doc
CA1
EA752
2001R26
ENG

Canadian Centre
For Foreign Policy
Development

Centre canadien
pour le développement
de la politique étrangère

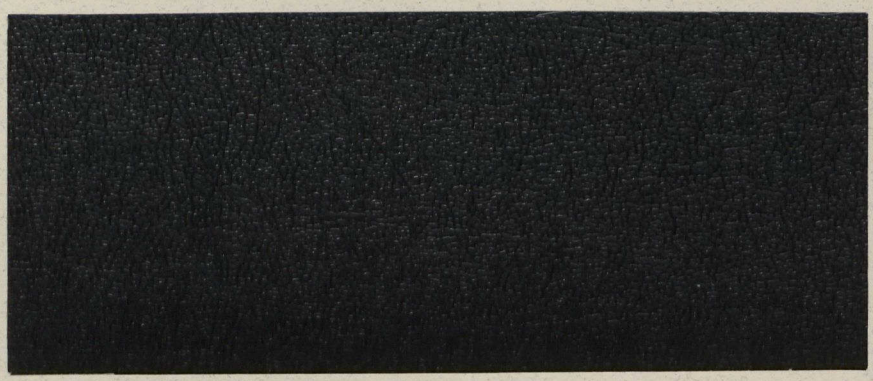
REPORT FROM THE ROUNDTABLE: PRIVACY, SOVEREIGNTY AND TECHNOLOGY

Marketa Geislerova,
Canadian Centre for Foreign Policy Development

March 23, 2001
Ottawa, Ontario

3008.8E

125 promenade Sussex Drive, Ottawa, Ontario K1A 0G2
Telephone/Téléphone : **613 944 8278** Fax/Télécopieur : **613 944 0687**
www.cfp-pec.gc.ca



CAI EA752 2001R26

Canadian Centre for Foreign Policy Development

Centre canadien pour le développement de la politique étrangère

125 Sussex Dr. Ottawa, Ontario K1A 0G2

REPORT FROM THE ROUNDTABLE: PRIVACY, SOVEREIGNTY AND TECHNOLOGY

Marketa Geislerova,
Canadian Centre for Foreign Policy Development

March 23, 2001
Ottawa, Ontario

3008.8E

6223218

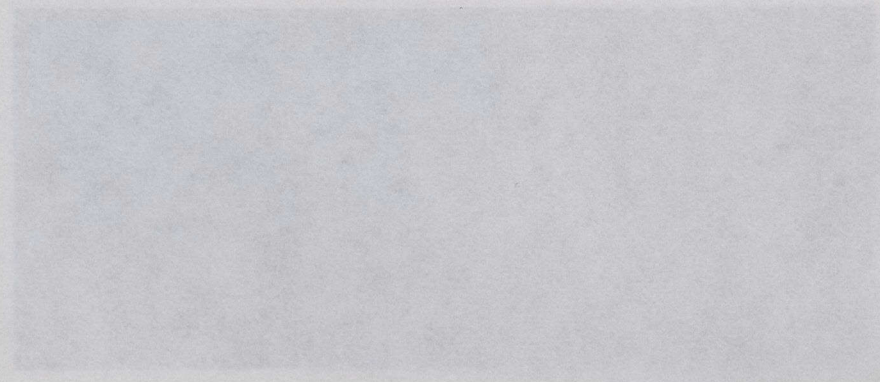
Dept. of Foreign Affairs
Min. des Affaires étrangères

AOUT AUG 2 8 2001

Return to Departmental Library
Retourner à la bibliothèque du Ministère

ISBN: 0-662-30863-8
E2-406/2001E

Tel.: (613) 944-8278
Internet address: http://www.cfp-pec.gc.ca Fax: (613) 944-0687



Dept. of Foreign Affairs
Min. des Affaires étrangères

AUG 2 8 2001

Return to Departmental Library
Retourner à la bibliothèque du Ministère

REPORT FROM THE ROUNDTABLE: PRIVACY, SOVEREIGNTY AND TECHNOLOGY

March 23, 2001
Ottawa, Ontario

On March 23, 2001, the Canadian Centre for Foreign Policy Development, in partnership with the International Crime Division of the Department of Foreign Affairs and International Trade, organised a roundtable on Privacy, Sovereignty and Technology. Experts, NGOs, business representatives and government officials met to discuss the changing concepts of privacy and sovereignty and to examine efforts to protect privacy from potential abuses. Participants included Liss Jeffrey (University of Toronto), Ann Cavoukian (Ontario Information and Privacy Commission), Scott Martin (The Personalization Consortium), and Terry Cormier (Director, International Crime Division, DFAIT). Steven Lee (Canadian Centre for Foreign Policy Development, DFAIT) chaired the meeting.

The report is divided into two main sections:

Key recommendations included:

Canada could take a lead on creating a global *Charter of Information Rights and Responsibilities,* drawing on relevant sections of the Canadian Charter of Rights and Freedoms and existing privacy legislation.

There is a need for an inclusive debate on privacy issues and instruments for deterring threats to privacy. The government should play a key role in mobilising Canadians and alerting them to the possible privacy threats they face. New technology and the power of networking could be used to get consultations underway.

1. Presentations

1.1. Times and Technologies in Flux: Rethinking Identities, Sovereignty and the Networks of Nations, Liss Jeffrey (McLuhan Program in Culture and Technology, University of Toronto)

Liss Jeffrey examined the concepts of privacy and sovereignty in the context of rapidly advancing technology. She said that new technology profoundly alters how we live on structural as well as individual levels. On a structural level, cultural, political, social and economic systems are in flux. New extraterritorial networks of nations, communities and individuals have emerged, challenging the traditional understanding of territorial boundaries, citizenship, jurisdiction and identity. Sovereignty may or may not correspond to our territorial borders, bringing forth questions including: What laws, rules and regulations can the Canadian government enforce and how? How is extraterritorial jurisdiction determined or, in other words, who rules cyberspace?

On an individual level, a shift in the "sense of the self" has occurred as a result of the growth of Internet and networking. The individual can be effectively posited *in relation* to a network, creating a new "geopolitical" dynamic explored in detail by Manuel Castells in *The Information Age: Economy, Society and Culture* (1996, 1997 and 1998).

The concept of privacy has been shifting as a result of these broad political, cultural and socio-economic changes. Privacy could be perceived:
- in terms of identity
- as an element of a person's security and by extension also global security
- as a cultural value within a broader context of values, including trust

This fast changing environment provides a fertile ground for what Jeffrey calls a "rogue" element – an unpredictable individual (hacker) who poses a threat to the network, a computer system, or the state. Mafia boy is a prime example of this phenomenon. Another example of a new threat is provided by the Ahmed Ressam case. The case fuelled the fears of many Canadians and Americans about the "sense of threat from the outside." Many observers were surprised by the ease with which Mr. Ressam used a forged passport to enter Canada and plan for terrorist activities in the U.S.

While the new environment and threats affect nearly everybody, discussion about how to address new challenges and ensure our safety/security has been restricted to government officials and a few experts. A more inclusive debate should take place. Among other matters, the schizophrenic attitudes exhibited in Canada and other countries, where "Orwellian fears"concerning the potential for invasive surveillance and criminal use of technology co-exist with an apathy about privacy, should be addressed. The debate should include other questions such as:

- How to ensure that the cure for threats to both, sovereignty and privacy, is not worse than the disease?
- How many of our rights to privacy are we prepared to give up to business for profit, to the state for law enforcement purposes, to our fellow citizens for "entertainment?"
- What are the tools needed to create a balance between deterring legitimate threats and ensuring our fundamental freedoms (i.e., freedom of thought, belief, opinion and expression), legal rights (i.e., rights related to search and seizure), diversity and culture?

Finding answers to the last question is particularly pertinent. The right balance is key in reconfiguring social relations and structures to fit new realities, which are mostly technologically determined. *In order to find a right balance between deterrence to threats and freedoms/rights, trust is essential.* Lack of trust interferes in e-commerce, for instance (i.e., willingness to use credit cards over the Internet). Trust allows societies to make tough choices and is crucial for social cohesion. One may perceive trust in cyberspace as giving up personal privacy. Therefore, among the key challenges today is to counter the declining levels of trust. A *Charter of Information Rights and Responsibilities* could be instrumental in creating this much needed balance, while addressing questions concerning trust. However, ensuring that our environment is safe and secure involves more than just the police. Civil society, government and business all should be included in the discussions on the domestic as well as the global level. On a related note the digital divide is not only about access, but also inclusion.

1.2. New Threats to Privacy and Sovereignty, Reg Whitaker (York University)

Reg Whitaker suggested that the threats to privacy and sovereignty posed by new technology are analogous for both the state and an individual. New technology poses threats to the boundaries of both states and individuals. The sovereignty of states is diminishing at the same time as individuals' private space is shrinking. As a result, new geopolitical and social structures are developing.

The retreat of the "Big Brother State" coincides with the advancement of new technology – paradoxically, a key tool in any state's surveillance toolbox. Money-flows are decentred. Networking has become a new paradigm. Meanwhile, state power has been "displaced" to the private sector and to society. *This displacement has meant that "coercion"– the traditional tool of social compliance, has shifted to a new form – "consent."* Increasingly we can see the use of positive inducement, with exclusion as a punishment, to generate consent. This "voluntary complicity" gives the emerging system a degree of resiliency higher than that afforded by the coercion-based system.

The displacement of state power has also contributed to a new, rather disconcerting, trend: *People are treated more as consumers than citizens, their consumer preferences and behaviour are closely monitored and profiled by governments themselves, by private companies, or by private companies hired by governments.* In a sense, capital has contributed to the elimination of public and personal space.

There are three categories of responses to protect privacy in the context of the emerging social structures. All of these categories treat personal information as a commodity. As a result, questions of ownership, control, and use are all defined in consumer terms. They include:

1. Do it yourself – requires the adoption of technology to fight threats posed by technology.
2. Industrial self-regulation – the private sector sets rules it voluntarily accepts to play by (under the threat of litigation if the established rules are violated). Microsoft, for instance, has adopted this approach. It plays a gate-keeper role, not only to protect its system, but to head-off a potential threat of government regulation. This approach is common in the U.S.
3. Government regulation – an approach more common in Europe and in Canada.

Privacy, perceived as "me against the state or society," ignores the safety and the well being of a community. *The good of the community (i.e., Internet free of child pornography) needs to be balanced with an individual's right to privacy.* In order to build a healthy community, individuals have to forfeit some of their rights.

The control states commanded over capital flows, the licit economy (i.e., fiscal and monetary policy), the illicit economy, service standards and delivery (i.e., national standards), migration, ideas and images, have all diminished significantly. The ability of the state to censor has also declined. No single state is capable of managing the range of borderless threats that exists today. However, there are five key global strategies to cope:

1. enhanced cooperation among states (while international cooperation may be difficult to achieve, states with large markets *can* impose decisions),
2. resource pooling,
3. information sharing,
4. enforcement mobilisation,
5. shifting partnerships with non-state actors.

Reg Whitaker addressed three additional points related to coping strategies:

1. The coping strategies should operate on the same level as the threats. In doing so, boundaries will be effectively reconstituted.
2. Some technology that enables threats can be used to inhibit them, if used collectively.
3. Paradoxically, states must give up some measure of their sovereignty in order to protect sovereignty.

1.3. Challenges for International Cooperation: How are Norms Created? Terry Cormier (International Crime Division, DFAIT)

Terry Cormier addressed the creation of new norms at the global level. There has been a growth in international crime as a result of globalization. The digital environment facilitates the growth of international crime and offers new challenges to law enforcement. It also brings new threats to privacy. The state has a responsibility to counter these trends. He stressed the need for a coherent strategy and a coordinated approach.

Privacy should be perceived as a value. Equating privacy with security and in extension with sovereignty, Terry Cormier said that rights to privacy should be protected from new trans-border threats. Several important questions need to be addressed in this context including: Who should protect the rights to privacy? What is private in a borderless digital world? How is state power affected by new technology?

Canadian foreign policy in this area has four key objectives:
1. projecting Canadian values abroad
2. reflecting domestic priorities
3. forward-looking identification of new threats
4. managing ongoing issues.

Building norms includes questions such as, for instance: How should issues be put on the agenda? Should they be put forward by the private sector, civil society, individuals, or the state? Whose agenda is it? Does it belong to Canada, other Western states, or communities of internet providers? How to secure law enforcement, judicial and political cooperation?

Types of norms include:
- binding international laws
- non-binding international laws
- voluntary codes of conduct for industry
- statements of principle
- Resolutions of the Security Council
- the body (history) of existing norms.

Norm setting is relatively fast. Conventions, such as the global Convention against Transnational Organised Crime were negotiated and signed fairly quickly. Setting norms involves six main

steps:
1. identify problem
2. gather information
3. identify common parameters
4. identify partners
5. develop shared understanding
6. sell the norm (selling the norms requires a shared understanding, allies, and discussion fora)

A set of dilemmas should be addressed in the process of consultation and negotiation, they include:
- Who to consult (everybody has a stake in privacy issues)?
- How to balance competing perspectives and values?
- How to ensure public accountability and transparency (for which demand has grown)?

International challenges for Canada include:
- finding partners
- squaring different cultural parameters
- squaring different criminal justice systems
- defining crime
- building multilateral coalitions, such as the G-8 (this becomes particularly important because perpetrators can target more than one country at once)

There are many variables during the negotiating period. One must expect that ideas will be pushed back and should be flexible. He raised the importance of a multilateral approach and highlighted the need for international judicial and law enforcement cooperation.

The Canadian government should play a key role for several reasons:
- Constitutional (binding agreements require government involvement)
- Charter of Rights
- to protect Canadian interests
- to project Canadian values
- to develop consensus

Possible outcomes include:
- domestic law
- political will
- ongoing review of Multilateral Evaluation Mechanism (MEM)
-Transnational Organised Crime Convention

In conclusion, he stressed the need to:
- protect ourselves from threats posed by the "dark side of globalization"
- tackle international crime on the international level
- support international discussion on what privacy means as a value

- focus on what the next steps are.

2. Discussion

2.1. The Concepts of Privacy and Sovereignty

Two dichotomies emerged during the discussion on privacy:

1. Tangible privacy *versus* intangible privacy

A point was made that a distinction should be made between tangible and intangible privacy. While the former refers to the security of a private space (i.e., home), the latter refers to a commodity (i.e., a piece of information which can be sold for entertainment). The attitude of the Canadian public towards privacy was described as schizophrenic because there seems to be a desire for disclosure of intangible privacy, as the number of people watching the Oscars, for instance, indicates. The opposite is true for tangible privacy. *Therefore, it would appear that as a commodity, privacy is not inherently valuable.*

2. Consumer privacy *versus* citizen privacy

Reg Whitaker drew attention to the dichotomy between consumer privacy and citizen privacy. Following up on his presentation, he highlighted the fact that citizens are active participants in public governance (through various organisations or associations, for instance) and help shape the system. He reiterated that the emerging social structure in the West does not facilitate participation, instead the state itself treats citizens as passive consumers who buy into whatever is already cooked-up for them. The system is formidable because instead of simply putting up with it, as before, people actually buy into it. The "sign or die" element of many contracts underlines the point about the lack of choice rather well. There is undoubtedly a "voluntary involuntary transfer of information" to banks, for instance. But the complicity inherent in the new system is deeper. "We are agreeing to work within the system and in extension, to being treated as consumers." The "citizen as a consumer" perspective obfuscates the need for having a public persona, he said. There is a danger that today, people live in anonymity, without a shared history.

Balancing privacy and concerns such as having a "healthy" community is key. Privacy should be redefined and thought about more as a social right that contributes to democratic citizenship. People need private space in which they can develop themselves in relation to the society that in turn impacts on this development.

Two other important observations were made about privacy:

1. Privacy could be defined as "invented" and, therefore, culturally relative. Privacy has evolved to become meaningful.

2. While protecting privacy may contribute to (national and private) security, it does not equate security, as Terry Cormier indicated.

The concept of sovereignty was also briefly addressed. Some said that sovereignty is still not fully appreciated in the context of Internet and networking. Questions to consider include: Where does jurisdiction and sovereignty start and end? Who is running cyberspace? Is cyberspace American?

2.2. Agency

The participants discussed the degree of agency an individual has over information. In this context some suggested that a distinction is made between a situation whereby privacy is forgone with sanction and a situation where information is obtained surreptitiously or by force of law. On the one hand, there are many instances where people give away information if the "price is right." On the other hand, concerns about privacy are high when mail is opened and e-mail monitored by the police.

These conflicting attitudes to privacy rights could be countered by ensuring that Canadians are in control of the information they give and that they have venues to redress misuse. However, this may be difficult to achieve. The challenge in attempting to see one's own credit records may demonstrate the point aptly. In the absence of a standard, "sign or die pressure" is exhorted on individuals in countless situations including, signing hospital admission forms or loan agreements.

A point was made that the decision whether private information is used for commercial purposes should rest with the individual, rather than the state or a private business. "Many Canadians actually wish to exchange their private information for something they value" (i.e., providing personal information in order to get a tailored service). Others pointed out that some people "agree" to sell their organs as well, suggesting that, just as selling organs, privacy issues are not simply reducible to consent.

Some suggested that uninformed consent effectively amounts to coercion. Others pointed out that informed consent could be interpreted as a "notice," in the context of a "sign or die pressure." Yet another point was that consent is a valid term, provided a choice was given.

2.3. Public Engagement

Some participants suggested that many Canadians do not fully understand the value of information they give away (i.e., the way behavioural information could be profiled and used) and the threat of "rogue" entities. Moreover, ongoing global level negotiations on issues related to privacy and sovereignty, including cybercrime, are closed to the public. NGOs and civil society in general are unlikely to be admitted to state fora (UN, OSCD, Council of Europe)

addressing privacy and international crime issues.

Some suggested that there is a need to get the public more engaged. Broad social endorsement and input are needed in order to build new norms. The government should play a key role in mobilising Canadians and alerting them to the possible privacy threats they face. Others said that a dominant government role is unlikely due to limited resources. Moreover, there is not much the government can do if the public does not show interest. So far, there has not been a ground-swell of interest concerning privacy issues. Nonetheless, a campaign on the line of Mothers Against Drunk Driving, could be effective. New technology and the power of networking could be used to get consultations underway.

A survey of privacy laws across different countries demonstrates the importance of public engagement in global level negotiations rather well. The survey showed a dismal record when it came to governments upholding privacy laws (for instance, the survey indicated that the Swedish government was wiretapping leftists for decades), leading some to conclude that "the debate includes no honest brokers."

A point was made that since the issues affect the lives of nearly everybody, it is difficult to determine who to consult, how, and with what objectives in mind.

2.4. The Role of Trust

The participants largely agreed that in order to find the right balance between deterrence to threats and freedoms/rights, trust is essential. Some suggested that to develop trust, inequalities in wealth and power have to be addressed and an open, inclusive discussion launched. Building an agreement at home and gaining trust of young people is essential not only to questions related to privacy, but also to the fabric of Canadian society.

Distrust is related to a lack of legitimacy of public institutions as well as the corporate sector. In the latter instance, the rise of internet has allowed the private sector to surreptitiously collect and use information without the knowledge of the public.

Some participants suggested that the motto "trust no one" is perhaps the most adequate under the current circumstance. Others said that while finding trust may be difficult, it is "out there." Building trust requires due process and a transparent justice system. Today, there is no due process in the private sector, where personal data is treated as an exchange commodity.

2.5 Modes of Regulating Privacy

A metaphor was made comparing the West with ancient Greece before it disintegrated due to the lack of social, cultural, and legal cooperation among city states. Just like the West today, ancient Greece was linked primarily by trade and commerce. While economic interdependence deepens, there is a lack of standardisation of policy on trans-boundary issues, such as sexual exploitation

of children. Common norms and parameters are hard to develop even among developed industrialised countries. *In order to prevent a similar fate to that of ancient Greece, efforts should be made to set baseline standards and bridge jurisdictional boundaries.*

Some participants said that finding the balance between deterrence to threats and freedoms/rights is not new. The dilemma comes especially into focus when weighing law enforcement against freedoms/rights. There is an acceptable latitude for legitimate law enforcement rooted in a general understanding that rights are not absolute. *The real question is how to effect containment on a law enforcement latitude. Determining containment is perhaps best done on a case by case basis.*

A point was added that there exists no adequate oversight of enforcement at the domestic level, and none at all at the global level. *Transparency should be enhanced to reduce the risk of plummeting trust.* Some said that the presence of an oversight mechanism is sometimes as valuable as oversight itself. In other words, the threat of punishment is an effective compliance tool.

A set of privacy principles:
1. Notice. The notice provides customers with clear and conspicuous notice of information practices, including what information is collected, how it is collected, held, shared and used. It may include:
- transparency of data collection
- methods for collecting information both, directly from individual customers and from 3rd parties
- what information is retained and for how long
- whether or not information is combined from multiple sources
- whether or not information is disclosed to other parties.

2. Relevance. Only that information which is necessary to perform a specified set of tasks is collected.
3. Security. All information is safeguarded with appropriate security methods and technologies.
4. Choice. Consent through notice and an opportunity to opt-out or explicit permission obtained in advance will be sought in advance of collecting, holding, using or sharing information.
5. Sensitive Information. Without expressed and informed consent, sensitive information will not be shared.
6. Access and Accuracy. Reasonable access to information will be offered to the owners of that information, subject to legal, technological or security constraints. Reasonable efforts will be made to give owners the opportunity to correct or delete information and keep it accurate.
7. Discrimination. Discrimination on the basis of collected information should be prevented.

Two views emerged about how to best regulate privacy:
1. Combination of self regulation and government regulation (i.e., combining Ethical Information Management with litigation)
2. Government regulation

Some participants suggested that self regulation could adequately meet privacy requirements if a set of privacy principles is observed, under the threat of litigation. A suggestion was made that *Ethical information management could include 3rd party audits*. Auditors would examine how a firm handles information and give a seal of approval when it does so ethically.

There was a general agreement that self regulation is not enough and that a "stick" is required to enforce privacy rights in the form of fines or damaged reputation. Participants endorsed partial self regulation. "More things can be achieved with a smile and a gun than a smile alone."

A point was also raised that technology does not have to be privacy-invasive. Instead, technology could be made privacy-protective and reveal much less.

Some participants said that the free market approach to regulating privacy is insufficient. The sheer strength of the U.S. market makes the free trade argument false. Rather than operating on the same playing field with the U.S., Canadian markets are dominated by the U.S. This trend is a part and parcel of our loss of sovereignty to the private sector. Consumer data is not benign. Profiles of Canadians can easily be set-up on a commercial basis by private companies. People do not have time to understand all the intricacies related to privacy and sovereignty issues. Moreover, which computer system to use to address them? *It is government's responsibility to sign international covenants that deter privacy and sovereignty-related threats.*

Others raised caution, asking where to draw the line of government involvement before it becomes paternalistic, or even worse, totalitarian. They pointed out that governments are not neutral, their decisions are affected by lobbying, for instance. At the same time, regulation of information is necessary to ensure that it is accurate and real. Moreover legislation has to be developed aimed at protecting the little guy, since power relationships play a big role in how privacy is treated. A proper balance between self regulation and government regulation has to be found. In order to find this balance the question whether the government is a threat or a safeguard should be addressed.

2.6. Tools for Regulating Privacy

Some said that legislation dealing with privacy already exists including the Canadian Charter of Rights and Freedoms, the Privacy Act, private sector legislation, EU, OECD, Safe Harbours, etc.. Rather than creating new Charters, efforts should be made to enforce the existing instruments. Moreover, existing instruments may be weakened if yet another instrument is to be negotiated and implemented.

Others emphasised the need for a Charter of Information and Responsibilities with a consolidated set of principles, going beyond privacy to include access (i.e., the digital divide). Before developing ethical information management on a case by case basis, a Charter could serve as a framework, addressing how information is collected, housed, and manipulated. *Canada could take a lead on creating such an instrument, drawing on the relevant sections of its own Charter of Rights and Freedoms and other privacy legislation. While in the U.S. the perception that the state is an enemy may dominate, Canadians have a more balanced view. This may contribute to a synergy among civil society, business and the government and could create a balance between individual rights and corporate goals.*

Legislation to prosecute crimes such as sex exploitation of children and child sex tourism also exists in Canada. However there has not been one case prosecuted yet because procedures are too complicated. We need to relinquish some of our rights to help catch criminals.

Some participants cautioned that the Cybercrime Treaty could actually interfere with the Canadian Charter. The charter sets higher standards than the Treaty. In this way, treaties may be used to lower existing legal or even constitutional protections.

International cooperation for criminal activity could be hindered by legal systems of individual countries. For instance, during the consultation process leading to the creation of the Competition Act, it became clear that confidentiality arrangements in Canada do not necessarily exist in the countries with which Canada shares its information.

The Chair concluded the roundtable by thanking all the participants. He summarised key points of the discussion and emphasised the importance of the discussion around citizens vs consumers - or the transition from citizen to consumer. He suggested that this analysis and perspective might be especially useful to explore in the context of the North American Free Trade Agreement (NAFTA) and other trade agreement generated policy developments. He also drew attention to the changing nature of sovereignty over time. Initially, sovereignty was vested in God. Later on it shifted to the Church, the Absolute Monarch, and the elites. Today, sovereignty is vested in the nation state and in some cases "the people." Just as before, the concept may well prove transitory, Steven Lee said. He closed the session by encouraging further cooperation among the participants.

Privacy, Sovereignty and Technology

List of Participants

March 23, 2001

Brian O'Higgins
Vice President
Entrust Technologies

Stephanie Perrin
Chief Privacy Officer
Zero Knowledge Systems USA

David Banisar
Deputy Director
Privacy International Washington Office

Sarwar Kashmeri
CEO and Publisher
ebizChronicle.com

Peter Hope-Tindall
President and CEO
dataPrivacy Partners

Christopher Taylor
Senior Vice President
Law and Regulatory Affairs
Canadian Cable Television Association

Scott Martin
Vice President
CRM and Alliances/Critical Mass
Founder and President
The Personalization Consortium

Kathleen Priestman
Public Interest Advocacy Centre

Patrick Sullivan
VP of Privacy and Information Policy
Guardent (USA)

Barbara McIsaac
Lawyer
McCarthy Tétrault

Reg Whitaker
Professor
Department of Political Science
York University

Liss Jeffrey
Professor
McLuhan Program in Culture & Technology
University of Toronto

Ron Deibert
Professor
Department of Political Science
University of Toronto

David Hicks
Professor
Department of Criminology
University of Ottawa

Lesia Stangret
National Post Correspondant

Ann Cavoukian
Commissioner (Ontario)
Information and Privacy Commission

Heather Black
General Counsel
Office of the Federal Privacy Commissioner

David McKendry
Commissioner
Canadian Radio-Television and
Telecommunications Commission

Rosanne McKay
Strategic Policy and Planning Branch
RCMP

John Schmidt
Assistant Director, Planning
Financial Transactions and Reports Analysis
Centre of Canada (FINTRAC)

Joanna Leslie
Privacy Coordinator
FINTRAC

Erin McKey
Counsel
International Assistance Group
Department of Justice

Denis Kratchanov
Senior Counsel / Director
Information Law and Privacy Section
Department of Justice

Donald K. Piragoff
General Counsel
Criminal Law Policy Section
Department of Justice

Gareth Sansom
Senior Cryptography Analyst
Criminal Law Policy Section
Department of Justice

Ken Huband
Consultant, Privacy Policy
Industry Canada

Jane Hamilton
Policy Analyst, E-Commerce Policy
Industry Canada

Gregory Edwards
Analyst
Canadian Security Intelligence Service

Jerry Shelest
Senior Analyst
Solicitor General Canada

Pierre Labelle
PolicyAnalyst
Solicitor General Canada

Terry Cormier
Director
International Crime Division
DFAIT

Reid Cooper
International Crime Officer
International Crime Division
DFAIT

Dan Purdy
International Crime Officer
International Crime Division
DFAIT

Steven Lee
Executive Director
Canadian Centre for Foreign Policy Development

Marketa Geislerova
Rapporteur
Canadian Centre for Foreign Policy Development

Canadian Centre
For Foreign Policy
Development

Centre canadien
pour le développement
de la politique étrangère

125 promenade Sussex Drive Ottawa, Ontario K1A 0G2

SELECTED CCFPD REPORTS FROM 2000-2001[1]

Conflict Prevention and Peacebuilding

Renewing Partnerships for the Prevention of Armed Conflict: Options to Enhance Rapid Deployment and Initiate a UN Standing Emergency Capability. Peter Langille, Global Human Security Ideas and Initiatives. Fall 2000.

Report from the Roundtable on Expert Deployment to International Peace Operations. CCFPD. September 12, 2000.

Canadian Peacebuilding in the Middle East: Case Study of the Canada Fund in Israel/Palestine and Jordan. Tami Amanda Jacoby, University of Manitoba. Fall 2000.

Les Enterprises canadiennes et la consolidation de la paix. Jean-Francois Rioux, Francisco-José Valiente, and Christian Geiser, Université du Québec a Montréal. Le 31 octobre 2000.

Nuclear Weapons and Small Arms

Ballistic Missiles Foreign Experts Roundtable Report. Ernie Regehr, Project Ploughshares and Peter Moore, CCFPD. March 30, 2000.

NATO-Nuclear Weapons Roundtable Report. CCFPD. August 24-25, 2000.

Small Arms and the OAS Roundtable Report. CCFPD. April 28, 2000.

Examen des récentes initiatives gouvernementales et d'ONG concernant les armes légères et appréciation sur leur efficience: proposition pour un indice de sécurité individuelle (ISI). Frances Gaudreault et al. Summer 2000.

Globalization and Firearms: A Public Health Perspective. Wendy Cukier et al. Fall 2000.

Borders

Perspectives on the Borderless World: Issues for Canada. Heather Nicol and Ian Townsend-Gault. Fall 2000.

New Diplomacy

Report from the Roundtable on Just War and Genocide. CCFPD. December 8-9, 2000.

Report from the Ottawa Roundtable for the International Commission on Intervention and State Sovereignty (ICISS). CCFPD. January 15, 2001.

.../2

[1] **Visit www.cfp-pec.gc.ca for more reports and other publications.**

Tel./Tél. : (613) 944-8278 Fax/Télécopieur : (613) 944-0687
www.cfp-pec.gc.ca

Children's Rights
Children and Violent Conflict: Meeting the Challenge of Diversity. Erin Baines, Dalhousie University; Barry Burciul, University of Toronto. Summer 2000.

Business and Labour
Canadian Firms, Canadian Values. Canadian Business for Social Responsibility. May 2000.

Africa
Report from the Ottawa Nigeria Roundtable. CCFPD. March 20, 2000.

Asia-Pacific
APEC Media Monitoring Report: A Synopsis of Key Findings from IMPACS' 1999 Youth Internship Project. Institute for Media, Policy and Civil Society. 2000.

Report from the Burma and Drugs Roundtable. CCFPD. May 15, 2000.

Report from the North Korea Roundtable. CCFPD. January 22, 2001.

Report from the Victoria Roundtable on Indonesia. CCFPD. March 13, 2000.

Europe
Report on Cyprus: Living Together in the New Century Roundtable. CCFPD. February 14, 2000.

Americas
Canada, Indigenous Peoples and the Hemisphere Roundtable Report. CCFPD. March 23, 2000.

CCFPD Summary Report: The Americas. CCFPD. Fall 2001.
Rapport de syntèse du CCDPE: les Amériques. CCFPD. Fall 2001.

Threats to Democracy in America. Max Cameron, Canadian Foundation for the Americas (FOCAL). March 3-4, 2000.

Report from the Roundtable on Governance, Civil Society and the Americas. CCFPD. January 28, 2000.

Report from the Roundtable on Canada-Cuba Relations. CCFPD. January 18, 2000.

Look Ahead to Windsor Roundtable Report (OAS). CCFPD. April 26, 2000.

Culture
Commerce International et diversité culturelle: la recherche d'un dificile équilibre. Ivan Bernier, Université Laval and Dave Atkinson. 2000.

Circumpolar Issues
Roundtable on Northern Foreign Policy: Feedback and Look Ahead. CCFPD. February 5, 2001.

Foreign Policy Research
Gendered Discourses, Gendered Practices: Feminists (Re)Write Canadian Foreign Policy. Claire Turenne Sjolander, University of Ottawa; Heather Smith, University of Northern British Columbia; Deborah Stienstra, University of Winnipeg. May and July 2000.

LIBRARY E A/BIBLIOTHEQUE A E
3 5036 20099719 8

DOCS
CA1 EA752 2001R26 ENG
Geislerova, Marketa
Report from the roundtable :
privacy, sovereignty and technolog
62231218