Special Report: New Threats To Privacy: The Intensifying Scrutiny at Airports,” *Business Week*, June 5, 2002.

⁸⁵ Robert O’Harrow Jr., “Intricate Screening Of Fliers In Works -- Database Raises Privacy Concerns,” *Washington Post*, February 1, 2002, at A01.

⁸⁶ “Iris Scans Take off at Airports,” *ComputerWorld*, July 17, 2002.

⁸⁷ Ricardo Alonso-Zaldivar, “‘Trusted’ Air Travelers Would Minimize Wait Security: Passengers who Voluntarily Agree to a Background Check Could be Issued a Special Credential,” *Los Angeles Times*, February 5, 2002.

There was considerable discussion in the United States in introducing such a national ID card scheme but no formal policy was introduced. Meanwhile non-citizens may already be tracked at border entry points and as they move within the country. A system called Student and Exchange Visitor Information System keeps track of foreign students to ensure that they are still registered and maintains a log of their addresses.

The United Kingdom is proposing the implementation of ‘entitlement cards’ in an effort to deal with immigration and illegal work, identity theft, but also supported by the fight against terrorism. Similarly, Hong Kong is planning to introduce a biometric chip identity card to verify fingerprints to authenticate travelers into China.

None of the above trends are necessarily new; the novelty is the speed in which these policies gained acceptance, and in many cases, became law.

Identity systems

Identity (ID) cards

Identity (ID) cards are in use in one form or another in virtually all countries of the world. The type of card, its functions, and integrity vary enormously. While a number of countries have official, compulsory, national ID cards that are used for a variety of purposes, many countries do not. These include Australia, Canada, India, Ireland, New Zealand, the United States and the Nordic countries. Those that do have such a card include Belgium, Egypt, France, Germany, Greece, Hong Kong, Malaysia, and South Africa.

Nationwide ID systems are established for a variety of reasons. Race, politics and religion often drive the deployment of ID cards.⁸⁸ The fear of insurgence, religious differences, immigration, or political extremism have been all too common motivators for the establishment of ID systems that aim to force undesirables in a State to register with the government, or make them vulnerable in the open without proper documents.

⁸⁸ Richard Sobel, *The Degradation of Political Identity Under a National Identification System*, 8 B.U. J. Sci. & Tech. 37, 48 (2002). See also National Research Council, “IDs -- Not That Easy: Questions About Nationwide Identity Systems,” 2002, available at <http://www.nap.edu/catalog/10346.html?opi_newsdoc041102>.

In recent years technology has rapidly evolved to enable electronic record creation and the construction of large commercial and state databases. A national identifier contained in an ID card enables disparate information about a person that is stored in different databases to be easily linked and analyzed through data mining techniques. ID cards are also becoming "smarter" - the technology to build microprocessors the size of postage stamps and put them on wallet sized cards has become more affordable. This technology enables multiple applications such as a credit card, library card, health care card, driver's license and government benefit program information to be all stored on the same national ID along with a password or a biometric identifier. Governments in Finland, Malaysia, and Singapore have experimented with such "Smart" ID cards. In July 2002, the Labor government in the United Kingdom launched a six-month public consultation process on whether the United Kingdom should adopt an "entitlement card" with similar features.⁸⁹ Critics contend that such cards, especially when combined with information contained in databases, enable intrusive profiling of individuals and create a misplaced reliance on a single document, which enables precisely the type of fraud the cards are meant to eliminate.⁹⁰

In a number of countries, these systems have been successfully challenged on constitutional privacy grounds. In 1998, the Philippine Supreme Court ruled that a national ID system violated the constitutional right to privacy.⁹¹ In 1991, the Hungarian Constitutional Court ruled that a law creating a multi-use personal identification number violated the constitutional right of privacy.⁹² The 1997 Portuguese Constitution states "Citizens shall not be given an all-purpose national identity number."⁹³

In other countries, opposition to the cards combined with the high economic cost and other logistical difficulties of implementing the systems has led to their withdrawal. Massive protests against the Australia Card in 1987 resulted in the near collapse of the government. Card projects in South Korea and Taiwan were

⁸⁹ "Entitlement Cards and Identity Fraud: A Consultation Paper," Presented to the Parliament by the Secretary of State for the Home Department, July 2002, available at <http://www.homeoffice.gov.uk/cpd/entitlement_cards.pdf>.

⁹⁰ Simon Davies. "The Id Card Is The Fraudster's Friend," *The Sunday Telegraph*, July 7, 2002. See also, Oscar H. Gandy, Jr., *The Panoptic Sort: A Political Economy of Personal Information* (Westview Press 1993).

⁹¹ Philippine Supreme Court Decision of the National ID System, July 23, 1998, G.R. 127685, available at <<http://bknet.org/laws/nationalid.html>>.

⁹² Constitutional Court Decision No. 15-AB of 13 April 1991, available at <http://www.privacy.org/pi/countries/hungary/hungarian_id_decision_1991.html>.

⁹³ Article 35 (5), Constitution Of The Portuguese Republic 1976 (as amended), available at <http://www.parlamento.pt/leis/constituicao_ingles/crp_uk.htm#article_35>.

also stopped after widespread protests. In the United States plans to convert the state driver's license into a nationwide system of identification have stalled because of the stiff resistance from a broad coalition of civil society groups.⁹⁴

Biometrics

Biometrics is the identification or verification of someone's identity on the basis of physiological or behavioral characteristics. Biometrics involves comparing a previously captured unique characteristic of a person to a new sample provided by the person. This information is used to authenticate or verify that a person is who they said they were (a one-to-one match) by comparing the previously stored characteristic to the fresh characteristic provided. It can also be used for identification purposes where the fresh characteristic is compared against all the stored characteristics (a one-to-many match). New biometric technology attempts to automate the identification or verification process by converting the provided biometric into an algorithm, which is then used for matching purposes. The computer matching technique necessarily produces either false positives, where a person is incorrectly identified as someone else, or false negatives, where a person who is meant to be identified by the system is not correctly identified. The two error rates are dependent, so for example reducing the number of false positives increases the number of false negatives. The tolerance level is adjusted depending on the need for security in the application.

The most popular forms of biometric ID are fingerprints, retina/iris scans, hand geometry, voice recognition, and digitized (electronically stored) images. The technology is gaining interest from governments and companies because, unlike other forms of ID such as cards or papers, it can be more difficult to alter or tamper with one's own physical or behavior characteristics. Important questions remain, however, about the effectiveness of the automated biometric matching techniques, particularly for large-scale applications.⁹⁵ Critics also argue that widespread deployment of biometric identification technology could remove the veil of anonymity or pseudo-anonymity in most daily transactions through the creation an electronic trail of people's movements and habits.⁹⁶

⁹⁴ See generally EPIC's National ID Pages <http://www.epic.org/privacy/id_cards/>.

⁹⁵ Deutsche Bank Research, "Biometrics – Hype and Reality," May 22, 2002, available at <<http://www.dbresearch.com/PROD/999/PROD0000000000043270.pdf>>

⁹⁶ Roger Clarke, "Biometrics and Privacy," April 15, 2001, available at <<http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html>>.

Biometrics schemes are being implemented across the world. The technology is widely used in small settings for access control to secure locations such a nuclear facility or bank vault. It is increasingly being used for broader applications such as retail outlets, government agencies, childcare centers, police forces and automated-teller machines. Spain has commenced a national fingerprint system for unemployment benefits and healthcare entitlements. Russia has announced plans for a national electronic fingerprint system for banks. Jamaicans are required to scan their thumbs into a database before qualifying to vote in elections. In France and Germany, tests are under way with equipment that puts fingerprint information onto credit cards. Many computer manufacturers are considering including biometric readers on their systems for security purposes.

The most controversial form of biometrics – DNA identification – is benefiting from new scanning technology that can automatically match DNA samples against a large database in minutes. Police forces in several countries including Canada, Germany, and the United States have created national DNA databases. Samples are being routinely taken from a larger group of people. Initially, it was only individuals convicted of sexual crimes. Then it was expanded to people convicted of other violent crimes and then to arrests. Now, many jurisdictions are collecting samples from all individuals arrested, even for the most minor offenses. Former New York City Mayor Rudolf Giuliani even proposed that all children have a DNA sample collected at birth. In Australia, the United Kingdom, and the United States, police have been demanding that all individuals in a particular area voluntarily provide samples or face being considered a suspect. United States Attorney General Ashcroft has testified that he has asked the FBI to increase the capacity of its database from 1.5 million to 50 million profiles.⁹⁷

At the same time, DNA data has been used as exculpatory evidence in many criminal trials. (For more discussion of this subject see the section on *Genetic Identification* at 78)

Surveillance of Communications

Most countries around the world regulate the interception of communications by governments and private individuals and organizations. These controls typically

⁹⁷ Attorney General Transcript, News Conference - DNA Initiatives, Monday, March 4, 2002, DOJ Conference Center.

take the form of constitutional provisions protecting the privacy of communications and laws and regulations that implement those requirements.

There has been great pressure on countries to adopt wiretapping laws to address new technologies. These laws are also in response to law enforcement and intelligence agencies pressure to increase surveillance capabilities. In Japan, wiretapping was only approved as a legal method of investigation in 1999. Other countries such as Australia, Germany, New Zealand, South Africa and the United Kingdom have all updated their laws to facilitate surveillance of new technologies.

The United States government has been at the forefront of promoting greater use of electronic surveillance. Former FBI Director Louis Freeh traveled extensively around the world, promoting the use of wiretapping in newly democratic countries such as Hungary and the Czech Republic. At the same time, the United States has led world efforts to ensure that all communications technologies have built in surveillance capabilities and to prohibit the manufacture and use of equipment that cannot be eavesdropped upon. The United States has also been working through international organizations such as the OECD, G-8 and the Council of Europe to promote surveillance.

Legal Protections and Human Rights

It is recognized worldwide that wiretapping and electronic surveillance is a highly intrusive form of investigation that should only be used in limited and unusual circumstances. Nearly all major international agreements on human rights protect the right of individuals from unwarranted invasive surveillance.

Nearly every country in the world has enacted laws on the interception of oral, telephone, fax and telex communications. In most democratic countries, intercepts are initiated by law enforcement or intelligence agencies only after it has been approved by a judge or some other kind of independent magistrate or high level official and generally only for serious crimes. Frequently, it must be shown that other types of investigation were attempted and were not successful. There is some divergence on what constitutes a 'serious crime', and appropriate approval.

A number of countries including France and the United Kingdom have created special commissions that review wiretap usage and monitor for abuses. These bodies have developed an expertise in the area that most judges who authorize

surveillance do not have, while they also have the ability to conduct follow up investigations once a case is complete. In other countries, the Privacy Commission or Data Protection Commission has some ability to conduct oversight of electronic surveillance.

An important oversight measure that many countries employ is the requiring of annual public reporting of information about the use of electronic surveillance by government departments. These reports typically provide summary details about the number of uses of electronic surveillance, the types of crimes that they are authorized for, their duration and other information. This is a common feature of wiretap laws in English-speaking countries and many others in Europe. Countries that issue annual reports on the use of surveillance include Australia, Canada, France, New Zealand, Sweden, the United Kingdom, and the United States.

These countries recognize that it is necessary to allow for people outside governments to know about its uses to limit abuses. They are widely used in many countries by the Parliaments for oversight and also by journalists, NGOs and others to examine the activities of law enforcement. The reports have shown an increase in the use of surveillance in many countries including the United States and the United Kingdom while others such as Canada have remained steady.

These laws are designed to ensure that legitimate and normal activities in a democracy such as journalism, civic protests, trade union organizing or political opposition are free from being subjected to unwarranted surveillance because they have different interests and goals than those in power. It also ensures that relatively minor crimes, especially those that would not generally involve telecommunications for facilitation, are not used as a pretext to conduct intrusive surveillance for political or other reasons.

However, wiretapping abuses have been revealed in most countries, sometimes occurring on a vast scale involving thousands of illegal taps. The abuses invariably affect anyone “of interest” to a government. Targets include political opponents, student leaders and human rights workers.⁹⁸ This can occur even in the most democratic of countries such as Denmark and Sweden, where it was recently disclosed that intelligence agencies were conducting surveillance of thousands of left-leaning activists for nearly 40 years.

⁹⁸ United States Department of State, Country Report on Human Rights Practices 1997, January 30, 1998.

The U.N. Commissioner on Human Rights in 1988 made clear that human rights protections on the secrecy of communications broadly covers all forms of communications:

Compliance with Article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.⁹⁹

The need for greater protection is recognized by many democratic countries around the world. Increasingly new standards, technologies and new policies are complicating the situation.

Legal and Technical Standards for Surveillance: Building in Big Brother

In the past 15 years, the United States government has led a worldwide effort to limit individual privacy and enhance the capability of its police and intelligence services to eavesdrop on personal conversations. This campaign had two strategies. The first is to promote laws that make it mandatory for all companies that develop digital telephone switches, cellular and satellite phones and all developing communication technologies to build in surveillance capabilities; the second is to seek limits on the development and dissemination of products, both in hardware and software, that provide encryption, a technique that allows people to scramble their communications and files to prevent others from reading them.¹⁰⁰

Law enforcement agencies have traditionally worked closely with telecommunications companies to formulate arrangements that would make phone systems “wiretap friendly.” These agreements range from allowing police physical access to telephone exchanges, to installing equipment to automate the interception. Because most telecommunications operators were either monopolies or operated by government telecommunications agencies, this process was generally hidden from public view.

⁹⁹ United Nations Human Rights Commissioner, The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Article 17), CCPR General Comment 16, April 8, 1988.

¹⁰⁰ See David Banisar and Simon Davies, “The Code War,” Index on Censorship, January 1998.

Following deregulation and new entries into telecommunications in the United States in the early 1990s, law enforcement agencies, led by the FBI, began demanding that all current and future telecommunications systems be designed to ensure that they would be able to conduct wiretaps. After several years of lobbying, the United States Congress approved the Communications Assistance for Law Enforcement Act (CALEA) in 1994.¹⁰¹ The act sets out legal requirements for telecommunications providers and equipment manufacturers on the surveillance capabilities that must be built into all telephone systems used in the United States. In 1999, at the request of the Federal Bureau of Investigation, an order was issued under CALEA requiring carriers to make available the physical location of the antenna tower that a mobile phone uses to connect at the beginning and end of a call.¹⁰²

Due to heavy lobbying, the Internet Service Providers in the United States have so far been exempted from implementing these technical requirements. In other countries the computer industries have not been so fortunate. In Australia the Telecommunications Act 1997 places obligations on telecommunications operators to positively assist law enforcement in the performance of their duties and to provide an interception capability. The costs of these obligations are borne by the operators themselves.¹⁰³ Furthermore, the 2001 Cybercrime Act allows executing officers to require a “specified person” with “knowledge of a computer or a computer system” to provide assistance in accessing, copying or converting data held on or accessible from that computer. Failing to provide this assistance is an offence punishable by six months imprisonment.¹⁰⁴

In the United Kingdom the Regulation of Investigatory Powers Act 2000 requires that telecommunications operators maintain a “reasonable interception capability” in their systems and be able to provide on notice certain “traffic data.”¹⁰⁵ It also imposes an obligation on third parties to hand over encryption keys. These requirements were recently clarified in the Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002.

¹⁰¹ See EPIC Wiretap Pages <<http://www.epic.org/privacy/wiretap/>>.

¹⁰² Third Report and Order adopted by the Federal Communications Commission, In the Matter of Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, FCC 99-230 (1999) (the "Order"). The Order was released on August 31, 1999. A summary of the Order was published in the Federal Register on September 24, 1999. See 64 Fed. Reg. 51710.

¹⁰³ Telecommunications Act 1997, Parts 14 and 15.

¹⁰⁴ Cybercrime Act 2001, No. 161, 2001, inserting sections 3LA and 201A in the Crimes Act 1914, available at <<http://scaleplus.law.gov.au/html/pasteact/3/3486/pdf/161of2001.pdf>>.

¹⁰⁵ Regulation of Investigatory Powers Act 2000, sections 12 (1) and 22 (4) respectively, available at <<http://www.hmso.gov.uk/acts/acts2000/20000023.htm>>.

In the Netherlands, a new Telecommunications Act was approved in December 1998 that required that Internet Service Providers have the capability by August 2000 to intercept all traffic with a court order and maintain users logs for three months.¹⁰⁶ The law was enacted after XS4ALL, a Dutch ISP, refused to conduct a broad wiretap of electronic communications of one of its subscribers. In New Zealand, the Telecommunications (Residual Powers) Act 1987 requires network operators to assist in the operation of a call data warrant (equivalent to the United States trap and trace or pen register warrant).¹⁰⁷ An obligation to assist in the operation of a full interception warrant is now also being considered in New Zealand. The Telecommunications (Interception Capabilities) Bill currently being drafted by the Government would require all Internet Service Providers and telephone companies to upgrade their systems so that they are able to assist the police and intelligence agencies intercept communications. It would also require a telecommunications operator to decrypt the communications of a customer if that operator had provided the encryption facility.¹⁰⁸

In January 2002, a new Law on the surveillance of mail and telecommunications entered into force in Switzerland, requiring ISPs to take all necessary measures to allow for interception.¹⁰⁹

International cooperation played a significant role in the development of these standards. In 1993, the FBI began hosting meetings at its research facility in Quantico, Virginia called the “International Law Enforcement Telecommunications Seminar” (ILETS). The meetings included representatives from Canada, Hong Kong, Australia and the European Union. At these meetings, an international technical standard for surveillance, based on the FBI’s CALEA demands, was adopted as the “International Requirements for Interception.” In January 1995, the Council of the European Union approved a secret resolution adopting the ILETS standards.¹¹⁰ Following this, many countries adopted the resolution into their domestic laws without revealing the role of the FBI in developing the standard. Following the adoption, the European Union and the

¹⁰⁶ Telecommunications Act 1998. Rules pertaining to Telecommunications (Telecommunications Act), December 1998.

¹⁰⁷ Telecommunications (Residual Powers) Act 1987, section 10D.

¹⁰⁸ “Interception Capability – Government Decisions,” New Zealand Government Executive Press Release, March 21, 2002, available at <<http://www.executive.govt.nz/speechaptercfm?speechralph=37658&SR=0>>.

¹⁰⁹ Loi fédérale sur la surveillance de la correspondance postale et des télécommunications, (www.admin.ch/ch/f/rs/c780_1.html) and the respective new decree (www.admin.ch/ch/f/rs/c780_11.html)

¹¹⁰ Council Resolution of 17 January 1995 on the lawful interception of telecommunications, Official Journal of the European Communities November 4, 1996, available at <http://europa.eu.int/eur-lex/en/lif/dat/1996/en_496Y1104_01.html>.

United States offered a Memorandum of Understanding (MOU) for other countries to sign to commit to the standards. A number of countries including Canada and Australia immediately signed the MOU. Others were encouraged to adopt the standards to ensure trade. International standards organizations, including the International Telecommunications Union and the European Telecommunication Standardisation Institute (ETSI), were then successfully approached to adopt the standards.

The ILETS group continued to meet. A number of committees were formed and developed a more detailed standard extending the scope of the interception standards. The new standards were designed to apply to a wide range of communications technologies, including the Internet and satellite communications. It also set more detailed criteria for surveillance across all technologies. The result was a 42-page document called ENFOPOL 98 (the European Union designation for documents created by the European Union Police Cooperation Working Group).¹¹¹

In 1998, the document became public and generated considerable criticism. The committees responded by removing most of the controversial details and putting them into a secret operations manual that has not been made publicly available. The new document, now called ENFOPOL 19, expanded the type of surveillance to include “IP address (electronic address assigned to a party connected to the Internet), credit card number and E-mail address.”¹¹² In April 1999, the Council proposed the new draft council resolution to adopt the ENFOPOL 19 standards into law in the European Union. The Council of Ministers revised the document and, in June 2000, approved a resolution calling for countries:

to ensure that, in the development and implementation – in cooperation with communication service providers – of any measures which may have a bearing on the carrying out of legally authorised forms of interception of telecommunications, the law enforcement operational needs... are duly taken into account¹¹³

¹¹¹ ENFOPOL 98, September 1998, available (in German) at <<http://www.heise.de/tp/deutsch/special/enfo/6326/1.html>>. See also Duncan Campbell, “Special Investigation: ILETS and the ENFOPOL 98 Affair,” Heise Online, April 29, 1999, available at <<http://www.heise.de/tp/english/special/enfo/6398/1.html>>.

¹¹² Draft Council Resolution on the Lawful Interception of Telecommunications in Relation to New Technologies ENFOPOL 19, March 15, 1999.

¹¹³ Council of the European Union, Council Resolution on law enforcement operational needs with respect to public telecommunication networks and services, 9194/01, ENFOPOL 55, June 20, 2001.

The annex for the document sets out detailed guidelines for interception requirements for “all telecommunications services, circuit and packet switched, fixed and mobile networks and services.” It expands the coverage of the original International User Requirements (IURs) to now include networking technologies, without acknowledging that technologies such as computer networking generate more and greater details of information including web browsing and mobile location information and thus applying traditional surveillance analogies result in more intrusive surveillance.

Internet Surveillance: Black Boxes and Key Loggers

A related development has been the use of “black boxes” on ISP networks to monitor user traffic. The actual workings of these black boxes are unknown to the public. What little information has been made public reveals that many of the systems are based on “packet sniffers” typically employed by computer network operators for security and maintenance purposes. These are specialized software programs running in a computer that is hooked into the network at a location where it can monitor traffic flowing in and out of systems. These sniffers can monitor the entire data stream searching for key words, phrases or strings such as net addresses or e-mail accounts. It can then record or retransmit for further review anything that fits its search criteria. In many of the systems, the boxes are connected to government agencies by high speed connections.

The April 2000, it was publicly revealed that the FBI had developed and was using an Internet monitoring system called “Carnivore” (now called DCS 1000).¹¹⁴ The system places a PC running Windows NT at an Internet Service Provider’s offices and can monitor all traffic about a user including e-mail and browsing. Carnivore “can scan millions of e-mails a second” and “would give the government, at least theoretically, the ability to eavesdrop on all customers’ digital communications, from e-mail to online banking and Web surfing.”¹¹⁵ In response to the public uproar over Carnivore, Attorney General Janet Reno announced that the technical specifications of the system would be disclosed to a “group of experts” to allay public concerns.¹¹⁶ In the fall of 2000, the Justice Department commissioned a team of experts at the IIT Research Institute and the Illinois Institute of Technology Chicago-Kent College of Law (IITRI) to

114 Testimony of Robert Corn-Revere, before the Subcommittee on the Constitution of the Committee on the Judiciary, United States House of Representatives, The Fourth Amendment and the Internet, April 6, 2000, available at <<http://www.house.gov/judiciary/corn0406.htm>>.

115 “FBI’s System to Covertly Search E-Mail Raises Privacy,” Wall Street Journal, July 11, 2000.

116 “Reno to double-check Carnivore’s bite,” Reuters, July 13, 2000.

undertake an independent review of the carnivore system. The IITRI group issued its final report on Carnivore in December 2000 and made several recommendations for changes to the system.¹¹⁷

In some countries, there have been laws or decrees enacted to require the systems to build in these boxes. Russia was the first country where this requirement was made public, and according to Russian computer experts, the United States government advised them on implementation. In 1998, the Russian Federal Security Service (FSB) issued a decree on the System for Operational Research Actions on the Documentary Telecommunication Networks (SORM-2) that would require Internet Service Providers to install surveillance devices and high speed links to the FSB which would allow the FSB direct access to the communications of Internet users without a warrant.¹¹⁸ ISPs are required to pay for the costs of installing and maintaining the devices. When an ISP based in Volgograd challenged FSB's demand to install the system, the local FSB and Ministry of Communication attempted to have its license revoked. The agencies were forced to back off after the ISP challenged the decision in court. In a separate case, the Supreme Court ruled in May 2000 that SORM-2 was not a valid ministerial act because it failed several procedural requirements.

Following the Russian lead, in September 1999, Ukrainian President Leonid Kuchma proposed requiring that Internet Service Providers install surveillance devices on their systems based on the Russian SORM system. The rules and a subsequent bill were attacked by the Parliament and withdrawn. However, in August 1999, the security service visited a number of the large ISPs who were reported to have installed the boxes.

In the Netherlands, following the passage of the 1998 Telecommunications Act (see above), the Dutch Forensics Institute¹¹⁹ developed a "black-box" for ISPs to install on their networks. The black box would be under control of the ISP and turned on after receiving a court order. The box would look at authentication traffic of the person to wiretap and divert the person's traffic to law enforcement if the person is online. Due to the inability of ISPs to adopt the requirements of the law, however, its implementation has been delayed.

¹¹⁷ IITRI, Independent Technical Review of the Carnivore System, Final Report, December 8, 2000, available at <http://www.epic.org/privacy/carnivore/carniv_final.pdf>.

¹¹⁸ "Russia Prepares To Police Internet," The Moscow Times, July 29, 1998. More information in English and Russian is available from the Moscow Libertarian Forum <<http://www.libertarium.ru/libertarium/sorm/>>.

¹¹⁹ See Dutch Forensics Institute Homepage <<http://www.holmes.nl/>>.

In China, a system known as the “Great Firewall” routes all international connections through proxy servers at official gateways, where Ministry for Public Security (MPS) officials identify individual users and content, define rights, and carefully monitor network traffic into and out of the country. At a recent security industry conference, the government announced an ambitious successor project known as “Golden Shield.” Rather than relying solely on a national intranet, separated from the global Internet by a massive firewall, China will now build surveillance intelligence into the network, allowing it to “see”, “hear” and “think.”¹²⁰ Content-filtration will shift from the national level to millions of digital information and communications devices in public places and people’s homes.¹²¹ The technology behind Golden Shield is incredibly complex and is based on research developed largely by Western technology firms, including Nortel Networks, Sun Microsystems and others. The Golden Shield efforts do not signal an abandonment of other avenues of access and content control. For example, details are only beginning to emerge about a new “black box” device, derived from technology previously used in airline cockpit data recorders, and broadly similar to the Carnivore system. Chinese Internet police would use the black box technology to monitor dissidents and collect evidence on illegal activities.¹²²

New methods of surveillance, and in particular those capable of circumventing encryption, are also being developed. One such technological device is a “key logger” system. A key logger system records the keystrokes an individual enters on a computer’s keyboard. Keystroke loggers can be employed to capture every key pressed on a computer keyboard, including information that is typed and then deleted. Such devices can be manually placed by law enforcement agents on a suspect’s computer, or installed “remotely” by placing a virus on the suspect’s computer that will disclose private encryption keys.

The question of such surreptitious police decryption methods arose in the case of *United States v Scarfo*.¹²³ There, the FBI manually installed a key logger device on the defendant’s computer in order to capture his PGP encryption password. Once they discovered the password, the files were decrypted, and incriminatory

¹²⁰ G. Walton, *China’s Golden Shield: Corporations and the Development of Surveillance Technology in the People’s Republic of China*, (Rights and Democracy, 2001) at 9
<<http://serveur.ichrdd.ca/english/commdoc/publications/globalization/goldenShieldEng.html>>.

¹²¹ B. Rappert, “Assessing the Technologies of Political Control” (1999) 36(6) *J. of Peace Research* 741. The Golden Shield Project contemplates automated voice recognition through digital signal processing; distributed, network video surveillance; and, content-filtration of the Internet.

¹²² See e.g. L. Weijun, “China Plans to Build Internet Monitoring System,” *China News Daily*, March 20, 2001
<<http://www.cnd.org/Global/01/03/20/010320-3.html>>.

¹²³ *United States v. Scarfo*, 180 F. Supp. 2d 572 (D.N.J. 2001)

evidence was found. In December 2001, the United States FBI confirmed the existence of a similar technique called "Magic Lantern."¹²⁴ This device would reportedly allow the agency to plant a Trojan horse keystroke logger on a target's computer by sending a computer virus over the Internet; rather than require physical access to the computer as is now the case. The new Danish Anti-Terrorism law, enacted in June 2002, appears to give law enforcement the power to secretly install this kind of snooping software on the computers of criminal suspects.¹²⁵

Transactional and Location Data: Surveillance and New Communications Technologies

As new telecommunications technologies emerge, many countries are adapting existing surveillance laws to address the interception of networked and mobile communications. These updated laws pose new threats to privacy in many countries because the governments often simply apply old standards to new technologies without analyzing how the technology has changed the nature and sensitivity of the information. It is crucial for the protection of privacy and human rights that transactional data created by new technologies is given greater protection under law than traditional telephone calling records and other transactional information found in older systems.

In the traditional telephone system, transactional data usually takes the form of telephone numbers or telephone identifiers, the call metrics (e.g. length of call, time and date), countries involved, and types of services used. This data is usually collected and processed by telephone companies for billing and network efficiency (e.g. fault correction) purposes. While this data is stored by telephone companies, it is available to law enforcement authorities. Communications content, i.e. conversations, are not stored routinely. As a result, the obstacles to law enforcement access to this data were minimal: traffic data was available, legally less sensitive, and so accessible with lower authorization and oversight requirements. The content of communications was treated as more sensitive, and more invasive, and more difficult to collect, thus typically requiring greater authorization and oversight mechanisms.

Different communications infrastructures give rise to different forms of transactional data, however. When surfing the net, a user can visit dozens of

¹²⁴ Elinor Mills Abreu, "FBI Confirms 'Magic Lantern' Project Exists," Reuters, December 12, 2001.

¹²⁵ Law No. 378, June 6, 2002.

sites in just a few minutes and reveal a great deal about their personal situation and interests. This can include medical, financial, social interests and other highly personal information. As the Council of Europe acknowledges in the Explanatory Report of the Convention on Cybercrime,

The collection of this data may, in some situations, permit the compilation of a profile of a person's interests, associates and social context. Accordingly Parties should bear such considerations in mind when establishing the appropriate safeguards and legal prerequisites for undertaking such measures.¹²⁶

The detailed and potentially sensitive nature of the data makes it more similar to content of communications than telephone records.

Similarly, location information generated by mobile communications infrastructure, such as mobile phones and mobile IP, is more sensitive than the mere location of a fixed telephony communication. Mobile communications location information can provide details of an individual's movements and activities and whom they have met with. This location information may be combined with other transactional information such as websites visited using the mobile device, individuals called, search engine requests; all used to create a considerable profile. This affects a wide variety of human rights beyond the right of privacy including the rights of free speech and assembly.

Moreover, newer mobile communications protocols are becoming increasingly specific about location data, and the availability of this information is becoming part of the actual communications protocol. That is, the means of identifying the location of a device is becoming more precision-based, and this location information is communicated to a number of parties, not necessarily only between the device and the mobile communications operator. As a result, the location of the device can be more easily discerned, not necessarily requiring access to the data held by the operator.

In addition to this data that naturally arises the functioning of a wireless network, there are other initiatives driving the development of technologies that build in location-tracking capabilities. For example, in the United States, the Federal Communications Commission (FCC) directed wireless telephone service providers to begin implementing Automatic Location Identification (ALI) for emergency (911) calls by October 1, 2001. The ALI "accuracy standards" require

¹²⁶ Council of Europe Convention on Cybercrime (ETS no: 185), opened for signature on November 8, 2001.

providers to develop capabilities that will permit the location of users with the following degrees of precision: for handset-based solutions – 50 meters for 67 percent of calls, 150 meters for 95 percent of calls; for network-based solutions – 100 meters for 67 percent of calls, 300 meters for 95 percent of calls.¹²⁷ Other wireless devices and services increasingly are coming into use, including wireless personal digital assistants (PDAs), wireless Internet access, and automotive navigation and assistance services (telematics), which when combined with Global Positioning Satellite capabilities, can determine the physical locations of users very precisely.

While there is likely to be strong commercial and law enforcement demand for the collection and use of the location data generated by these services, a legal framework to protect privacy specifically with respect to location information has not yet been implemented. In the absence of legal clarity, some operators have been keeping this kind of data indefinitely. In October 2001, British mobile operator Virgin Mobile revealed that it had retained all call records since it was created in 1999. Similarly, in November 2001, it was reported that Irish operators, Eircell and Digifone, were holding customer records for more than six years. In both cases, the operators, stated that they believed they were required to keep these records under the law.¹²⁸

The level of legal protection afforded to other traffic data is similarly unclear. Policies generally treat all of this transactional data as ‘traffic data’; this data then bears the protections afforded under the traditional telephone system. The United Kingdom in its Regulation of Investigatory Powers Act 2000 accepted, after an extensive debate, that there are varying levels of sensitivity to this data, and separates ‘traffic data’ (source and destination of a transaction used for routing within a network) from the more sensitive ‘communications data’ that includes URLs, domain names, etc. The latter requires greater authorization and oversight procedures. Not all countries have pursued this line of reasoning.

Previous United States policy differentiated between traffic data on cable and telephone communications. The Cable Act traditionally protected traffic data to a greater degree than telephone traffic data. Now that cable infrastructure is used for internet communications (which were previously used over telephone lines, and thus traditional laws applied), successive White House administrations worked to erase this distinction, finally succeeding with the USA-PATRIOT Act.

¹²⁷ See generally <<http://www.fcc.gov/e911/>>.

¹²⁸ “Telecom Companies Stored Information for Over Six Years,” BNA World Data Protection Report, Volume 1, Issue 12, December 2001.

Rather than deal with the specifics of digital communications media and services, the changes in United States law reduces the protections of traffic data for all communications to what had previously existed for telephone communications data. This was clearly intended, under the guise of technological neutrality. According to Attorney General Ashcroft:

Agents will be directed to take advantage of new, technologically neutral standards for intelligence gathering. (...) Investigators will be directed to pursue aggressively terrorists on the internet. New authority in the legislation permits the use of devices that capture senders and receivers addresses associated with communications on the Internet.¹²⁹

*Retention of Traffic and Location Data*¹³⁰

On May 30, 2002, the European Parliament voted on the new European Union Telecommunications Privacy Directive.¹³¹ In a remarkable reversal of their original opposition to data retention, the members voted to allow each European Union government to enact laws to retain the traffic and location data of all people using mobile phones, SMS, landline telephones, faxes, e-mails, chatrooms, the Internet, or any other electronic communication devices, to communicate. The new Directive reverses the 1997 Telecommunications Privacy Directive by explicitly allowing European Union countries to compel Internet service providers and telecommunications companies to record, index, and store their subscribers' communications data.¹³² The data that can be retained includes all data generated by the conveyance of communications on an electronic communications network ("traffic data") as well as the data indicating the geographic position of a mobile phone user ("location data").¹³³ The contents of communications are not covered by the data retention measures. These requirements can be implemented for purposes varying from national security to criminal investigations and prevention, and prosecution of criminal offences, all without specific judicial authorization.

¹²⁹ Testimony of the Attorney General to the Senate Committee on the Judiciary, Washington DC, September 25, 2001.

¹³⁰ See EPIC's Data Retention Page <http://www.epic.org/privacy/intl/data_retention.html>.

¹³¹ Directive 2002/75/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (still unpublished). An unofficial consolidated version is available at <http://www.gilc.org/as_voted_2nd_read.html>.

¹³² Article 15(1), id.

¹³³ Article 2(b) and (c), id.

Although this data retention provision is supposed to constitute an exception to the general regime of data protection established by the directive, the ability of governments to compel Internet service providers and telecommunications companies to store all data about all of their subscribers can hardly be construed as an exception to be narrowly interpreted. The practical result is that all users of new communications technologies are now considered worthy of scrutiny and surveillance in a generalized and preventive fashion for periods of time that States' legislatures or governments have the discretion to determine. Furthermore, because of the cross-border nature of Internet communications, this Directive is likely to have negative repercussions for citizens of other countries. There is a significant risk that non-European Union law enforcement agencies will seek data held in Europe that it can not obtain at home, either because it was not retained or because their national law would not permit this kind of access.

During the debates on the Directive, many members of the European Parliament, and the European Union privacy commissioners consistently opposed data retention, arguing that, these policies are in contravention of data protection practices of deletion of data once it is no longer required for the purpose for which it was collected; and also in contravention of proportionality principles in accordance with constitutional laws and jurisprudence. Similarly, the Global Internet Liberty Campaign, a coalition of 60 civil liberties groups organized a campaign and drafted an open letter to oppose data retention. The letter was sent to all European Parliament members and heads of European Union institutions after more than 16,000 individuals from 73 countries endorsed it in less than a week.¹³⁴ The letter asserted that data retention (for reasons other than billing purposes) is contrary to well-established international human rights conventions and case law.

While a few other countries have already established data retention schemes (Belgium, France, Spain and the United Kingdom) the implementation phase of the Directive's data retention provision may be bumpy in other Member States. The Directive may be seen as being in conflict with the constitutions of some European Union countries, with respect to fundamental rights such as the presumption of innocence, the right to privacy, the secrecy of communications, or freedom of expression.¹³⁵

¹³⁴ Open Letter to Mr. Pat Cox, President, European Parliament, from the Global Internet Liberty Campaign, May 2002, at <http://gilec.org/cox_en.html>.

¹³⁵ This is the case in Spain where the recent law allowing data retention for a year has been challenged as being in direct opposition to the Spanish Constitution. For more details see <<http://www.kriptopolis.com/net/tc.php>>.

'Cybercrime': International Initiatives in Harmonizing Surveillance

A related effort for enhancing government control of the Internet and promoting surveillance is also being conducted in the name of preventing “cyber-crime,” “information warfare” or protecting “critical infrastructures.” Under these efforts, proposals to increase surveillance of the communications and activities of Internet users are being introduced as a way to prevent computer intruders from attacking systems and to stop other crimes such as intellectual property violations.

The lead bodies internationally are the Council of Europe and the G-8, while there has also been some activity within the European Union.¹³⁶ The United States has been active behind the scenes in developing and promoting these efforts.¹³⁷ After meeting behind closed doors for years, these organizations finally, in 2000, made public proposals that would place restrictions on online privacy and anonymity in the name of preventing cyber-crime.

Council of Europe

The Council of Europe is an intergovernmental organization formed in 1949 by West European countries. There are now 43 member countries. Its main role is “to strengthen democracy, human rights and the rule of law throughout its member states.” Its description also notes that “it acts as a forum for examining a whole range of social problems, such as social exclusion, intolerance, the integration of migrants, the threat to private life posed by new technology, bioethical issues, terrorism, drug trafficking and criminal activities.”

On September 8, 1995, the Council of Europe approved a recommendation to enhance law enforcement access to computers in member states. The Recommendation of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information states:

Subject to legal privileges or protection, investigating authorities should have the power to order persons who have data in a computer system under their control to provide all necessary information to enable access to a computer system and the data therein. Criminal procedure law should ensure that a similar order can be given to other persons who have

¹³⁶ Dr Paul Norman, “Policing 'high tech crime' in the global context: the role of transnational policy networks,” available at <<http://www.bileta.ac.uk/99papers/norman.htm>>.

¹³⁷ For details see <<http://www.privacyinternational.org/issues/cybercrime/>>.

knowledge about the functioning of the computer system or measures applied to secure the data therein.

Specific obligations should be imposed on operators of public and private networks that offer telecommunications services to the public to avail themselves of all necessary technical measures that enable the interception of telecommunications by the investigating authorities.

Measures should be considered to minimize the negative effects of the use of cryptography on the investigation of criminal offenses, without affecting its legitimate use more than is strictly necessary.

In 1997, the Council of Europe formed a Committee of Experts on Crime in Cyber-space (PC-CY). The group met in secret for several years drafting an international treaty and in April 2000, released the “Draft Convention on Cyber-crime, version 19.” A number of subsequent versions were released until version 27 was released in June 2001.

The convention has three parts. Part I proposes the criminalization of on-line activities such as data and system interference, the circumvention of copyright, the distribution of child pornography, and computer fraud. Part II requires ratifying states to pass laws to increase their domestic surveillance capabilities to cater for new technologies. This includes the power to intercept internet communications, gain access to traffic data in real-time or through preservation orders to ISPs, and access to secured or “protected” data. The final part of the treaty requires all states to cooperate in criminal investigations. So, for example, country A can request country B to utilize any of the aforementioned investigative powers within country B for a crime that is being investigated in country A. There is no requirement for the crime in country A to actually qualify as a crime in country B, i.e. no requirement for dual-criminality. In this sense, the convention is the largest mutual legal assistance regime in criminal matters ever created.

The draft convention text was strongly criticized by a wide variety of interested parties including privacy and civil liberties groups for its promotion of surveillance and lack of controls such as authorization requirements and dual criminality;¹³⁸ prominent security experts for previously articulated limitations

¹³⁸ See, for example, Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime, October 18, 2000 at <<http://www.gilc.org/privacy/coe-letter-1000.html>>; and Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime Version 24.2, December 12, 2000 at <<http://www.gilc.org/privacy/coe-letter-1200.html>>.

on security software;¹³⁹ and industry for the costs of implementing the requirements, and the challenges involved in responding to requests from 43 different countries. The European Union's Data Protection Working Group has expressed concern regarding the convention's implications upon privacy and human rights, concluding that:

The Working Party therefore sees a need for clarification of the text of the articles of the draft convention because their wording is often too vague and confusing and may not qualify as a sufficient basis for relevant laws and mandatory measures that are intended to lawfully limit fundamental rights and freedoms.¹⁴⁰

The convention text was finalized in September 2001. After the terrorist attacks on the United States, the convention was positioned as a means of combating terrorism. A signing ceremony took place in November where it was signed by thirty countries, and later signed by another four. Only one country, Albania, has ratified the convention at the time of publication of this report. The Convention is open to the members of the Council of Europe and to countries that were involved in the development, which includes the United States, Canada, Japan and South Africa. All members of the latter group have signed on.

The convention will come in to force once ratified by five signatory states, of which three must be members of the Council of Europe. Once it is in force, other non-COE countries like China and Singapore can also ask to join. The Australian government announced in July 2001 that its bill on computer crime, which requires users to provide encryption keys, is based on the Convention.¹⁴¹

A draft protocol on Racism and Xenophobia is currently under consideration. This protocol apparently will require the criminalization of certain forms of Internet speech that some might find offensive.¹⁴² There was some discussion of a second protocol on "terrorist messages and the decoding thereof," however discussion on this matter has not advanced publicly.¹⁴³

¹³⁹ Statement of Concerns, July 20, 2000. <<http://www.cerias.purdue.edu/homes/spaf/coe/index.html>>.

¹⁴⁰ European Union Article 29 Data Protection Working Group, Opinion 4/2001 On the Council of Europe's Draft Convention on Cyber-crime, March 22, 2001

¹⁴¹ Cybercrime Bill 2001 Second Reading Speech by the Attorney General, The Parliament of the Commonwealth of Australia.

¹⁴² See, e.g., Global Internet Liberty Campaign, Member Letter to Council of Europe Secretary-General Walter Schwimmer, February 6, 2002, <http://www.gilc.org/speech/coe_hatespeech_letter.html>.

¹⁴³ See, e.g., Global Internet Liberty Campaign, Member Letter to Council of Europe Secretary-General Walter Schwimmer, February 28, 2002, <http://www.gilc.org/speech/coe_hatespeech_2.html>.

G-8

The Group of 8 (G-8) is made up of the heads of state of eight industrialized countries in the world (Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States. The European Commission participates as an observer). The leaders have been meeting annually since 1975 to discuss issues of importance, including economics and finance, transnational organized crime, terrorism, and the information society.

Since 1995, the G-8 has become increasingly more involved in the issue of high-tech crime, and has created working groups and issued a series of communiqués from the leaders and action plans from justice ministers. Much of this work has been coordinated by the Lyon Group, established formally in 1997.

At the Birmingham, England summit in May 1998, the G-8 adopted a recommendation on ten principles and a ten-point action plan on high-tech crime. The ministers announced:

We call for close cooperation with industry to reach agreement on a legal framework for obtaining, presenting and preserving electronic data as evidence, while maintaining appropriate privacy protection, and agreements on sharing evidence of those crimes with international partners. This will help us combat a wide range of crime, including abuse of the Internet and other new technologies.

The G-8 has met several times with industry and is actively promoting requirements that Internet Service Providers maintain records of all of their users' activities in case there is a future need to investigate a crime that might have occurred. These requirements were strongly criticized at a meeting held by the G-8 in Japan in 2001 where industry and a civil liberties group were invited and a draft press release and guidelines that promoted data retention had to be withdrawn after they had already been made public.

The G-8 has continued its activity in the area of law enforcement and combating terrorism, however. Throughout 2002 a number of summits involving Finance Ministers, Justice and Interior Ministers, and heads of state have released a number of statements regarding increased surveillance, traceability of

communications,¹⁴⁴ and data retention.¹⁴⁵ Increased cooperation across borders was discussed at length; and as with the Council of Europe convention, no requirements of dual-criminality or double-criminality are necessary.

The European Union

In July 2000, the Commission announced plans for a new directive for fighting cyber-crime.¹⁴⁶ A communication was released in January 2001.¹⁴⁷ While similar to the Council of Europe convention in many ways, the Commission's proposal also included proposals regarding data retention and the reduction of anonymity. These policies were sought within "public forums" (only with limited invited speaking slots) in the fall of 2001, with unclear and unpublished results.

The retention proposal was sought in the alternative forum of the electronic services data protection directive in the European Parliament. The substantive law measures of criminalizing data and systems interference and defining other such offences are being pursued as a Council Framework Decision, currently in draft mode.¹⁴⁸ This initiative is designed to be consistent with the Council of Europe and G-8 activities.

The Organisation for Economic Co-Operation and Development (OECD)

In contrast to many of these law enforcement-driven initiatives, the Organisation for Economic Co-Operation and Development (OECD) has tended to take a broader view of security issues. In 1992, the OECD issued Guidelines for the Security of Information Systems.¹⁴⁹ Containing nine principles, the Guidelines stress the importance of ensuring transparency, proportionality and other democratic values when establishing measures, practices and procedures for the security of information systems. In the fall of 2001, the OECD Working Party on

¹⁴⁴ Recommendations for Tracing Networked Communications Across National Borders in Terrorist and Criminal Investigations, published at the G8 Justice and Interior Ministers' Meeting in Mont-Tremblant, Quebec, May 2002.

¹⁴⁵ Principles on the Availability of Data Essential to Protecting Public Safety, published at the G8 Justice and Interior Ministers' Meeting in Mont-Tremblant, Quebec, May 2002.

¹⁴⁶ "European Union Ministers Vow Cyber Crime Crackdown," Reuters, July 29, 2000.

¹⁴⁷ Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM(2000) 890 final, January 26, 2001, available at <<http://www.privacyinternational.org/issues/cybercrime/eu/>>.

¹⁴⁸ Commission Proposal for a Council Framework Decision on Attacks against Information Systems (COM (2002) 173 final), April 19, 2002.

¹⁴⁹ OECD Guidelines for the Security of Information Systems, adopted November 1992, available at <<http://www.oecd.org/EN/document/0,,EN-document-29-nodirectorate-no-24-10249-29,00.html>>

Information Security and Privacy (WPISP) established a group of experts to conduct a review of these guidelines (such a review must take place every five years). The group of experts met four times between December 2001 and June 2002 and recommended a number of changes. The OECD is expected to formally release the revised guidelines in the fall of 2002. Although the guidelines have been substantially revised, the need to ensure key democratic values, such as openness, transparency and the protection of personal information, is nonetheless reiterated in the principles.

National Security, Intelligence Agencies and the “Echelon system”

In the past several years, there has been considerable attention given to mass surveillance by intelligence agencies of international and national communications. Investigations have been opened and hearings held in parliaments around the world about the “Echelon” system coordinated by the United States.

Immediately following the Second World War, in 1947, the governments of the United States, the United Kingdom, Canada, Australia and New Zealand signed a National Security pact known as the “Quadripartite,” or “United Kingdom - United States” (UKUSA) agreement. Its intention was to seal an intelligence bond in which a common national security objective was created. Under the terms of the agreement, the five nations carved up the earth into five spheres of influence, and each country was assigned particular signals intelligence (SIGINT) targets.

The UKUSA Agreement standardized terminology, code words, intercept handling procedures, arrangements for cooperation, sharing of information, Sensitive Compartmented Information (SCI) clearances, and access to facilities. One important component of the agreement was the exchange of data and personnel.

The strongest alliance within the UKUSA relationship is the one between the United States National Security Agency (NSA), and Britain’s Government Communications Headquarters (GCHQ). The NSA operates under a 1952 presidential mandate, National Security Council Intelligence Directive (NSCID) Number 6, to eavesdrop on the world’s communications networks for intelligence and military purposes. In doing so, it has built a vast spying operation that can reach into the telecommunications systems of every country on earth. Its operations are so secret that this activity, outside the United States,

occurs with little or no legislative or judicial oversight. The most important facility in the alliance is Menwith Hill, a Royal Air Force base in the north of England. With over two dozen domes and a vast computer operations facility, the base has the capacity to eavesdrop on vast chunks of the communications spectrum. With the creation of Intelsat and digital telecommunications, Menwith Hill and other stations developed the capability to eavesdrop on an extensive scale on satellite-borne fax, telex and voice messages.

The current debate over NSA activities has focused on the existence of a signals intelligence system known as "Echelon." United States officials have refused to confirm the existence of this or any other surveillance systems. In May 2001, the European Parliament's Temporary Committee on the Echelon Interception System (established in July 2000) issued a report concluding that "the existence of a global system for intercepting communications . . . is no longer in doubt."¹⁵⁰ According to the committee, the Echelon system (reportedly run by the United States in cooperation with Britain, Canada, Australia and New Zealand) was set up at the beginning of the Cold War for intelligence gathering and has developed into a network of intercept stations around the world. Its primary purpose, according to the report, is to intercept private and commercial communications, not military intelligence.

The report recommended "self-protection" by EU citizens and companies, and encouraged further development and use of encryption technology within Europe to protect communications against surveillance. The report also recommended actions to be taken by the European Parliament during its September 2001 session in Strasbourg. These included provisions for the United States to (1) Negotiate and sign an agreement with European Union (European Union) requiring both parties to "observe, vis-à-vis the other, the provisions governing the protection of the privacy of citizens and the confidentiality of business communications applicable to its own citizens and firms;" (2) Sign the international covenant on civil and political rights so complaints by individuals could be submitted to Human Rights Committee created by the covenant; (3) Negotiate with member states code of conduct akin to that of European Union; and (4) Begin a dialog with the European Union on economic intelligence gathering. (On this point the Committee did not find widespread evidence of Echelon being used primarily for economic intelligence gathering). The Committee also recommended that Germany and United Kingdom condition

¹⁵⁰ European Parliament, Temporary Committee on the Echelon Interception System, Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON interception system) (2001/2098(INI)), May 18, 2001 (adopted July 11, 2001), available at <http://www.europarl.eu.int/tempcom/echelon/pdf/prechelon_en.pdf>.

further authorization of United States communications interception operations within their territories on United States compliance with European Convention on Human Rights. No further action on these recommendations has been taken.

Prior to issuing its report, the Temporary Committee traveled to Washington DC to meet with senior Bush administration government and intelligence officials to discuss Echelon. When they arrived, however, their meetings with these officials at the Departments of State, Commerce and Defence, the CIA and the NSA were cancelled at the last minute. The European Parliament subsequently issued a Resolution protesting this move.¹⁵¹

The work of the recent Temporary Committee was based on two earlier reports of the European Parliament. The first, "An Appraisal of the Technologies of Political Control,"¹⁵² was published in 1997 and stated that the NSA had established an integrated communications surveillance capability in Europe. It described Echelon as a communications intelligence sharing sub-system capable of scanning particular communications to detect information of interest. In 1999, the second European Parliament report, "Interception Capabilities 2000" set out the technical specifications of the interception system.¹⁵³ The report described the merger of Echelon and the International Law Enforcement Telecommunications Seminar (ILETS) stating that in time, the two vast systems - one designed for national security and one for law enforcement - would merge, and in the process will compromise national control over surveillance activities.

These recent events have left observers contemplating two profound conclusions. First, as long as the UK-USA SIGINT partners police and govern their own operations outside of actual effective parliamentary and judicial oversight, there is good reason to believe that SIGINT can be turned against individuals and groups exercising civil and political rights. There is ample evidence that the activities of Greenpeace, Christian Aid, Amnesty International, the International Committee to Ban Landmines, the Tibetan government-in-exile, various anti-globalization movements like the Independent Media Center, and the International Committee of the Red Cross have been targeted by UKUSA agencies. Second, there is an increasing blurring between the activities of

¹⁵¹ Steve Kettmann, "U.S. Echelon Snub Angers Europe," Wired News, May 18, 2001, available at <<http://www.wired.com/news/privacy/0,1848,43921,00.html>>

¹⁵² Published by STOA (Science and Technology Options Assessment). Reference Project No. IV/STOA/RSCH/LP/politicon.1

¹⁵³ Report to the Director General for Research of the European Parliament (Scientific and Technical Options Assessment programme office) on the development of surveillance technology and risk of abuse of economic information, available at <<http://jya.com/echelon-dc.htm>>.

intelligence agencies and law enforcement. The creation of a seamless international intelligence and law enforcement surveillance system has resulted in the potential for a huge international network that may, in practice, negate current rules and regulations prohibiting domestic communications surveillance by national intelligence agencies.

Audio Bugging

Advances in technology are also making it easier and cheaper to conduct covert audio surveillance. Bugs come in many shapes and sizes. They range from micro engineered transmitters the size of an office staple, to devices no bigger than a cigarette packet that are capable of transmitting video and sound signals for miles. Many of the bugs are cleverly camouflaged. They are hidden in everything from umbrella stands to light shades. Sometimes, the infiltrator will hide them in a business or sports trophy where they will stay indefinitely. The latest bugs remain active with their own power supply for around ten years.

Laws restricting the use of covert audio devices vary widely across the world. Many countries have provisions in their general wiretap laws that also cover the use of bugs. The European Court of Human Rights has ruled several times that all signatories of the Convention must enact laws governing their use. While it is illegal in most circumstances in the United States to use or sell such devices, the British market had no restrictions whatever until recently. As one private investigator told the London Daily Telegraph, "It's a game anyone can play." Millions of bugs are sold every year in Asian countries such as Hong Kong and Japan.

The devices are used for a variety of reasons. In many Asian countries, use of the devices for industrial espionage is widespread. They are also frequently used in the workplace or in homes. Law enforcement and intelligence agencies also use the devices but according to government records in the United States, Canada and other countries, they are used much less frequently than traditional wiretaps for law enforcement purposes.

Video Surveillance

Surveillance cameras (also called Closed Circuit Television or CCTV) are increasingly being used to monitor public and private spaces throughout the world. The leader is the United Kingdom, where between 150 and 300 million

pounds per year is spent on expanding a surveillance industry that has an estimated 1.5 million cameras watching public spaces.¹⁵⁴ Many Central Business Districts in Britain are now covered by surveillance camera systems involving a linked system of cameras with full pan, tilt, zoom and night vision or infrared capability. CCTV systems are also in wide use in several other European countries where they are closely regulated. Surveillance of public spaces has grown markedly in the United States and Australia. In New York City, the NYCLU Surveillance Camera Project identified 2,397 cameras in Manhattan.¹⁵⁵ The Mayor of Washington, D.C. has proposed a "London style" blanket surveillance of public areas to cover the several public protests that takes place in the capital.¹⁵⁶ In Singapore, cameras are widely deployed for traffic enforcement and to prevent littering. Several governments are now considering using surveillance systems as an anti-terrorism tool. Some observers believe the surveillance camera phenomenon is dramatically changing the nature of cities. The technology has been described as the "fifth utility," where CCTV is being integrated into the urban environment in much the same way as the electricity supply and the telephone network in the first half of the century.¹⁵⁷

The camera system is designed to serve as a deterrent to crime and for evidence gathering purposes. Generally these systems have been rolled out with little prior research into the effectiveness or appropriateness of the technology, as in most cases the deployment is driven by a public relations need to create the impression of heightened security.¹⁵⁸ The evidence supporting the effectiveness of the camera system has been inconclusive. A new study announced in June 2002 found that in many areas with CCTV that crime increased and that street lighting was a more effective deterrent.¹⁵⁹ In March 2002, a report issued by researchers at the University of Hull, United Kingdom found that cameras do not have a major impact on most criminal activity, and even where they appear to have an effect it is because that crime is often just displaced elsewhere.¹⁶⁰ Recent studies

¹⁵⁴ Jeffery Rosen, "A Cautionary Tale for a New Age of Surveillance," *New York Times Magazine*, October 7, 2001.

¹⁵⁵ NYCLU Surveillance Camera Project <<http://www.nyclu.org/surveillance.html>>. See also, *New York Surveillance Camera Players* <<http://www.notbored.org/the-scp.html>>.

¹⁵⁶ "Eyes in the Sky: DC Police Are Building a Network of Cameras To Keep Tabs on the Public," *Wall Street Journal Classroom Edition*, April 2002

¹⁵⁷ Stephen Graham, *The Fifty Utility*, Index on Censorship, Issue 3, 2000, available at <<http://www.indexoncensorship.org/300/gra.htm>>.

¹⁵⁸ See Michael McCahill & Clive Norris, "Literature Review," *Urbaneye Working Paper No. 2*, March 2002, available at <<http://www.urbaneye.net>>.

¹⁵⁹ "CCTV not a crime prevention cure-all, says report," *NACRO*, June 28 2002, available at <<http://www.nacro.org.uk/templates/news/newsItem.cfm/2002062800.htm>>.

¹⁶⁰ Michael McCahill and Clive Norris "CCTV in Britain," *Working Paper No. 3*, *Urbaneye Project*, Centre for Criminology and Criminal Justice, University of Hull, March 2002, available at <<http://www.urbaneye.net>>.

conducted by the Scottish Center for Criminology have yielded similar results.¹⁶¹ Questions are now surfacing about the use of cameras in Australia.¹⁶²

As surveillance systems appear poised to become a part of the urban landscape, scholars, data protection commissioners, legislators, and the public are beginning to grapple with the implications of this new technology.¹⁶³ In July 2000, the United Kingdom Data Protection Commissioner issued a code of practice on the use of CCTV. The code sets out guidelines for the operators of CCTV systems and makes clear their obligations under the recently implemented Data Protection Act 1998.¹⁶⁴ Also in 2000 the Greek Data Protection Commissioner issued a directive prohibiting the use of CCTV except in certain circumstances.¹⁶⁵ In Sweden, the 1998 Law on Secret Camera Surveillance restricts the use of video surveillance. Norway's Personal Data Registers Act of 2000 also provides specific rules for video surveillance. Canada's privacy commissioner has been very active in limiting surveillance cameras and has recently launched a lawsuit against the Royal Canadian Mountain Police, calling their use of the system an unconstitutional breach of privacy.¹⁶⁶ Washington, D.C. is considering regulations that will subject video surveillance to the same restrictions that are imposed on electronic surveillance, including requiring judicial and public oversight over the system's operation. Campaigns have begun in several countries to stop the spread of surveillance camera systems.¹⁶⁷ For the past four years, an international coalition composed of artists, scientists, engineers, scholars, and others have declared December 24 to be "World Sousveillance" day, and have staged several public protests to draw attention to the use of surveillance cameras.¹⁶⁸

¹⁶¹ The Scottish Centre for Criminology, Crime Prevention Publications, available at <<http://www.scotcrim.u-net.com/researchc.htm>>; and, Al Webb, "'Spy' Cameras vs Villains in Britain," UPI. March 8, 2002

¹⁶² Bruce Andrews. "Here's Looking at You", Australian Center for Independent Journalism, April 2002 <http://www.reportage.uts.edu.au/stories/2002/social/cctv_24042002.html>

¹⁶³ See "On the Threshold to Urban Panopticon? Analysing the Employment of CCTV in European Cities and Assessing its Social and Political Impacts," a four year European Commission funded project, available at <<http://www.urbaneye.net>>.

¹⁶⁴ United Kingdom Data Protection Commission, CCTV Code of Practice, July 2000, available at <<http://www.dataprotection.gov.uk/dpr/dpdoc.nsf/ed1e7ff5aa6def30802566360045bf4d/db76232b37b5bb648025691900413c9d?OpenDocument>>.

¹⁶⁵ Hellenic Republic Data Protection Authority, Directive On Closed Circuit Television Systems, September 29, 2000.

¹⁶⁶ Charles Mandel, "Security Cams not OK in Canada?" Wired News. April 16, 2002 <<http://www.wired.com/news/politics/0,1283,51821,00.html>>.

¹⁶⁷ See generally Privacy International, CCTV Pages, <<http://www.privacyinternational.org/issues/cctv/index.html>>; "Watching Them, Watching Us," United Kingdom CCTV Surveillance Regulation Campaign, <<http://www.spy.org.uk/>>; EPIC, Observing Surveillance Project, <<http://www.epic.org/privacy/surveillance>>.

¹⁶⁸ World Sousveillance Day <<http://wearcam.org/wsd.htm>>.

The debate over the appropriateness of surveillance technology is likely to become sharper as the technology becomes increasingly sophisticated. New systems can digitally record images, which facilitate easy archiving, recovery, and sharing of information. Features include night vision, computer-assisted operation, and motion detection facilities that help improve the operator's attentiveness by sounding an alert if suspicious activity is taking place. The clarity of the pictures is usually excellent, with many systems being able to read a newspaper at a hundred meters. Technology is also being developed to spot patterns in the surveillance data such as recognizing faces, analyzing crowd behavior, and scanning the intimate area between skin surface and clothes using "passive millimeter wave technology" to search for contraband or weapons.¹⁶⁹ Research into these technologies is receiving significant government funding for crime fighting and anti-terrorism purposes.¹⁷⁰

Face Recognition

Face recognition technology utilizes computerized pattern matching technology to automatically identify peoples' faces. While it is still very much in its infancy, it raises significant public policy questions because it enables the covert identification and classification of people in public. The borough of Newham in the United Kingdom first deployed a face recognition system to scan faces against a database to identify people "of interest." The Reykjavik airport in Iceland was among the first airports to use the technology. In the United States, this same kind of face recognition technology was used at the 2001 Super Bowl in Tampa, Florida to compare the faces of attendees to faces in a database of mug shots. There was widespread public outcry, prompting some to call the event the "Snooper Bowl."¹⁷¹

Face recognition technology is still not reliable. For instance, it was not accurate enough for use in the Salt Lake Winter Olympic games where the security chief said that "it's just not proven technology yet."¹⁷² Studies sponsored by the United States Defense Department have also shown the system is right only 54% of the time and can be significantly compromised by changes in lighting, weight, hair,

¹⁶⁹ Ivan Amato. "Beyond X-ray Vision: Can Big Brother see right through your clothes?" Discover Volume 23 No. 7 (July 2002) <http://www.discover.com/july_02/feattechapterhtml>

¹⁷⁰ See United States Defense Department's Human ID at a Distance Project <<http://www.darpa.mil/iao/HID.htm>>

¹⁷¹ For more information, see EPIC's Face Recognition page <<http://www.epic.org/privacy/facerecognition/>>.

¹⁷² "Games Notebook," The Ottawa Citizen, February 10, 2002.

sunglasses, subject cooperation, and other factors.¹⁷³ Tests on the face recognition systems in operation at Palm Beach Airport in Florida,¹⁷⁴ and Boston Logan Airport have also shown the technology to be ineffective and error-ridden.¹⁷⁵

As the power and capabilities of surveillance technology increases while the cost and size of systems decreases, there will be further incentives to use the technology. Critics see this trend as a reason to develop appropriate regulations to safeguard privacy and to prevent the misuse of the technology.¹⁷⁶

Satellite Surveillance

Developments in satellite surveillance (also called “remote sensing”) are also occurring at a fast pace, and embrace features similar to those of more conventional visual surveillance. Satellite resolution has constantly improved over the past decade. Since the end of the Cold War, companies such as EarthWatch, Motorola and Boeing have invested billions of dollars to create satellites capable of mapping the most minute detail on the face of the earth.

A commercial satellite capable of recognizing objects the size of a student’s desk was launched from the United States in September 1999 and began releasing images in October 2000.¹⁷⁷ The Ikonos is most powerful commercial imaging satellite ever built. Its parabolic lens can recognize objects as small as one meter anywhere on earth and the according to the company, viewers can see individual trees, automobiles, road networks, and houses. The satellite, owned by Denver company Space Imaging, will be the first of a new generation of high resolution satellites using technology formerly restricted to government security agencies. Another ten companies have received licenses to launch equally powerful satellites and several are expected to launch shortly.

¹⁷³ Declan McCullagh and Robert Zarate, “Scanning Tech a Blurry Picture”, Wired News, February 16, 2002, available at <<http://www.wired.com/news/print/0,1294,50470,00.html>>.

¹⁷⁴ American Civil Liberties Union Press Release, “Data on Face-Recognition Test at Palm Beach Airport Further Demonstrates Systems’ Fatal Flaws,” May 14, 2002, available at <<http://www.aclu.org/news/2002/n051402b.html>>.

¹⁷⁵ Hiawatha Bray, “‘Face Testing’ at Logan is Found Lacking,” Boston Globe, July 17, 2002, available at <http://www.boston.com/dailyglobe2/198/metro/_Face_testing_at_Logan_is_found_lacking+.shtml>.

¹⁷⁶ See Testimony of Marc Rotenberg before D.C. City Council, June 2002 <http://www.epic.org/privacy/surveillance/testimony_061302.html>

¹⁷⁷ See <<http://www.spaceimaging.com/>>.

The technology is already being used for a vast range of purposes from media reporting of war and natural disasters, to detecting unlicensed building work and even illegal swimming pools. Public interest groups are using the information to show images of nuclear testing by countries and even images of secret United States bases such as Area 51 in Nevada.¹⁷⁸

While industry looks for the opportunity to exploit current spy satellite technology, a great deal of effort is being made to integrate the existing images with ground-based Geographic Information System (GIS) databases than can provide detailed data on human activity. Double clicking on a satellite image of an urban area can reveal precise details of the occupants of a target house. The “Open Skies” policy accepted worldwide means that there are few restrictions of the use of the technology.¹⁷⁹

But the companies have a distance to go before they catch up with governments. It is estimated that the current generation of secret spy satellites such as the Ikon/Keyhole-12 can recognize objects as small as 10cm across and some analysts say that it can image a license plate.¹⁸⁰ Boeing recently landed a 10-year contract from the United States Government for a Future Imagery Architecture (FIA) to replace the KH satellites and the ground infrastructure.¹⁸¹ The FIA is based on a constellation of new satellites that are smaller, less expensive, and placed in orbit to allow for real-time surveillance of battlefields and other targets.

Electronic Commerce

Surveillance by law enforcement is not the only concern users should have about their online privacy. The growth of the Internet and electronic commerce has dramatically increased the amount of personal information that is collected about individuals by corporations. As consumers engage in routine online transactions, they leave behind a trail of personal details, often without any idea that they are doing so. Much of this information is routinely captured in computer logs.

Most on-line companies keep track of users’ purchases. This information ranges from the trivial to the most sensitive and, unless adequately protected, can be

¹⁷⁸ See e.g. Federation of American Scientists, Dimona Photographic Interpretation Report, available at <http://www.fas.org/nuke/guide/israel/facility/dimona_pir.html>.

¹⁷⁹ Id.

¹⁸⁰ “Spy Satellites: the Next Leap Forward,” *International Defense Review*, January 1, 1997.

¹⁸¹ “Boeing to build new United States satellites,” *Jane's Defense Weekly*, September 15, 1999.

used for purposes that seriously harm the interests of the consumer. Other companies gather personal information from visitors by offering personalized services such as news searches, free email and stock portfolios. They then sell, trade or share that information among third party companies without the consumer's expressed knowledge or consent. The perceived value of this kind of information is behind the stock-market valuations of many dotcom companies.

Spam

Many on-line companies, for example, provide lists of their customers' e-mail addresses to companies that specialize in sending unsolicited commercial e-mail (spam). Other companies mine e-mail address from sources such as messages posted on mailing lists, from newsgroups, or from domain name registration data. This results in consumers being barraged by advertisements and "once-off" deals by companies or people they have never even heard of. Studies show that consumers resent spam both for the time it takes to process and for the loss of privacy resulting from their e-mail address circulating freely on countless directories.¹⁸² Furthermore, spam can result in significant economic loss to the consumer. A 2001 report by the European Commission found that "Internet subscribers worldwide are unwittingly paying an estimated 10 billion euros (\$9.36 billion USD) a year in connection costs just to receive 'junk' e-mails."¹⁸³ The Commission's recently passed Electronic Communications Privacy Directive prohibits unsolicited commercial marketing by e-mail without "opt-in" consent.¹⁸⁴ In Japan two new anti-spam laws were passed in 2002. The laws allow users of the Internet and text-enabled mobile phones to opt-out of spammers' contact lists, and require that all unsolicited commercial e-mail be clearly identified.¹⁸⁵

Profiling

Probably even more worrying is the increasing practice of "online profiling" Internet users. Companies, including Internet Service Providers, web site hosts

¹⁸² For more information on SPAM generally and how to reduce it see <<http://www.junkbusters.com>> and <<http://www.cauce.org/>>.

¹⁸³ European Commission, Unsolicited Commercial Communications and Data Protection, January 2001 available at <http://europa.eu.int/comm/internal_market/en/dataprot/studies/spam.htm>.

¹⁸⁴ 2439th Council meeting, Luxembourg, June 25, 2002. Transcripts of proceedings available at <http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=PRES/02/1800|AGED&lg=EN>.

¹⁸⁵ Toru Takahashi, "2 new laws aimed at cutting spam," Daily Yomiuri (Japan), July 2, 2002 <<http://www.yomiuri.co.jp/newse/20020702wo32.htm>>.

and others, monitor users as they travel across the Internet, collecting information on what sites they visit, the time and length of these visits, search terms they enter, purchases they make or even “click-through” responses to banner ads. In the off-line world this would be comparable to, for example, having someone follow you through a shopping mall, scanning each page of every magazine you browse though, every pair of shoes that you looked at and every menu entry you read at the restaurant. When collected and combined with other data such as demographic or “psychographic” data, these diffuse pieces of information create highly detailed profiles of net users. These profiles have become a major currency in electronic commerce where they are used by advertisers and marketers to predict a user’s preferences, interests, needs and possible future purchases. Most of these profiles are currently stored in anonymous form. However, there is a distinct likelihood that they will soon be linked with information, such as names and addresses, gathered from other sources, making them personally identifiable.

The most pervasive tracking technology is the cookie. The cookie is a small file containing an ID number that is placed on a user’s hard drive by a website. Cookies were developed to improve websites’ ability to track users over a session. The cookie can also notify the site that the user has returned and can allow the site to track the user’s activities across many different visits. The use of cookies expanded greatly when it was realized that a single cookie could be used across many different sites. This led to the development of advertising network companies that can track users across thousands of sites. The largest ad service, DoubleClick, has agreements with over 11,000 websites and maintains cookies on 100 million users; each linking to hundreds of pieces of information about the user’s browsing habits. It is possible to configure the common browsers to reject or send a warning notice before cookies are set. This does not provide much protection, however, as websites will often refuse access to users who do not accept cookies or send out so many repeated attempts that the user accepts the cookie in order to get uninterrupted access.

A more secretive manner of monitoring online users takes place through the use of web bugs. Web bugs are invisible graphics that are placed on Web sites or in emails in order track visitors to that Web site or the recipients of emails (often spam). A Web bug on a Web site collects information such as the IP address of the visiting computer, the browser being used, the time of the ‘hit’, and also a previously set cookie value. In an email a Web bug is used to discover if and when the email message was read, how many times it was forwarded, and the IP address of the recipient. A marketing email directing users to Web sites can also

be used to link the email addresses of those that later visit the site to their cookie data. Web bugs can also be used in newsgroup messages to track readers.¹⁸⁶

In the offline world, profiling has been thriving for decades.¹⁸⁷ Profiling companies build personally-identifiable databases based a plethora of sources including supermarket purchases, product warranty cards, public records, census records, magazine and catalog subscriptions, and surveys. This is done in the absence of legislation to prevent dossier building. Companies also "enhance" dossiers that they already own by combining or "overlying" information from other databases. These dossiers may link individual's identities to any number of facts deemed private by advanced societies including medical conditions, physical characteristics, and lifestyle preferences.

The line between online and offline profiling has become more and more blurred. In 1999, DoubleClick announced that it was buying Abacus, owner of the largest direct marketing lists in the country, with information on the purchasing habits of 90 percent of all United States households, and that DoubleClick was going to merge information from the purchasing databases with information from online browsing. Following a public outcry, the company suspended its plan to merge personal data with profiles. However, in July 2000 the Federal Trade Commission reached an agreement with the Network Advertisers Initiative, a group consisting of the largest online advertisers including DoubleClick, which will allow for online profiling and any future merger of such databases to occur with only "opt-out" consent.¹⁸⁸

Another important player in this move towards complete identification of Internet users is the Microsoft Corporation. In 2001 Microsoft began aggressively promoting the Passport and Hailstorm services in preparation for the launch of Microsoft XP, the newest version of the Windows operating system. Passport is an online identification and authentication system, which employs a single sign-on system to facilitate e-commerce and browsing among different web sites that require a user to identify oneself. Once a user signs on to Passport, other affiliated sites visited by the user receive information about the user. Passport stores user information in a central database. The Passport service is intended to give Microsoft and Passport affiliates the ability to send unsolicited commercial email to Internet users and to profile their activities. To register for Passport, a

¹⁸⁶ For more information on Web bugs visit the Privacy Foundation <<http://www.privacyfoundation.net/resources/webbug.asp>>.

¹⁸⁷ See EPIC's Profiling page <<http://www.epic.org/privacy/profiling/>>.

¹⁸⁸ Electronic Privacy Information Center (EPIC) and Junkbusters. "Network Advertising Initiative: Principles not Privacy," July 28, 2000, available at <http://www.epic.org/privacy/internet/NAI_analysis.html>.

user must submit an e-mail address. Users can also submit their real name, city/locale, gender, age, occupation, marital status, personal statement, hobbies and interest, favorite quote, favorite things, a personal photo, and a home page. Hailstorm was a group of services (including MyAddress, MyProfile, MyContacts, MyNotifications, MyInbox, MyCalendar, MyDocuments, MyApplicationSettings, MyWallet, MyUsage, and MyLocation) that Microsoft intended to provide from central servers. In theory it would have collected an extraordinary range of consumer information. Privacy and consumer groups in the United States filed a series of complaints against Passport and Hailstorm with the Federal Trade Commission in 2001, detailing the risks to privacy and security in these systems. In July 2002, European Union (European Union) officials confirmed publicly that they were pursuing an investigation into Passport for breach of European privacy laws.¹⁸⁹

A competitor to Microsoft's Passport, Project Liberty, is being developed by a coalition of companies.¹⁹⁰ This identification system is similar to Microsoft's single sign-on, however, it allows users to choose what companies will receive personal information. The goal of Project Liberty is to facilitate information sharing so that companies can create and exchange profiles of individuals personal information.

Attempts at developing more permanent methods of identifying users have been underway for years. In 1999, Intel announced that it was including a serial number in each new Pentium III chip that could be accessed by websites and internal corporate networks. Most of the manufacturers suppressed the number after a consumer boycott was announced, and Intel announced in 2000 that it is dropping the serial number in future chips. Microsoft and RealAudio were discovered using the internal networking number found in most computers as another identifier for online users. Microsoft's Windows Media Player contains a globally-unique identifier (GUID) that can be tracked by website operators. The Internet Engineering Task Force has developed specifications for the next version of the Internet's underlying protocols called IPv6 that will assign a unique permanent ID number to every device hooked into the net, which could one day include refrigerators and VCRs.

¹⁸⁹ European Union Article 29 Data Protection Working Group, "First orientations of the Article 29 Working Party Concerning Online Authentication Services," July 2, 2002, available at <http://www.epic.org/redirect/eu_redirect.html>.

¹⁹⁰ See Project Liberty Homepage <<http://www.projectliberty.org/>>.

Security Breaches

The privacy of online consumers can also be seriously compromised by security breaches. Many web sites are poorly secured against accidental releases or deliberate attacks.¹⁹¹ In March 2000, De Beers lost 35,000 names, addresses, phone numbers and e-mail addresses of people inquiring about buying diamonds following a security breach. In April 2000, it was revealed that an unknown Microsoft engineer had included a backdoor into its web server software. If someone typed, “Netscape engineers are weenies!” backwards, they would have access to the websites and associated data. In August 2000, Kaiser Permanente, a top United States health insurer, admitted that it had compromised the confidentiality and privacy of its members when it sent over 800 e-mail messages, many containing sensitive information, to the wrong members.¹⁹² Similarly in July 2001, makers of the anti-depressant drug “Prozac” revealed the names and email addresses of over 700 patients that subscribed to the company’s email service for information on the drug and other issues.¹⁹³

Information Brokers and Seal Programs

Many companies offer what are known as “information brokering” services, whereby users provide information to the company, which then provides it to a third-party website with the consent of the user. These sites raise a question of trust. Given that many of them are run by the same Internet companies that are also major privacy invaders, the user must wonder why they should volunteer providing information to these companies.

A common practice among online companies is to sign on to a “seal” program in order to provide consumers with a sense of security that their personal information is being protected. These programs follow the traditional seal programs in laying down certain eligibility standards which participant companies must respect in order to get a compliance seal. The better seal programs conduct monitoring and compliance checks, provide educational information, offer consumer dispute resolution, and enforce sanctions against errant companies. There are many disadvantages of seal programs operating within a self-regulatory system. All too often, seal program operators have been

191 See, e.g., Eric Murray, SSL Server Security Survey, July 31, 2000 showing that encryption on most e-commerce sites is inadequate, <http://www.meer.net/~ericm/papers/ssl_servers.html>.

192 “Sensitive Kaiser E-Mails Go Astray,” Washington Post, August 10, 2000.

193 “Prozac Maker Reveals Patient E-Mail Addresses,” Washington Post, July 4, 2001, at E01.

shown to be ineffective and reluctant to take enforcement measures against their members including companies such as Microsoft.¹⁹⁴ A 1999 Forrester research report found that, “because independent privacy groups like TRUSTe and BBBOnline earn their money from e-commerce organizations, they become more of a privacy advocate for the industry – rather than for consumers.”¹⁹⁵

Privacy Enhancing Techniques

There are tools available that can be used to protect the privacy of users in many cases. These technologies are known as “Privacy Enhancing Technologies” (PETs) and are aimed at eliminating or limiting the collection and processing of identifiable data. Encryption is an important tool for protection against certain forms of communications surveillance. When properly implemented, a message is scrambled (encrypted) so that only the intended recipient will be able to unscramble (decrypt), and subsequently read, the contents. Pretty Good Privacy (PGP) is the best known encryption program and has hundreds of thousands of users. An alternative is the open source program called GNU Privacy Guard (GPG) that allows anyone to view the full source of the system to ensure that it does not allow for secret surveillance.¹⁹⁶ Cryptographic modules are also implemented in applications; for example web browsers, in order to maintain some confidentiality in electronic commerce transactions, include Secure Sockets Layer (SSL) to encrypt sessions between users and servers.

Traditional cryptography implementations protect only the confidentiality and integrity of the communications content. They do little to prevent the disclosure of traffic data; that is, it is still clear that person A is emailing person B, or that person A is visiting web site W. More sophisticated applications are required to maintain the privacy of these transactions. “Anonymous remailers” strip identifying information from e-mails and can stop traffic analysis. Services such as Anonymizer, provide anonymous websurfing, email messaging, banner ad and pop-up blocking and deletes cookies and web bugs after Internet sessions.¹⁹⁷

During the past year there were significant setbacks in the effort to develop commercially viable privacy enhancing techniques. In October 2001, Zero Knowledge Systems ceased to operate the Freedom Network, which used to

¹⁹⁴ “Just How Trusty is Truste,” *Wired*, April 9, 2002
<<http://www.wired.com/news/exec/0,1370,51624,00.html>>.

¹⁹⁵ Forrester Research Inc, “Privacy Wake-Up Call,” September 1, 1999.

¹⁹⁶ See <<http://www.gnupg.org/>>

¹⁹⁷ See <http://www.anonymizer.com>.

provide a fully encrypted and pseudonymous link between the user and secure servers, and replaced it with a simpler proxy-based service. In February 2002, a number of flaws were discovered in SafeWeb, an anonymous-surfing technology originally funded by the CIA.¹⁹⁸ In March 2002, Network Associates, the company that provided the commercial version of PGP, discontinued support for the application.¹⁹⁹ The international (free) version continues to be available from PGP International.²⁰⁰

At the same time, human rights groups and even large corporations explored new techniques to protect online privacy. The Canadian-based Privaterra worked with NGOs to encourage the use of strong encryption techniques and other methods for online privacy.²⁰¹ Hacktivism efforts continued with new efforts to empower dissident political organizations operating over the Internet. In July 2002, the international hacker group, Hactivismo, announced a new free service called “Camera Shy” to allow users to conceal messages in ordinary image files on the Internet. The browser-based steganography application automatically scans and decrypts content straight from the Internet and leaves no traces on the user’s system.²⁰² The global giant American Express is offering a system known as “Private Payments” to enable more private online commerce.²⁰³ Under this system a limited life transaction number, instead of the cardholder’s credit card number, is used to make online purchases.²⁰⁴

It is important to distinguish between genuine privacy enhancing techniques and data security technologies that seek to render processing safe but not to reduce the disclosure and processing of identifiable data.²⁰⁵ Moreover, there are many products offered by industry that are not privacy protective. Many of these systems, such as Microsoft’s Passport and the World Wide Web Consortium’s (W3C) Platform for Privacy Preferences (P3P), are designed to facilitate data sharing rather than to limit disclosure of personal information.²⁰⁶

¹⁹⁸ Declan McCullagh, “SafeWeb’s Holes Contradict Claims,” *Wired News*, February 12, 2002, available at <<http://www.wired.com/news/politics/0,1283,50371,00.html>>.

¹⁹⁹ Sam Costello, “Network Associates Abandons Search for PGP Buyer, Axes 18,” *IDG News Service*, March 6, 2002, available at <<http://www.nwfusion.com/news/2002/0306naipgp.html>>.

²⁰⁰ Homepage <<http://www.pgpi.com/>>.

²⁰¹ Homepage <<http://www.privaterra.com>>

²⁰² Eric Auchard, “Hacker Group Targets Countries that Censor Internet,” *Reuters*, July 14, 2002.

²⁰³ http://www26.americanexpress.com/privatepayments/info_page.jsp?pers_home=shoppvtpaymts

²⁰⁴ See Private Payments FAQ <<http://www26.americanexpress.com/privatepayments/faq.jsp>>.

²⁰⁵ Herbert Burkert, “Privacy-Enhancing Technologies: Typology, Critique, Vision” in Philip Agre and Marc Rotenberg, eds, *Technology and Privacy: The New Landscape* 125 (MIT Press 1997).

²⁰⁶ EPIC and Junkbusters, “Pretty Poor Privacy: An Assessment of P3P and Internet Privacy,” June 2000 <<http://www.epic.org/reports/prettypoorprivacy.html>>.

Electronic Numbering

Electronic Numbering (ENUM) is an Internet infrastructure that will allow a single number to reference contact or other information in a public database.²⁰⁷ Individuals or businesses holding an ENUM account will be able to store information, including phone numbers, e-mail addresses, voicemail numbers, fax numbers, or any other type of data in the ENUM database. Persons wishing to contact the entity would use the ENUM to query a public database for the stored information.

ENUM raises a host of privacy issues that are yet to be resolved. Most importantly, because of the different ways in which ENUM can provide means to contact a person, ENUM has the potential to become a Globally Unique Identifier (GUID). At a more fundamental level, issues of notice and individual participation have yet to be resolved.

The ENUM owner could also include certain suggestions for the use of the contact information. For instance, when using an ENUM to query the database at 10 PM on a Friday night, the database could respond with instructions to call a cell phone rather than a land line at the office. However, the person querying the ENUM database would receive all of the owner's contact information, and could simply choose to violate the instructions.

Since the ENUM database is public, one can assume that it will be mined for commercial purposes. This may lead to an unprecedented amount of spam, as a single ENUM can reveal multiple methods of contacting a person.

Public Records and Privacy, Public-Private Ventures

Increasingly, information is being harvested from public records to create detailed profiles on individuals. Public records may contain many types of personal information that are commercially valuable. These include: Social Security numbers, birth records, arrest information, civil case history, criminal case history, addresses, drivers license information, land sales transactions,

²⁰⁷ Current information on the development of ENUM is available at <http://www.enum-forum.org/>. See also EPIC's ENUM page <http://www.epic.org/privacy/enum/>.

records of asset holdings, ownership of corporations, marital status, presence of children, employment status, and health information.

Maintaining accessible public records is important for scholarship, research, journalism, and governmental accountability. However, allowing unrestricted use of public records enables private, commercial, and governmental interests to invade individuals' privacy.²⁰⁸

The advent of remote electronic access to public records systems has raised the specter of vastly increased data mining and profiling. Mining a public records database soon will no longer require the time and expense involved in traveling to the physical location of the records. Data miners will be able to remotely access public records systems and use widely available software to harvest personal information. This harvesting of personal information already has had a substantial impact on individuals. In 2002, the Wall Street Journal reported that drug maker Eli Lilly had terminated employees for decade-old convictions discovered in dossiers aggregated from public records.²⁰⁹

Unrestricted commercial harvesting of public records has enabled the American government to obtain detailed dossiers on citizens with ease. Through private-public partnerships, several profiling companies make consumer dossiers available to the government. One company in particular, ChoicePoint, has emerged as the leading provider for law enforcement and other government agencies.²¹⁰ ChoicePoint maintains web pages customized for individual federal agencies to facilitate the sale of public record information to police.²¹¹ As a result of FOIA requests initiated by EPIC, it was discovered that ChoicePoint was selling the national ID databases of several Latin American countries to the American immigration law enforcement agency.²¹²

²⁰⁸ Daniel J. Solove, Access and Aggregation: Public Records, Privacy, and the Constitution, 86 Minnesota Law Review 6 (2002).

²⁰⁹ "Firms Dig Deep Into Workers' Past Amid Post-Sept. 11 Security Anxiety," Wall Street Journal, March 12, 2002.

²¹⁰ "If the FBI Hopes to Get the Goods on You, It May Ask ChoicePoint," Wall Street Journal, April 13, 2001.

²¹¹ See ChoicePoint FBI <<http://www.cpfbi.com>>; ChoicePoint DEA <<http://www.cpdea.com>>; ChoicePoint Government <<http://www.cpgov.com>>.

²¹² Documents available at <<http://www.epic.org/privacy/publicrecords/inschoicepoint.pdf>>.

Digital Rights Management

In an effort to stem content and software piracy, a number of companies have developed Digital Rights Management (DRM) systems to prevent the unauthorized use of digital files.²¹³ DRM technologies can control file access (number of views, length of views), altering, sharing, copying, printing, and saving. These technologies may be contained within the operating system, program software, or in the actual hardware of a device. Some DRM technology can disable users' machines for unauthorized access to files. InTether Point-to-Point, for instance, imposes "penalties" for those who attempt an "illegal use" of a digital file.²¹⁴ Penalties include automatic rebooting of the users' machine, or destruction of the file the user is attempting to access.

These technologies have been developed with little regard for privacy protection. DRM technology usually requires the user to reveal his or her identity and rights to access the file. Upon authentication of identity and rights to the file, the user can access the content.

These systems can prevent anonymous consumption of content, and could be employed to profile users' preferences or to limit access to digital books, music, or programs. DRM technologies may "...enable an unprecedented degree of intrusion into and oversight of individual decisions about what to read, hear and view."²¹⁵ For instance, a DRM technology called Copyright Agent quietly scans peer to peer networks to discover whether users possess illegal content. If a copyright violation is found, the program automatically informs the users' Internet Service Provider that his or her service should be severed.²¹⁶

In February 2002, the European Commission Information Society Directorate held a workshop on DRM technologies to examine, among other issues, their effects on privacy.²¹⁷

In June 2002, Microsoft released information regarding its new "Palladium" initiative. Although, not much is known about the initiative, Palladium appears to

²¹³ See EPIC's DRM page <<http://www.epic.org/privacy/drm/>>.

²¹⁴ InTether Point to Point Product Page <<http://www.infraworks.com/p2p.html>>.

²¹⁵ Julie Cohen, A Right to Read Anonymously: A Closer Look at "Copyright Management" in *Cyberspace*, 28 Connecticut Law Review 981 (1996).

²¹⁶ Dawn C. Chmielewski, "Stealth Software Robot Puts Bootleggers on Notice," San Jose Mercury News <<http://www.chicagotribune.com/business/printedition/article/0,2669,SAV-0103190188,FF.html>>.

²¹⁷ More information and the final report of the workshop are available at <http://europa.eu.int/information_society/topics/multi/digital_rights/events/index_en.htm>.

be a more comprehensive version of its Hailstorm and Passport services. Through software and hardware controls, Palladium would place Microsoft as the gatekeeper of identification and authentication. Additionally, systems embedded in both software and hardware would control access to content, thereby creating ubiquitous DRM schemes that can track users and control use of media. Microsoft expects to have elements of the system in place by 2004.

Authentication and Identity Disclosure

As the architecture of authentication is developed and established through de jure, de facto, and technical standards, there are significant privacy implications. While authentication is considered essential for computer security, it may detract from individual privacy, depending on how authentication is implemented. In the best case scenario, individuals could choose to not authenticate in order to receive a given service, and authentication would involve the selective disclosure of some information that allows for the verification of the integrity of a transaction. In the worst case scenario, authentication can be implemented in such a way that every transaction an individual enters in, whether surfing the web, sending mail, accessing government services, and purchasing on-line, will be traced, tracked, audited, and compiled to an unprecedented degree. The resulting issue is what exactly is disclosed when authentication occurs, whether this involves the disclosure of personally identifiable information, and whether this is necessary and proportionate.

Defining Identity Disclosure

Policy processes often predetermine the form of authentication being considered in the very definition of the terms. Many of these processes, however, began in the midst of the cryptography policy debate in the 1990s, and carry much of the baggage from that era, such as the reliance on Trusted Third Parties²¹⁸ and X.509 identity certificates with limited signing capabilities.²¹⁹

²¹⁸ Licensing Of Trusted Third Parties For The Provision Of Encryption Services Public Consultation Paper on Detailed Proposals for Legislation, Department of Trade and Industry (1997); archived at <<http://www.fipr.org/polarch/ttp.html>>.

²¹⁹ Building Confidence in Electronic Commerce - A Consultation Document, Department of Trade and Industry (1999); archived at <<http://www.dti.gov.uk/cii/ecommerce/ukecommercestrategy/archiveconsultationdocs/introduction.shtml>>.

The ISO²²⁰ defines authentication as "the provision of assurance of the claimed identity of an entity." Industry Canada's definition, found in a 2000 consultation document on an authentication framework,²²¹ is "proof that users are who they claim to be (or that computer devices, software, etc. are what they purport to be)." Digital signature statutes around the world have been developed to allow for digital signatures to be used to sign legal documents (and extended logically to sales transactions, or signing documents and messages); embedded within these statutes again is identity-centrism, which is not a requirement necessarily of analogue-world signatures. UNCITRAL developed a model law on electronic signatures to meet this requirement, and define electronic signatures as "data in electronic form in, affixed to, or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message."²²²

As these articulations of digital signatures and certificates are used for purposes beyond signing legal documents, such as access control, the interpretive application of authentication becomes suspect. This poses a serious conflict with privacy principles, most notably informational self-determination as every time authentication occurs, assured-identity is disclosed, either through direct identification or through personally identifiable information. Likewise, at commercial level, identity disclosure is supported by the terminology. Consider the following statement from a senior vice president of the Information Technology Association of America:²²³

When people are online, they want to know with whom they are dealing. They want to know that people are who they say they are, and are going to follow through with commitments made over the Internet and thus supporting identity-disclosure for electronic transactions. Public Key Infrastructure vendors are supporting this view with the use of the X.509 standard of certificates that are bound to an identity by a Certificate Authority.

Even the Internet Engineering Task Force defines authentication as being identity-centric that is, "[t]he process of verifying an identity claimed by or for a

²²⁰ Glossary of IT Security Terminology, SC 27 Standing Document no 6, ISO/IEC JTC 1/SC 27, Doc. No.: SC 27 N 1954, Date: March 5, 1998.

²²¹ Building Trust and Confidence in Electronic Commerce: A Framework for Electronic Authentication, Industry Canada (2000) <<http://e-com.ic.gc.ca/english/documents/framework.pdf>>.

²²² United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Signatures (2001). Report of the Drafting Group, 34th session, Vienna, June 25 - July 13, 2001.

²²³ "Are You Who You Say You Are?" Wired News, March 31, 1999.

system entity."²²⁴ Additionally, the IETF has also been working on Public Key Infrastructure standards that bind identities to public keys.

Authentication services have another application beyond verifying signatures, however. While certificates and keys can be used for digitally signing documents, these certificates also act as an access control mechanism to provide a secure session. That is, traditionally if a user of a specific on-line service wishes to connect to that service, the user may present a username and password. Using authentication services instead, a user may present a certificate that contains a public key and identity signed by the service provider or another trusted third party, and this is in turn used to set up a secure session (Trusted Layer Session, or Secure Sockets Layer) with that service provider so that all communications between the user and the service provider are encrypted. The obligatory passage point is the disclosure of a greater level of personally identifiable information than previously, and in a more non-repudiable form (which thus introduces greater risks).²²⁵

Inscribing Identity into Policy

At the political level, authentication and identity are often synonymous. The Group of 8 industrialized countries (G8) has been working on the issue of authentication on two fronts. Under the auspices of the Lyon Subgroup on high-technology crime, the G8 has been proposing repeatedly²²⁶ the use of user authentication when on-line, and the use of machine authentication to create traceability in electronic transactions for investigative purposes and to gather evidence. In a separate forum, the G8 developed the Okinawa Charter on Global Information Society where the requirement for authentication was bound with initiatives to resolve the digital divide.²²⁷ As a result, the two foras and the two set of interests converge around authentication: the ability to support verification of the validity of transactions for the purpose of security, and the ability to identify individuals for surveillance.

²²⁴ Internet Security Glossary, RFC 2828, IETF Network Working Group, May 2000
<<http://www.ietf.org/rfc/rfc2828.txt>>.

²²⁵ Bohm, Nicholas, Ian Brown and Brian Gladman, "Electronic Commerce: Who Carries the Risk of Fraud?" *The Journal of Information, Law and Technology* (2000).

²²⁶ Communiqué Annex: Principles and Action Plan To Combat High-Tech Crime, G7 meeting of Justice and Interior Ministers, Washington DC, December 10, 1997
<<http://www.g8summit.gov.uk/prebham/washington.1297.shtml>>.

²²⁷ The charter is available at <<http://www.dotforce.org/reports/it1.html>>.

Inscribing Identity into Infrastructure

A public key infrastructure (PKI) has been heralded as the solution to many security problems. The infrastructure involves individuals with public and private keys which are semantically altered into certificates and signature keys respectively. Trust is developed through this transformation of the public key into a certificate: the owner of the public key registers the key with a CA who binds the identity of the individual with the key, creating the certificate. This certificate is then used to verify transactions signed with the private/signature key, and parties in a transaction can therefore ascertain the identity of the individual. The issue then becomes one of scale: if one certificate is issued by government for the use of gaining access to government services (as is often the proposed scheme under the auspice of Information Society projects, including the G8 Charter for example), then this very same certificate, or at least infrastructure of CAs may be used for purchases on-line with a number of service providers, or merely gaining access to information.²²⁸

Inscribing Identity into Technology

Authentication mechanisms are used within multiple applications varying from toll-machines through to copyright protection mechanisms. The inscription of identity within these technologies is occurring already. Mobile phones have authentication techniques that assure that a specific card is registered to a specific phone which is then registered to a specific individual; with next generation mobile phone applications, these devices will be used for electronic transactions, and geographic-based transactions -- which will all be based upon the identity of the individual. There have been proposals to also implement national ID cards into these mobile telephones.

Smartcards are the proffered technology for enabling digital signatures; these cards will be used for credit card transactions, and gaining access to other services such as prescription medicine, tolls for transportation, telephone calling cards, and even age-verification. Smartcards are thus built upon an identity-centric authentication infrastructure. In the future this trend of privacy-invasion may continue on to biometrics, and the prevention of piracy; but so long as

²²⁸ The Privacy Risks of Public Key Infrastructures, by Austin Hill and Gus Hosein, presented at the 21st Data Protection Commissioners Conference, Hong Kong, September, 1999.

authentication details are kept on the card, the cards will remain not only a privacy threat, but a security risk as well.²²⁹

Authentication without Identification

As a result of the political, infrastructural, and technological initiatives on authentication that tend towards identity-centrism, we are not only left with a situation where privacy is vastly reduced in all levels of life, i.e. not just on-line, but we also face challenges of functionality.

From the privacy perspective, the worst case scenario is that every transaction from purchasing transport tickets through to accessing information on government web-sites will be identity-centric. The Microsoft Corporation is attempting to create such an identity-centric system through the promotion of the Microsoft Passport and Hailstorm services platform.²³⁰ Passport is an online identification and authentication system that requires the submission of personal information. Increasingly, Passport membership is becoming a requirement for access to services on the Internet. Microsoft has stated that its "dream" is for every Internet user to have a Passport.²³¹

Shifting to a world of perfect-identity may meet the interests of industry and government in ascertaining the identity of who they are transacting with; however there are rising functionality challenges. The source of these challenges range from data protection regimes, efficiency of data communications and storage, resources and costs, and issues surrounding revocation and non-repudiation. These challenges may provide sufficient incentives for government and industry to begin looking for alternative regimes of authentication that are not necessarily identity-centric.

Although the political and commercial emphasis has been placed often upon identity-centric infrastructure where identity disclosure is required, alternative solutions do exist that allow for informational self-determination. That is, a user may select which personal information is to be disclosed in the authentication process while still maintaining the security benefits of identity-centric authentication. Such solutions promote the notion of user control over personal

²²⁹ Privacy Increases Smartcard Security, by Stefan Brands, Gus Hosein, and Stephanie Perrin, presented at the 22nd Data Protection Commissioners Conference, Venice, Italy, September 2000.

²³⁰ See EPIC's Passport Page <<http://www.epic.org/privacy/consumer/microsoft/>>.

²³¹ See <<http://www.microsoft.com/presspass/legal/apr02/04-22ntranscriptam.asp>>.

data, and minimizing the risks of all of the interested actors due to the above-mentioned functional challenges.²³²

Without considering these alternatives and resisting full disclosure, we will be forced to endure the political, commercial, and technical settlement of identity-disclosure for all transactions, both on-line and off, resulting in an infrastructure of surveillance that will transform how we view traditional controls such as checkpoints, ID cards, and passport controls.

Spy TV: Interactive Television & “T-Commerce”

The convergence of communications networks, computers and mass media into an interactive network combining television and the Internet is the next progression of the technology currently being developed. Already, the new boxes are replacing the traditional cable TV set-top box with an interactive device that also includes the functions of a limited personal computer and video recorder. At the same time, personal computers are regularly equipped with TV tuner cards to handle advanced video operations.

The designers of these new appliances paint a pleasant picture of the conveniences that will be available with these new systems. They anticipate that viewers will be able to make spur of the moment purchases over their boxes, based on what their favorite star is wearing or on an individually tailored ad that appears between shows. Communities will be formed as people chat live about the plots of their favorite shows or sporting events. Vast libraries of movies and shows will be available for renting on demand by just pressing a button on the remote control. The industry calls this “T-Commerce” for Television Commerce. Millions of users are expected to be using these in just the next few years, and the ad revenue to justify the new expensive boxes is expected to hit \$5 billion by 2004.

Interactivity has been the dream of the television industry since the invention of the TV. For several decades, there have been a series of expensive tests that have failed because the technology has been crude and expensive.²³³ The change that now makes ITV possible is the evolution of the Internet and its underlying

²³² Stefan Brands, *Rethinking Public Key Infrastructures and Digital Certificates -- Building in Privacy* (MIT Press 2000)

²³³ L. J. Davis, *The Billionaire Shell Game: How Cable Baron John Malone and Assorted Corporate Titans Invented a Future Nobody Wanted* (1998).

protocols and the advancement of digital television. These protocols are now being used to allow for interactive high-speed access to the Internet over existing cable lines. Slowly, intelligent cable TV boxes, which connect to broadband and interactive cable systems, are being deployed.

A number of companies have jumped into this new market in the last few years. The largest players are America Online and Microsoft. Microsoft purchased WebTV in 1998 and has also been including interactive television abilities in their operating systems for several years. Thus far, because of poor service, little interactive programming, and relatively high prices, the number of users has not significantly grown. They also are hampered by the need to use telephone lines to communicate with the service in most areas as cable lines are slowly becoming converted to interactive communications. America Online has announced that it will start deploying AOL TV in the United States in 2000. When its merger with media giant Time-Warner is complete, it will have control over a significant portion of the cable television lines and television shows in the United States. It is expected that AOL will use that market power to force the development of more interactive television and the deployment of interactive boxes that will be capable of tracking users even if they do not wish to use the functions.

Meanwhile, there are other companies that have developed devices that will automatically record television shows for viewers and make recommendations for new shows based on viewers' previous behavior. The new systems are being designed, like their Internet predecessors, to track every activity of users as they surf the net through the boxes. They also are being designed to track the shows and commercials users watch and to use that information to tailor advertising for the greatest effect.²³⁴ Rupert Murdoch said in the NewsCorp annual report, "It will tell us not only who our customers are, but what they buy, what they watch, what they read and what they want."²³⁵ George Orwell's vision of the television that watches you will soon be a standard consumer appliance.

Even where systems are designed not to report back this kind of information, there is increasing pressure from the content industries to build systems this way so that they can monitor viewer's habits and protect against copyright infringement. This year, SONICBlue Inc., the maker of Replay TV, a personal video recorder, was sued by the entertainment studios who argued that features allowing users to pause, fast forward, and skip commercials violated their

²³⁴ See David Burke, *Spy TV* (Slab-O-Concrete Press 1999), available at <<http://www.spyinteractive.com/spyinteractive/>>.

²³⁵ Cited in *Privacy Journal*, October 1999.

copyrights. As part of the lawsuit, the studios requested all data that the company had on its customers viewing habits, including what shows were recorded, watched, and forwarded to friends. Because the ReplayTV 4000 product did not transmit this sort of data back to the company, SONICblue had no data to provide to the studios. It was, therefore, ordered by a court to re-engineer its product and install software to record TV usage data and transmit that data back to SONICblue so that it could then be turned over to the studios. This order was overturned in May 2002 but the issue is likely to resurface.²³⁶

Unlike personal computers that give users control over their actions and choices, the new ITV systems are generally based on a sealed “black box” controlled by the company that gives the user little or no control. In the WebTV box, users are not able to refuse cookies or delete them afterwards. The systems are closed and it is difficult, if not impossible, for even advanced users to identify what the system is doing. It will also prevent users from being able to use their own software.

There are other significant differences in that the media is more top-down, and corporatized than the Internet, which is decentralized and allows nearly any user to set up his own web site and become a content producer. Many of the ITV providers describe their systems as “closed gardens” that will only show content that the providers have a financial interest in. Other information will either be banned or be slower or more difficult to locate and view.

Genetic Privacy

Genetic data poses unique privacy issues since it can serve as an identifier and can also convey sensitive personal information. Not only does genetic information provide a fingerprint through variations in genetic sequences; it also provides a growing amount of information about genetic diseases and predispositions.

Errors in the genetic code are responsible for an estimated 3,000 to 4,000 hereditary diseases, including Huntington's disease, cystic fibrosis, neurofibromatosis, Duchenne muscular dystrophy, and many others. What's more, altered genes are now known to play a part in cancer, heart disease, diabetes, and many other common diseases. In these more common and complex

²³⁶ Paramount Pictures Corp., et al. v. ReplayTV, Inc. and SONICblue, Inc., United States District Court, Central District of California, Case No. 01-09358 FMC (Ex). See EPIC's page on this case at <http://www.epic.org/litigation/replaytv/>.

disorders, genetic alterations increase a person's risk of developing that disorder. The disease itself results from the interaction of such genetic predispositions and environmental factors, including diet and lifestyle.²³⁷

Even more controversial than genetic predisposition to disease is the fact that "genes do appear to influence behavior."²³⁸ Genes have been found to influence homosexuality, thrill seeking and tendencies towards violent criminal behavior.²³⁹ Twin and adoption studies have shown that "nearly all behaviors that have been studied show moderate to high inheritability - usually to a somewhat greater degree than do many common physical diseases."²⁴⁰

The prevailing scientific opinion is that most behavior and human diseases are not the result of a single mutation or gene. Rather, most facets of human development "represent the culmination of lifelong interactions between our genome and the environment."²⁴¹ Currently available scientific knowledge thus does not seem to provide a strong link between an individual's genetic sequence and that person's eventual development of disease or personality traits; such conclusions are often speculative or, at best, matters of probability.

However, it is an area of scientific development that is undergoing rapid change and the body of knowledge about the human genome is increasing rapidly. The human genome sequence was published in February 2001, immediately kicking off a debate of the future of genetic technology and its impact on society - including privacy.²⁴² For example, United States Senators James M. Jeffords and Tom Daschle have commented, "[o]ne of the most difficult issues is determining the proper balance between privacy concerns and fair use of genetic information."²⁴³

²³⁷ "From Maps to Medicine: About the Human Genome Research Project," National Human Genome Research Institute, <http://www.nhgri.nih.gov:80/Policy_and_public_affairs/Communications/Publications/Maps_to_medicine/about.html>

²³⁸ Leroy Hood and Lee Rowen, "Genes, Genomes, and Society," *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era*, Edited by Mark A. Rothstein 27 (Yale University Press 1997).

²³⁹ *Id.*

²⁴⁰ Peter McGuffin, Brien Riley, Robert Plomin, "Genomics and Behavior: Toward Behavioral Genomics," *Science* 291 (5507): 1232, available at <<http://www.sciencemag.org/cgi/content/full/291/5507/1232>>.

²⁴¹ Leena Peltonen and Victor A. McKusick, "Genomics and Medicine: Dissecting Human Disease in the Postgenomic Era," *Science* 291 (5507): 1224, available at <<http://www.sciencemag.org/cgi/content/full/291/5507/1224>>.

²⁴² Genome Landmark, *Science* <<http://www.sciencemag.org/feature/data/genomes/landmark.shl>>.

²⁴³ James M. Jeffords and Tom Daschle, "Policy Issues in the Genome Era," *Science* 291 (5507): 1249, available at <<http://www.sciencemag.org/cgi/content/full/291/5507/1249>>.

Both the general public and scientific researchers have recognized that safeguards for genetic information are needed. For example, polls have found that 86% of adults believe that doctors should ask permission before conducting any genetic testing and 93% believe that researchers should do the same before any analysis.²⁴⁴ Dr. Francis S. Collins, Director of the National Human Genome Research Institute, has observed that "in genetics research studies, we are seeing individuals who opt not to participate in research because of their fear that this information could fall into the wrong hands and be used to deny them a job or a promotion."²⁴⁵

Genetic Identification

Unlike fingerprints, DNA sequences are not unique (identical twins have different fingerprints but the same DNA profiles). DNA identification works by comparing particular regions of two samples and looking for differences rather than comparing entire DNA sequences. Identification is actually a process of combining several such comparisons and calculating the probability that the two samples are a false match. "Provided that tests are actually looking at different regions of the genome, and provided that the genetic patterns aren't 'structured' within a community by inbreeding, using multiple tests can reduce the chance of a false match from one in a hundred to one in a million or even one in 500 million. But they can't entirely eliminate the chance of a false match."²⁴⁶ That has proven to be true in at least one instance. In Britain, a DNA match between evidence left at the scene of a robbery and an individual who had already been entered into that country's DNA database turned out to be false despite calculated odds of 37 million to one that a false match would occur. According to a FBI spokesman, "[t]here's a greater chance that you'll find a close match as the databases get bigger."²⁴⁷ Besides false matches, some criminals have become reportedly more savvy at manipulating results of DNA identification.²⁴⁸

²⁴⁴ Public Attitudes Toward Medical Privacy, conducted by the Gallup Poll for the Institute for Health Freedom, September 2000, available at <<http://www.forhealthfreedom.org/Gallupsurvey/IHF-Gallup.html>>.

²⁴⁵ Testimony of Francis S. Collins, M.D., Ph.D., Director, National Human Genome Research Institute, National Institutes of Health, Testimony Before the Health, Education, Labor, and Pensions Committee, United States Senate, Hearing on Genetic Information in the Workplace, July 20, 2000, available at <<http://labor.senate.gov/Hearings/july00hr/072000wt/072000jmj/collins720/collins720.htm>>.

²⁴⁶ Simson Garfinkel, Database Nation: The Death of Privacy in the 21st Century 49 (O'Reilly 2000).

²⁴⁷ Rebecca Pollard, "Crime Genes: A DNA Mismatch Raises Fears," ABCNews.com, June 19, 2000 <<http://abcnews.go.com/sections/tech/MITTechReview/techreview000608.html>>; Richard Willing, "Mismatch calls DNA tests into question," USA Today, February 8, 2000.

²⁴⁸ Richard Willing, "Criminals try to outwit DNA," USA Today, August 28, 2000.

Law enforcement agencies are increasingly relying upon DNA evidence thus making it important that any genetic data collected is uncontaminated and accurately processed. Judges and courts have issued warrants²⁴⁹, indictments²⁵⁰ and even convictions²⁵¹ based solely on DNA identification.

DNA identification is also heavily relied upon in order to exonerate previously convicted criminals. One of the best-known efforts is the Innocence Project at the Cardozo School of Law, Yeshiva University. Founded in 1992 by Professor Barry Scheck, the clinical law program provides legal assistance to persons challenging their convictions based on DNA evidence. The clinic has participated in thirty-six of the sixty-three convictions that have been overturned on the basis of DNA evidence since the 1980s. On the basis of the proportion of cases that have been overturned and related FBI data, the Innocence Project estimates that thousands of individuals wrongly convicted could be freed if provided with easier access to DNA testing.²⁵² Similar Innocence Project programs have also started at the University of Wisconsin Law School, the University of Washington School of Law and the Santa Clara University of Law.²⁵³

Despite the recognition of such limitations, there is a push for more and larger DNA databases. DNA databases are often created from a strictly law enforcement purpose, usually related to violent offenders, but have expanded in purpose and scope. "In less than a decade, we have gone from collecting DNA from convicted sex offenders – on the theory that they are likely to be recidivists and that they frequently leave biological evidence – to data banks of all violent offenders; to juvenile offenders in 29 states; to testing of persons who have been arrested, but not convicted of a crime."²⁵⁴ In the United States, local, state and federal law enforcement agencies contribute samples from crime scenes and those convicted of violent crimes into a national database to look for potential matches.²⁵⁵ In the United States, some officials have urged that non-violent

²⁴⁹ Richard Willing, "Police expand DNA use: Charge man with rape using only genetic profile," USA Today, October 25, 2000.

²⁵⁰ Michael Luo, "Unnamed Man Indicted by DNA: Suffolk DA Charges Suspect in 6 South Shore Rapes," Newsday, August 9, 2000.

²⁵¹ Bruce Hight, "DNA Can Carry Conviction," Austin-American Statesman, April 14, 2000.

²⁵² Cardozo Law Innocence Project <http://www.cardozo.yu.edu/innocence_project/>.

²⁵³ Frank J. Remington Center, Innocence Project <<http://www.law.wisc.edu/FJR/innocence/>>; Innocence Project Northwest <<http://www.law.washington.edu/ipnw/>>; Northern California Innocence Project <http://www.scu.edu/scu/law/clinic/Special_Projects/Innocence_Project/innocence_project.html>.

²⁵⁴ Testimony of Barry Steinhardt, Associate Director of the American Civil Liberties Union, Before the House Judiciary Committee, Subcommittee on Crime, March 23, 2000, available at <<http://www.aclu.org/congress/1032300a.html>>.

²⁵⁵ FBI Press Room, Press Release, October 13, 1998, DNA Index, available at <<http://www.fbi.gov/pressrel/pressrel98/dna.htm>>.

criminal offenders, such as burglars, to also be included in DNA databases.²⁵⁶ Other countries such as Great Britain are similarly considering proposals to expand their own national DNA databases.²⁵⁷ Several Australian states have been considering laws that would permit the creation of a national DNA database.²⁵⁸ One Australian legislator has even called for collecting DNA samples from babies at birth.²⁵⁹

Other, non-law enforcement related DNA databases have also emerged. Since the early 1990s, all personnel serving in the United States Armed Forces have been required to submit DNA samples to ensure later identification. The United States military's DNA depository "contains 2.1 million index card-sized files with the name, Social Security number, fingerprint and blood sample of every active duty military person."²⁶⁰ However, the program has faced resistance within the military's own ranks. In 1996, two United States Marines faced court-martials when they refused to provide DNA samples for the identification program.²⁶¹

In addition to government-related DNA identification, a new industry - paternity testing - has emerged, placing large amounts of genetic data wholly under private sector control. Despite the controversy surrounding law enforcement collection of DNA, a larger proportion of genetic identification is done to establish paternity. In the United States, part of the reason for the rise in paternity DNA testing are federal requirements for identifying fathers in order to receive child support.²⁶² Paternity testing previously required blood samples and was more difficult to perform than currently used DNA tests - which may only require a few strands of hair.²⁶³

²⁵⁶ "Slow Spiral: State DNA Lag Databases," *Government Technology*, April 2000, <<http://www.govtechapternet/publications/crimetech/Apr00/CTEDNA.phtml>>; "Maryland Seeks DNA of Criminals," *Washington Post*, March 24, 1999; Geraldine Sealey, "Debating DNA: The Ultimate Crimefighting Tool, or the Ultimate Invasion of Privacy," *ABCNews.com*, August 4, 1999.

²⁵⁷ "New doubts over DNA register," *The Guardian*, September 2, 2000, available at <<http://www.guardian.co.uk/Print/0,3858,4058441,00.html>>; Melissa Kite and Richard Ford, "Blair orders DNA register of criminals," *The Times*, September 1, 2000.

²⁵⁸ "Concern over proposed DNA databases," *Australian Broadcasting Corporation (ABC) Online*, January 24, 2000 <<http://www.abc.net.au/worldtoday/s95485.htm>>; Stewart Taggart, "DNA Testing Furor in Wee Waa," *Wired News*, April 18, 2000 <<http://www.wired.com/news/print/0,1294,35727,00.html>>.

²⁵⁹ "Call to take DNA from newborn babies to fight crime," *Independent News*, April 25, 2001 <<http://news.independent.co.uk/world/australasia/story.jsp?story=68669>>.

²⁶⁰ "Will DNA identification end Unknown Soldier tradition?" *Associated Press*, May 29, 1998 <<http://www.onlineathens.com/1998/052998/0529.a3soldier.html>>.

²⁶¹ Neil A. Lewis, "2 Marines who Refused to Comply with Genetic-testing Order Face a Court-Martial," *The New York Times*, April 13, 1996.

²⁶² Genelex: The Paternity DNA Testing Site, "Chapter 4: DNA in Parentage Testing, Updated for the Web Edition," April 2000 <<http://www.genelex.com/paternitytesting/paternitybook4.html>>.

²⁶³ DNAnow.com, "Frequently Asked Questions," <<http://www.dnanow.com/faq.html>>.

Genetic Testing

Advances in technology have made genetic testing easier and faster. According to genetic testing companies, kits costing \$100-\$2,000 are available for over 400 diseases with hundreds more coming on the way.²⁶⁴ The easy availability of tests vastly increases the amount of information at an individual's disposal. More problematic is the possibility that individuals will not be able to control when such testing is conducted or how the results may be used. The two most controversial areas of genetic testing are in the workplace and the provision of medical and life insurance. Also, as in genetic identification, genetic testing is prone to quality control issues. A 1999 survey of genetic testing facilities found that of the 245 laboratories examined, 36 failed to meet high quality assurance standards.²⁶⁵

A number of countries, such as Iceland and Estonia are building nationwide DNA databases for medical research. Many of these undertakings are encouraged by pharmaceutical companies and other business enterprises looking to make profits from new medical procedures and services. Some efforts have been made to establish legal frameworks for these databanks.²⁶⁶

Right Not to Know

While genetic screening has become easier and cheaper, treatment of genetic disease lags behind. Thus, while someone may have the ability to determine if they are at high-risk of disease, many people may choose not to find out due to the inability to take any precautionary measures. The concept of a "right not to know" would apply in these situations, allowing a person to control whether she has a certain genetic make-up.

For example, Huntington's disease is an inherited neurological disease that results in death by a person's late 30s or early 40s after extended deterioration of both mental and physical control. There is no treatment for the condition yet a reliable test for Huntington's does exist. The inheritability of the disease is straightforward; the children of a person with Huntington's will have a fifty-percent chance of also being affected. The resistance to knowing one's propensity

²⁶⁴ Lisa M. Krieger, "Genetic testing leaps ahead of social implications," San Jose Mercury News, July 3, 2001 <<http://www.siliconvalley.com/docs/news/depth/gene070301.htm>>.

²⁶⁵ Margaret M. McGovern, MD, PhD; Marta O. Benach; Sylvan Wallenstein; Robert J. Desnick, PhD, MD; Richard Keenlyside, MD, MS, "Quality Assurance in Molecular Genetic Testing Laboratories," *Journal of the American Medical Association*, Volume 281 No. 9, March 3, 1999, at 835-40 <<http://jama.ama-assn.org/issues/v281n9/abs/jto90000.html>>.

²⁶⁶ See, e.g., Iceland Act on Bio Banks.

for Huntington's is borne out in surveys finding that only 66 percent of those at risk of developing Huntington's would test themselves with 15 percent of that group indicating they would contemplate suicide if they tested positive. Of those indicating that they would not want to test themselves, 30 percent indicated they would consider suicide if they did find out that they would manifest the disease.²⁶⁷ Due to the emotional and psychological impact that such information would have, many people in these situations exercise their "right not to know" by refusing to test themselves.

In practice, maintaining a "right not to know" can be difficult. Due to the simple inheritability of Huntington's, one family member's decision to test herself for Huntington's will reveal information about other family members. For example, if a daughter decides to test herself for Huntington's due to a history of the disease through her mother's side of the family, the test results would indicate whether or not her mother also has the disease - thus compromising the mother's desire not to know.²⁶⁸

In the Workplace

As DNA and genetic databases become more common world-wide, there has been a concurrent rise in the use of testing by employers. Although there are legitimate uses of genetic testing, such as the prevention of occupational diseases, there is also a serious danger that employers will use these tests to discriminate against current or potential employees. Without legal intervention, information indicating, for example, whether someone is prone to a debilitating illness or even an "undesirable" condition (such as laziness or depression) may be used by employers to discriminate against employees.

Genetic screening in the workplace has been conducted for decades but, based on limited polling of employers, still seems relatively rare when compared to general medical information accessed by employers. Some of the earliest genetic screening took place as early as the 1960s. Dow Chemical conducted genetic monitoring (genetic tests conducted over time to detect possible mutagenic

²⁶⁷ Office of Technology Assessment (OTA): Genetic monitoring and screening in the workplace, OTA-BA-455 (Washington, United States Government Printing Office, October 1990), p. 13. (As cited in Conditions of Work Digest, "Workers' privacy III: Testing in the workplace," (International Labour Office 1993), at 66.)

²⁶⁸ See Margaret R. McLean, "When What We Know Outstrips What We Can Do," Markkula Center for Applied Ethics, Issues in Ethics - V. 9, N. 2, available at <<http://www.scu.edu/SCU/Centers/Ethics/publications/iie/v9n2/outstrips.html>>; Sally Lehrman, "Predictive Genetic Testing: Do You Really Want to Know Your Future?" The DNA Files, November 1998, available at <<http://www.dnfiles.org/about/pgm4/topic.html>>.

effects of the workplace environment) from 1964-1977.²⁶⁹ In 1982, a United States federal government survey found that 1.6 percent of companies were using genetic testing for employment purposes.²⁷⁰

Despite the uncertainty about how commonly workplace genetic testing takes place, it has happened. In 1994, employees at the Lawrence Berkeley National Laboratory at the University of California - Berkeley discovered the laboratory's surreptitious practice of testing its employee blood and urine samples for syphilis, sickle cell anemia and pregnancy.²⁷¹ The laboratory, funded by the United States Department of Energy, conducts non-classified research and had been testing its employees for decades.²⁷² In subsequent litigation, the government argued that since its employees had agreed to a general medical examination, they had no reason to expect that genetic testing would not also be conducted. The government also argued notice was provided via a list of tests to be conducted posted on an examining room wall. The government won at in the federal district court but the United States Court of Appeals for the Ninth Circuit reversed and concluded the conditions being tested for raised "the highest expectations of privacy."²⁷³ In 2000, the laboratory settled with employees for \$2.2 million, ceased conducting the tests and allowed earlier test results to be reviewed and deleted.

More recently, in February 2001, an employee of the Burlington Northern Santa Fe Railroad in the United States sued the company for conducting tests for a genetic predisposition associated with carpal tunnel syndrome. The company had allegedly collected blood samples from 125 employees and tested 18 of those samples without employee consent. The employee filing the suit had refused to contribute a blood sample and was told he would be investigated. The lawsuit

²⁶⁹ United States Congress, Office of Technology Assessment, *Genetic Monitoring and Screening in the Workplace* 44-45 (1990); *Are Your Genes Right for Your Job?* 3 Cal Law 25, 27 (May 1983). (As cited in *Employee Privacy Law*, ed. L. Camille Hébert, (West Group 2000) § 12:03.)

²⁷⁰ United States Congress, Office of Technology Assessment, *The Role of Genetic Testing in the Prevention of Occupational Diseases* 33-35 (1983); United States Congress, Office of Technology Assessment, *Genetic Monitoring and Screening in the Workplace* 173-177 (1990).

²⁷¹ Dana Hawkins, "A bloody mess at one federal lab: Officials may have secretly checked staff for syphilis, pregnancy, and sickle cell," *United States News and World Report*, June 23, 1997.

²⁷² Even more shocking was the practice of the research facility to test certain minority employees for particular traits. For example, while all new hires were tested for syphilis, only African-American and Latino employees were re-tested during subsequent medical examinations. Only one Caucasian employee was repeatedly tested for syphilis; he was married to an African-American woman. African-American employees were also repeatedly tested for sickle cell anemia although one test is normally sufficient.

²⁷³ *Norman-Bloodsaw v. Lawrence Berkeley Laboratory*, 135 F.3d 1260, 1269-70 (9th Cir. 1996). See also L. Camille Hébert, *Employee Privacy Law* § 12.07 (West Group 2000); "Court declares right to genetic privacy," *United States News and World Report*, February 16, 1998 <<http://www.usnews.com/usnews/issue/980216/16upda.htm>>.

alleges violation of disability law and existing legal prohibitions on genetic testing by employers.²⁷⁴

Insurance

While closely tied to workplace genetic testing (as employers may avoid hiring certain individuals to due to a perceived increase in the amount need for insurance coverage), genetic testing has also begun to be used in the provision of life and medical insurance directly. In February 2001, Norwich Union Life, one of Britain's largest insurers, admitted using genetic tests for breast and ovarian cancer and Alzheimer's disease to evaluate applicants. Moreover, Norwich Union Life was violating the industry's code of conduct since the genetic tests had not been approved by the government's Human Genetics Commission.²⁷⁵ The controversial practice resulted in some individuals paying higher insurance premiums based on genetic predispositions, creating political pressure to outlaw the use of genetic data by insurers in the United Kingdom altogether.²⁷⁶

While representatives of Norwich Union Life claimed that the genetic tests were not compulsory, simply providing lower premiums for people that do not test positive for genetic tests can lead to rampant genetic testing. An "assessment spiral" will result when one company offers discounts for those with a particular genetic profile, creating pressure on competitors to offer similar discounts in order to keep "low-risk" policy holders and resulting in higher premiums for those that are not tested or do not possess the correct genetic make-up.²⁷⁷ Thus, non-compulsory genetic testing can easily lead to genetic discrimination.

Legal Safeguards

Recognizing the issues implicated in widespread genetic testing, a number of international bodies have recommended that genetic testing should be carefully circumscribed by law. In 1989, the European Parliament issued a resolution recommending legislation to prohibit genetic testing for the purposes of selecting workers or examining employees without their consent. It advised that employees must be informed of any analysis and implications of genetic data before tests are

²⁷⁴ Dana Hawkins, "The dark side of genetic testing: Railroad workers allege secret sampling," United States News, February 19, 2001.

²⁷⁵ Melissa Kite, "Insurance firm admits using genetic screening," The Times, February 8, 2001.

²⁷⁶ T. R. Reid, "Britain Moves to Ban Insurance Gene Tests," The Washington Post, April 30, 2001.

²⁷⁷ See Mark A. Rothstein, "Genetic Secrets: A Policy Framework," Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era, Edited by Mark A. Rothstein (Yale University Press 1997), at 469-70.

carried out and allowed withdraw from testing at any time.²⁷⁸ The Council of Europe has also recommended that “the admission to, or the continued exercise of . . . employment, should not be made dependent on the undergoing of tests or screening.”²⁷⁹ Similarly, the World Medical Association (WMA) has issued statements to this effect. In 1992, issuing a Declaration on the Human Genome Project, it recommended the adoption of laws similar to those that prohibit “the use of race discrimination in employment or insurance.”²⁸⁰ In May 2000, it announced that it would draw up guidelines on the development of centralized health storage databases that will address “the issues of privacy, consent, individual access and accountability.”²⁸¹ In 1997, the United Nations Educational, Scientific and Cultural Organization (UNESCO) adopted a Universal Declaration on the Human Genome and Human Rights, outlining the rights of individuals to control the collection and use of genetic information.²⁸²

In many cases, genetic testing may be indirectly prohibited by existing labor codes.²⁸³ It is also possible that the use of genetic data by employers to discriminate against workers may violate equal opportunity or anti-discrimination laws. In the United States, for example, genetic testing may violate the 1964 Civil Rights Act that prohibits discrimination in employment on the basis of “race, sex, national origin, and religion,” or the Americans with Disabilities Act of 1990, which prohibits discrimination in employment against a “qualified individual with a disability.”²⁸⁴

Governments are also beginning to address the privacy issues directly. In the United States, most laws applying to genetic discrimination, testing or identification have been passed by states rather than the federal government. As of 1997, twelve states prohibit genetic discrimination in employment, 16 states prohibit genetic discrimination in insurance and more than 40 states have

²⁷⁸ European Parliament, “Resolution on the Ethical and Legal Problems of Genetic Engineering,” OJ, No. C.96, April 17, 1989.

²⁷⁹ Council of Europe, Committee of Ministers: Recommendation No. R(92)3 on Genetic Testing and Screening for Health Care Purposes, Principle 6 (a) <<http://www.cm.coe.int/ta/rec/1992/92r3.htm>>.

²⁸⁰ See International Labour Office, Conditions of Work Digest: Worker’s Privacy Part II: Monitoring and Surveillance in the Workplace (1993) 12(1).

²⁸¹ WMA To Draw Up Health Database Guidelines, WMA Press Release, 8 May 2000, <http://www.wma.net/e/press/00_11.html>.

²⁸² United Nations Educational, Scientific and Cultural Organization (UNESCO), “Universal Declaration on the Human Genome and Human Rights,” November 11, 1997 <<http://unesdoc.unesco.org/images/0010/001096/109687eb.pdf>>. Also see “Implementation of the Universal Declaration on the Human Genome and Human Rights: Report by the Director-General,” September 22, 1999 <<http://unesdoc.unesco.org/images/0011/001173/117335e.pdf>>.

²⁸³ See generally, International Labour Office, Conditions of Work Digest: Worker’s Privacy Part III: Testing in the Workplace, (1993) 12(2).

²⁸⁴ Pub. L. No. 101-335 (1990), codified at 42 United StatesC. §§ 1201.

established DNA databases for law enforcement purposes.²⁸⁵ In 2000, President Clinton issued an executive order prohibiting the use of genetic information in federal agency hiring and promotion decisions.²⁸⁶

Workplace Privacy

Workers around the world are frequently subject to some kind of monitoring by their employers.²⁸⁷ Employers supervise work processes for quality control and performance purposes. They collect personal information from employees for a variety of reasons, such as health care, tax, and background checks.

Traditionally this monitoring and information gathering involved some form of human intervention and either the consent, or at least the knowledge, of employees. The changing structure and nature of the workplace, however, has led to more invasive and often, covert, monitoring practices which call into question employee's most basic right to privacy and dignity within the workplace. The progress in technology has facilitated an increasing level of automated surveillance. Now the supervision of employee's performance, behavior and communications can be carried out by technological means, with increased ease and efficiency. The technology currently being developed is extremely powerful and can extend to every aspect of a workers life. Software programs can record keystrokes on computers and monitor exact screen images, telephone management systems (TMS) can analyze the pattern of telephone use and the destination of calls, and miniature cameras and "Smart" ID badges can monitor an employee's behavior, movements, and even physical orientation

Advances in science have also pushed the boundaries of what personal details and information an employer can acquire from an employee. Psychological tests, general intelligence tests, performance tests, personality tests, honesty and background checks, drug tests, and medical tests are routinely used in workplace recruitment and evaluation methods. Since the discovery of DNA there has also been an increased use of genetic testing, allowing employers to access the most intimate details of a person's body in order to predict susceptibility to diseases, medical or even behavioral conditions. The success of the Human Genome Project will likely make this kind of testing more prevalent.

²⁸⁵ Mark A. Rothstein, *Genetic Secrets: A Policy Framework* 456.

²⁸⁶ Executive Order 13145 - To Prohibit Discrimination in Federal Employment Based on Genetic Information, February 10, 2000, available at <<http://www.nara.gov/fedreg/eo2000.html#13145>>.

²⁸⁷ See EPIC's Workplace Privacy Page <<http://www.epic.org/privacy/workplace/>>.

Employers' collection of personal information and use of surveillance technology is often justified on the grounds of health and safety, customer relations or legal obligation. However, according to a recent study of the Privacy Foundation, it is actually the low cost of surveillance technologies, more than anything else that contributes to the increased monitoring.²⁸⁸ In many cases workplace monitoring can seriously compromise the privacy and dignity of employees. Surveillance techniques can be used to harass, discriminate and to create unhealthy dynamics in the workplace.

Legal Background

Privacy advocates have long maintained that providing notice of a monitoring or surveillance policy should, as a bare minimum, be required before employers can engage in such invasive activities. They support strong privacy principles in the workplace such as the International Labor Office's "Code of Practice on the Protection of Workers' Personal Data," which protect employees' personal data and fundamental right to privacy in the technological era.²⁸⁹ These guidelines were issued by the ILO in 1997, following three comprehensive studies on international workers' privacy laws.²⁹⁰ The general principles of the code are:

- personal data should be used lawfully and fairly; only for reasons directly relevant to the employment of the worker and only for the purposes for which they were originally collected;
- employers should not collect sensitive personal data (e.g., concerning a worker's sex life, political, religious or other beliefs, trade union membership or criminal convictions) unless that information is directly relevant to an employment decision and in conformity with national legislation;
- polygraphs, truth-verification equipment or any other similar testing procedure should not be used;
- medical data should only be collected in conformity with national legislation and principles of medical confidentiality; genetic screening should be prohibited or limited to cases explicitly authorized by national

²⁸⁸ The Privacy Foundation, *The Extent of Systematic Monitoring of Employee E-mail and Internet Use*, July 9, 2001 <<http://www.sonic.net/~undoc/extent.htm>>

²⁸⁹ "Protection of workers' personal data," *An ILO Code of Practice*, Geneva, International Labour Office (1997).

²⁹⁰ International Labour Office, *Conditions of Work Digest: Worker's Privacy Part I: Protection of Personal Data* (1991) 10 (2); *Worker's Privacy Part II: Monitoring and Surveillance in the Workplace* (1993) 12(1); and *Worker's Privacy Part III: Testing in the Workplace*, (1993) 12(2).

legislation; and drug testing should only be undertaken in conformity with national law and practice or international standards;

- workers should be informed in advance of any advance monitoring and any data collected by such monitoring should not be the only factors in evaluating performance;
- employers should ensure the security of personal data against loss, unauthorized access, use, alteration or disclosure; and
- employees should be informed regularly of any data held about them and be given access to that data.

The code does not form international law and is not of binding effect. It was intended to be used “in the development of legislation, regulations, collective agreements, work rules, policies and practical measures.” Unfortunately, however, the laws differ greatly from country to country and in some there are few legal constraints on workplace surveillance. In the United States, for example, the courts have typically been slow to recognize employees’ rights to privacy. There has not yet been any satisfactory and uniform determination of what level of privacy employees are entitled to and how that privacy should be protected. Many believe that since employers have ownership or “control” over the working premises, its contents and facilities, and that employees give up all rights and expectations to privacy and freedom from invasion. Others simply avoid the question by making employees consent to surveillance, monitoring and testing as a condition of employment. Legislation has recently been introduced, however, which would prevent employers from secretly monitoring the communications and computer use of their employees.²⁹¹

In European countries, the collection and processing of personal information is uniformly protected by the Data Protection Directive. The 1997 Telecommunication directive, however, provides for the confidentiality of communications for “public” systems and therefore would not cover privately owned systems in the workplace.²⁹² Nonetheless, many European countries, such as Austria, Germany, Norway and Sweden have strong labor codes and privacy laws that directly or indirectly prohibit or restrict this kind of surveillance. In Finland, a new law on Data Protection in Working Life entered into force in October 2001. In October 2000, the United Kingdom Privacy Commissioner

²⁹¹ The “Notice of Electronic Monitoring Act” (S.2898 and H.R.4908), introduced July 20, 2000.

²⁹² Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector (Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997) <<http://www2.echo.lu/legal/en/dataprot/protection.html>>.

issued a draft code of guidance for employer/employee relationships.²⁹³ In March 2002 the first part of this code, on data protection in recruitment and selection of employees was issued.²⁹⁴ Three further parts on employment records, monitoring at work and medical information and testing will be issued over the next few months. In 1999 the Swedish government established a Committee to study workplace privacy issues. In March 2002 the Committee issued a proposal recommending specific legislation to protect the personal information of current employees, former employees and employment applicants in both the private and public sectors.²⁹⁵ In May 2002, the European Union Article 29 Data Protection Working Party issued a working paper on monitoring and surveillance of electronic communications in the workplace. The document set out a list of questions to be asked before any monitoring measure is put in place for example: Is the monitoring activity transparent to the workers? Is it necessary? Could not the employer obtain the same result with traditional methods of supervision? Is the processing of personal data proposed fair to the workers? Is it proportionate to the concerns that it tries to ally? It set out examples of what could be considered as legitimate monitoring activities and acceptance limits of surveillance of employees.²⁹⁶

There have also been developments outside of Europe on this issue. In June 2002, the Hong Kong Data Protection Commission issued a draft a code of practice on workplace for public consultation. The draft code covers telephone, CCTV, email and computer usage and possibly location monitoring.²⁹⁷ In Australia the Privacy Amendment (Private Sector) Act 2000 put in place limited restrictions on employer's monitoring of communications by requiring the establishment of formal email use policies that must be made clear to all employees. It also requires employers to prove that the monitoring of e-mails is justifiable for instance on grounds of excessive use of email, distributing offensive material, suspected criminal activities or passing on sensitive

²⁹³ Data Protection Commissioner, Employment: (Draft COP), October 2000, available at <<http://www.dataprotection.gov.uk/dpr/dpdoc.nsf>>.

²⁹⁴ Data Protection Commissioner, Employment: Part 1: Recruitment & Selection, Employment Practices, Data Protection Code, March 2002, available at <<http://wood.cta.gov.uk/dpr/dpdoc.nsf - 25/02/99>>.

²⁹⁵ The proposal (in Swedish with a summary in English) is available at <http://naring.regeringen.se/propositioner_mm/sou/pdf/sou2002_18a.pdf>.

²⁹⁶ Article 29 Data Protection Working Party, Working Document on The Surveillance Of Electronic Communications In The Workplace, 5401/01/EN/Final WP 55, May 29, 2002, available at <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp55_en.pdf>.

²⁹⁷ Privacy Commissioner for Personal Data, Draft Code of Practice on Monitoring and Personal Data Privacy at Work, (Hong Kong, PCO, 2002), available at <<http://www.pco.org.hk/english/ordinance/codes.html>>.

information.²⁹⁸ However, the legislation grants exemptions to small businesses and the media and also exempts all employee records in any industry sector.

Performance Monitoring

Automated workplace monitoring has become increasingly common in recent years. Even in workplaces staffed by highly skilled information technology specialists, bosses demand the right to spy on every detail of a workers performance. Modern networked systems can interrogate computers to determine which software is being run, how often, and in what manner. A comprehensive audit trail gives managers a profile of each user, and a panorama of how the workers are interacting with their machines. Software programs can also give managers total central control individual PCs. A manager can now remotely modify or suspend programs on any machine, while at the same time reading and analyzing email traffic and Internet activity. A recent report by the American Management Association found that nearly 80 percent of major U.S companies monitor employees at work by checking communications such as telephone conversations, computer files, emails and Internet connections or by using video surveillance for performance evaluation and security purposes.²⁹⁹

An employer can monitor the level of use of a computer through monitoring the number of keystrokes a word processing employee enters in a specified period of time or the amount of time a computer is idle during the workday. Numerous technologies are available which monitor and analyze the performance of IT workers. Some allow network administrators to observe an employee's screen in real time, scan data files and e-mail, analyze keystroke performance, and even overwrite passwords. Once this information is collected, it can be analyzed by standard processing programs to determine a worker's performance profile. These monitoring products are sold at very low prices and have infiltrated the market. These snooping programs have also become popular not just among employers but also law enforcement agencies, private attorneys, investigators, and suspicious lovers.

The use of video cameras and closed circuit televisions (CCTV) is another common way of monitoring employees within the workplace. Even areas where employees would previously have enjoyed high expectations of privacy, such as

²⁹⁸ Helene Zampetakis, "Email snooping almost banned," Information Technology News Service, June 26, 2001 <<http://it.mycareer.com.au/news/2001/06/26/FFXDJRS4DOC.html>>.

²⁹⁹ American Management Association, Annual Survey on Workplace Monitoring and Surveillance 2001, April 18, 2001.

bathrooms or locker rooms, have come under increasing surveillance. The American Civil Liberties Union (ACLU) reports cases of postal workers in New York City finding hidden cameras in the restroom stalls and of waiters in the Boston Sheraton being secretly videotaped in the hotel locker room.³⁰⁰ Where staff are more mobile, companies are now using a range of technologies to track geographic movements.³⁰¹ Some hospitals now require nurses to wear badges on their uniforms so they can be located constantly.³⁰² Advances in this area now allow carrier companies to place an electronic mechanism (described as a geostationary satellite-based, mobile communications system)³⁰³ on trucks that then sends back to a main terminal the exact position of the vehicle at all times. In this way, carrier companies can ensure that no side trips nor other deviations are taken from the prescribed route.³⁰⁴ Wide area systems such as Trackback are in use throughout the United Kingdom.

Telephone Monitoring

Telephone surveillance has become endemic throughout the private and public sector. In the United States, employers have broad discretion to monitor employees' calls for "business purposes." Companies are extensively using telephone analysis technology. Call center workers for British Telecom are regularly presented with a comprehensive analysis sheet, showing their performance relative to other workers. Airline reservations clerks in the United States and elsewhere wear telephonic headsets that monitor the length and content of all telephone calls, as well as the duration of their bathroom and lunch breaks.³⁰⁵ In one instance, telephone calls received by airline reservation agents were electronically monitored on a second-by-second basis: agents were allowed only 11 seconds between each call and 12 minutes of break time each day.³⁰⁶ Other airline agents have complained that they are evaluated based on how many times they use a customer's name during a call or how often they try to overcome a customer's initial objections to buying a ticket.

³⁰⁰ ACLU, Workplace Rights, Electronic Monitoring <<http://www.aclu.org/library/pbr2.html>>.

³⁰¹ Laura Pincus Hartman, "The Economic and Ethical Implications of New Technology on Privacy in the Workplace," *Business and Society Review*, March 22, 1999.

³⁰² "Monitoring Shrinks Worker Privacy Sphere," Eric Auchard, Reuters, May 29, 2001.

³⁰³ "Bulkmatic Equips Fleet with OmniTRACS System," Qualcomm Press release, December 19, 1996. <<http://www.qualcomm.com/Press/pr961219c.html>>.

³⁰⁴ Qualcomm Press release, December 19, 1996.

³⁰⁵ Laura Pincus Hartman, "The Economic and Ethical Implications of New Technology on Privacy in the Workplace," *Business and Society Review*, March 22, 1999.

³⁰⁶ Charles Pillar, "Bosses with X-Ray Eyes," *MacWorld*, July 1993.

The level of sophistication of telephone surveillance systems can be astonishing. Some systems can record all transactional activity on a phone, together with destination numbers and times. Other technology can then process and analyze this data. A British program called “Watcall,” produced by the Harlequin company, can analyze telephone calls and group them into “friendship networks” to determine patterns of use.³⁰⁷ Voice mail systems are also subject to systematic or random monitoring by managers. Most new systems have default pass codes for administrators, and these can open all message boxes.

E-mail and Internet Use Monitoring

Computers and networks are particularly conducive to surveillance. The Privacy Foundation study (above) found that 14 million employees in the United States are subject to this kind of surveillance on a continuous basis. This number obviously increases dramatically when random surveillance checks are included. Employers can monitor e-mail by randomly reviewing e-mail transmissions, by specifically reviewing transmissions of certain employees, or by selecting key terms to flag e-mail. In the latter case software analyses a company’s entire e-mail traffic phrase by phrase, and draws conclusions about whether a message is legitimate company business. It can be instructed to search for specific keywords and “damaging” phrases. Some programs can even use algorithms to analyze communications patterns and turn them into images. Monitors can then look at these images to follow traffic patterns and detect whether sensitive data is at risk.

Many employers rely on software for remote monitoring of e-mail messages. With a few clicks they can see every e-mail message that employees send or receive and determine whether they are “legitimate” or not. Managers give a variety of reasons for installing such software. Some say it is to protect trade secrets or preventing sexual harassment incidents. Others want to prevent oversized-mails clogging networks and using too much bandwidth. Others simply don’t want employees “wasting” company time by using the systems for personal activities. In an ideal world, this monitoring should follow the conventional format, i.e., identical to the quality check that has applied to correspondence sent out on company letterhead. However, the speed and efficiency of e-mail means that digital communication involves a vast intersection with personal correspondence. It also has features more in common with an internal memo, for which there has always been less monitoring and management.

³⁰⁷ Simon Davies, “Watch out for the Old Bill,” Daily Telegraph, April 29, 1997.

According to the American Management Study (above) nearly two thirds of all companies discipline employees for abuse of email or Internet connections and 27% dismiss employees for those reasons. In 2000, Dow Chemical Company in the United States fired 50 employees and threatened 200 others with suspension after they found “offensive” material in their e-mail. The company opened the personal e-mail of more than 7,000 employees.³⁰⁸ Similarly, the New York Times fired 23 employees in 1999 for sending “obscene” messages.

These cases raise complex legal and ethical questions concerning an employee’s fundamental right to privacy and due process. What if employees are sent “offensive” e-mails by accident or maliciously? The e-mail cannot simply be deleted. It remains logged on the company server, threatening the relationship of trust between employee and management. Or what if an employee is dismissed on the grounds of sensitive personal information (for example relating to sexual preferences, a medial condition, etc.) gathered through a system? This problem also arises when companies monitor all Internet activity looking for visits to “inappropriate” sites. At first sight, such surveillance has elements in common with traditional surveillance for hard copy pornography, but there are significant dangers to workers in the realm of electronic surveillance. The use of spam e-mail to advertise X rated sites results in workers entering sites that appear to be quite benign. Or websites may be accidentally visited when displayed as a “hit” in response to a perfectly innocent search query. The surveillance technology does not, however, distinguish between an innocent mistake and an intentional visit.

The monitoring of chat room visits has also created some distress in the workplace. There is an increasing trend among companies to dismiss and/or sue employees for divulging company “trade secrets” or defaming the company in chat rooms. These have become known as “John Doe” cases. As most people log on to chat rooms anonymously or using an alias, once a company observes a certain party in a chat room engaging in “illegitimate” speech, they must subpoena the message-board services such as Yahoo or America Online, to obtain the identify the specific author. The service providers often turn over identifying information when presented with a subpoena without any notice to the individual. The number of these cases is rapidly increasing and threatens not only the privacy of employees but also their rights to anonymity and free speech.

308 ‘Dow Chemical Fires Employees Over Inappropriate E-mails’, ABCNEWS.com, July 27, 2000.

Drug Testing

There is also an increasing amount of drug testing in many countries. The number of companies using these tests has risen proportionately with the decreasing costs of the tests. For many employees, drug testing is now a standard part of working life. Companies routinely administer tests in the recruitment stage or at intermittent periods during employment even where there is no evidence of misconduct, poor performance or any other reason to suspect drug use. There are thousands of easy to use kits, which can detect traces of drugs within minutes and without the need for a laboratory, available on the market today. Most of these tests analyze hair or urine samples to detect traces of drugs such as amphetamines, marijuana, cocaine, opiates and methamphetamines.

The issue of wide scale “preventative” drug testing raises a whole host of questions concerning privacy, bodily integrity, freedom and the presumption of innocence. The process of testing itself can be hugely invasive. Observers are often present to prevent employees tampering with samples. In the case of urine testing this can be particularly offensive. Consider the case of one employee who wrote:

I waited for the attendant to turn her back before pulling down my pants, but she told me she had to watch everything I did. I am a 40-year-old mother of three: nothing I have ever done in my life equals or deserves the humiliation, degradation and mortification I felt.³⁰⁹

This type of test can quickly turn from a necessary evil needed to protect lives and reputations to intimidation and harassment. It raises questions about whether the benefits to employers really outweigh the rights and dignity of workers. Manufacturing companies wishing to sell their products obviously claim they can. They extol the advantages of drug tests, claiming they can save employers thousands by reducing incidences of absenteeism, low productivity, accidents, injuries, compensation and health care claims. Governments generally have also encouraged testing as part of a larger war on drugs. What employers are not told, however, is that there are also numerous ethical and economic disadvantages to drug testing.

Drug testing fosters a climate of negativity based on suspicion and secrecy rather than trust, openness and respect. Low morale or resentment among workers may

³⁰⁹ From a letter to the American Civil Liberties Union describing a workplace drug test. See, ACLU, Drug Testing: A Bad Investment, September 1999 <<http://www.aclu.org/issues/worker/drugtesting1999.pdf>>.

consequently lead to low productivity or profits. In addition, even though individual tests may no longer be expensive, because they are so sweepingly administered among employees, they may be costing employers far more than they are saving them. Catching one or two light drug users for every few thousand people tested is hardly an economical justification for the initial outlay. Even if tests do reveal traces of drugs there is no clear evidence to suggest that mild drug use has a greater effect on productivity than, for example, alcohol. Dismissing workers on grounds of policy and suspicion rather than performance and proof, may result in the loss of valuable employees to the employer. Testing does not involve good management policy. Evidence has not shown that drug testing can deter future use, and it is in no way a substitute for proper guidance, support and counseling. In fact, in an ironic twist, routine testing may even encourage more serious drug usage among employees. As one commentator says:

If one wants to get inebriated on a Friday night and still pass a urine test Monday, smoking a joint would be foolish. Cocaine and alcohol would represent the “safer” choices of intoxicants because alcohol is “legal” and cocaine cannot be detected in the body as long.³¹⁰

Finally, drug testing is inaccurate and can often lead to false and misleading results. A report by the Ontario Information and Privacy Commissioners’ Office says up to 40 per cent of tests are inaccurate.³¹¹ Highly sensitive tests can be positive even when the drug sought is not present. Some say positive reactions may result from a carry-over following a strongly positive earlier or from human error, such as contamination due to failure to cleanse equipment.³¹² Others note that certain legal substances can also result in positive tests for illegal drugs. For example, there have been reports of Vicks inhalers resulting in positive tests for amphetamines and methamphetamines, standard anti-inflammatory drugs like Ibuprofen showing up positive on marijuana tests, and even traces of morphine being detected from poppy seeds.³¹³

310 Ethan A. Nadelmann, "Drawing the Line on Drug Testing". IntellectualCapital.Com, October 14, 1999, available at <http://www.lindesmith.org/library/ethan_drugtesting2.html>

311 Information and Privacy Commissioner/Ontario, Workplace Privacy: The Need for a Safety-Net, November 1993. <http://www.ipc.on.ca/english/pubpres/sum_pap/papers/safnet-e.htm>

312 Morgan, John P. "Problems of Mass Urine Screening for Misused Drugs." *Journal of Psychoactive Drugs*. Volume 16(4) (1984): 305-317. available at The Lindesmith Center - Drug Policy Foundation <<http://www.lindesmith.org/library/grmorg2.html>>

313 National Academy of Sciences, "Under the Influence? Drugs and the American Work Force," 1994. Also, ACLU, Drug Testing: A Bad Investment, September 1999. <<http://www.aclu.org/issues/worker/drugtesting1999.pdf>>