PRIVACY COMMISSIONERS TAKE CENTER STAGE

SOME SAY PRAGMATISTS, SOME SAY PATSIES

BY WILLIAM BONNER

Four Privacy commissioners offered us insight into their world yesterday. Ann Cavoukian, Information and Privacy Commissioner, Ontario, Canada; Stephen Lau, Privacy Commissioner for Personal Data, Hong Kong; Malcolm Crompton, Federal Privacy Commissioner of Australia; Hansjuergen Garstka, Data Protection and Information Commissioner of the State of Berlin each operate within different governmental structures and different legislative frameworks. Each commissioner provided a brief outline of their formal roles and capabilities revealing considerable variances in length of time that privacy legislation has been in place, the sectors that are covered, the formal authority of the commissioners to access sites and information and their respective powers of enforcement.

In spite of these differences, there were some striking similarities. The commissioners felt that their ability to positively impact the privacy value extended beyond their purely legislated powers. They emphasized the need to be involved in providing education and the importance of building a general awareness of privacy issues in all constituencies, public and private, businesses and individuals. Examples of such activities include never turning down a invitation to a speaking engagement and actively seeking our audiences such as system developers. System developers have a variety of options in their toolkits, each capable of meeting the overall system objectives, but each having potentially different impacts on privacy. Through increased awareness and education, privacy considerations can gain broader support and in the case of system developers, the very expensive retrofitting of systems to protect privacy can be avoided if they had been built into the systems as it was built. This also provides a good opportunity for the commissioners to meet with people with a vested interest in their world.

The opening of the tenth conference on Computers, Freedom and Privacy coincided with an auspicious event in the privacy arena: the passing of Bill C-6 through the Canadian Parliament. Bill C-6 extends privacy protection at the federal level to the private sector and in the case of system developers, the very expensive retrofitting of systems to protect privacy can be avoided if they had been built into the systems as it was built. This also provides a good opportunity for the commissioners to meet with people with a vested interest in their world.

CAVOUKIAN LAUDS PASSAGE OF CANADIAN PRIVACY BILL

The opening of the tenth conference on Computers, Freedom and Privacy coincided with an auspicious event in the privacy arena: the passing of Bill C-6 through the Canadian Parliament. Bill C-6 extends privacy protection at the federal level to the private sector and in the case of system developers, the very expensive retrofitting of systems to protect privacy can be avoided if they had been built into the systems as it was built. This also provides a good opportunity for the commissioners to meet with people with a vested interest in their world.

The plaintiff in the case, Peter Junger, is a professor at Case Western University School of Law and author of Computers and the Law. It is his book, which includes a chapter containing encryption code, that is at the heart of the controversy. While the United States Export Administration permitted the printed book to be freely exported, the administration also held that distributing electronic copies via the Internet would require an export license. Junger then filed suit against William Daley, U.S. Secretary of Commerce, claiming that source code is speech protected by the First Amendment.

Among other responses, the United States argued that source code is not sufficiently expressive to be protected by the First Amendment. Unfortunately for free speech advocates, the district court judge agreed with the defendants and decided in their favor with a summary judgment. "Those of us watching the case were disappointed that it was not decided on the merits," said Mike Godwin, Senior Legal Editor for the Electronic Frontier Foundation.

"The implications of this are immense, especially when you consider that forced speech is prohibited under the First Amendment as censorship," according to Jim Dempsey of the Center for Democracy and Technology. "Taking this decision to its fullest extent means that any government requirements on software design may force First Amendment issues." Tuesday's decision is not the final word on all the issues in the lawsuit; the 6th Circuit sent the case back to the district court for further consideration. "The decision did not answer all the questions raised by the litigation, but the 6th Circuit did articulate the important principle that code is speech," said Godwin.

SOURCE CODE IS PROTECTED

BY ERNEST MILLER

Attendees at the Computers, Freedom and Privacy conference were pleased by a decision on Tuesday by the U.S. Court of Appeals for the Sixth Circuit that source code should be considered speech protected by the First Amendment. "This is the best possible decision you could expect from the Sixth Circuit," said Michael Froomkin, Professor of Law at the University of Miami. "This will now be the leading precedent in this area."

Although the decision was limited to the question of whether source code could be protected as free speech, the language could not be stronger. "Because computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment," Chief Judge Boyce Martin in the unanimous decision.

The plaintiff in the case, Peter Junger, is a professor at Case Western University School of Law and author of Computers and the Law. It is his book, which includes a chapter containing encryption code, that is at the heart of the controversy. While the United States Export Administration permitted the printed book to be freely exported, the administration also held that distributing electronic copies via the Internet would require an export license. Junger then filed suit against William Daley, U.S. Secretary of Commerce, claiming that source code is speech protected by the First Amendment and that the export regulations are an unconstitutional prior restraint on speech.

Among other responses, the United States argued that source code is not sufficiently expressive to be protected by the First Amendment. Unfortunately for free speech advocates, the district court judge agreed with the defendants and decided in their favor with a summary judgment. "Those of us watching the case were disappointed that it was not decided on the merits," said Mike Godwin, Senior Legal Editor for the Electronic Frontier Foundation.

"The implications of this are immense, especially when you consider that forced speech is prohibited under the First Amendment as censorship," according to Jim Dempsey of the Center for Democracy and Technology. "Taking this decision to its fullest extent means that any government requirements on software design may force First Amendment issues." Tuesday's decision is not the final word on all the issues in the lawsuit; the 6th Circuit sent the case back to the district court for further consideration. "The decision did not answer all the questions raised by the litigation, but the 6th Circuit did articulate the important principle that code is speech," said Godwin.

SOURCE CODE IS PROTECTED

BY ERNEST MILLER

Attendees at the Computers, Freedom and Privacy conference were pleased by a decision on Tuesday by the U.S. Court of Appeals for the Sixth Circuit that source code should be considered speech protected by the First Amendment. "This is the best possible decision you could expect from the Sixth Circuit," said Michael Froomkin, Professor of Law at the University of Miami. "This will now be the leading precedent in this area."

Although the decision was limited to the question of whether source code could be protected as free speech, the language could not be stronger. "Because computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment," Chief Judge Boyce Martin in the unanimous decision.

The plaintiff in the case, Peter Junger, is a professor at Case Western University School of Law and author of Computers and the Law. It is his book, which includes a chapter containing encryption code, that is at the heart of the controversy. While the United States Export Administration permitted the printed book to be freely exported, the administration also held that distributing electronic copies via the Internet would require an export license. Junger then filed suit against William Daley, U.S. Secretary of Commerce, claiming that source code is speech protected by the First Amendment and that the export regulations are an unconstitutional prior restraint on speech.

Among other responses, the United States argued that source code is not sufficiently expressive to be protected by the First Amendment. Unfortunately for free speech advocates, the district court judge agreed with the defendants and decided in their favor with a summary judgment. "Those of us watching the case were disappointed that it was not decided on the merits," said Mike Godwin, Senior Legal Editor for the Electronic Frontier Foundation.

"The implications of this are immense, especially when you consider that forced speech is prohibited under the First Amendment as censorship," according to Jim Dempsey of the Center for Democracy and Technology. "Taking this decision to its fullest extent means that any government requirements on software design may force First Amendment issues." Tuesday's decision is not the final word on all the issues in the lawsuit; the 6th Circuit sent the case back to the district court for further consideration. "The decision did not answer all the questions raised by the litigation, but the 6th Circuit did articulate the important principle that code is speech," said Godwin.
On Friday, at the conference’s last session, we will celebrate 10 years of CFP with a special panel featuring some of the most influential and memorable participants throughout the conference’s storied history. In preparation, we asked the past CFP chairs about their view of where the conference has been and where it is going.

GEORGE TRUBOW LOOKS BACK

Q: WHAT MADE THE CFP THAT YOU CHAIRED SPECIAL?
A: “...OUTSIDE OF THE FACT THAT IT WAS A DAMN GOOD PROGRAM!!
• IT’S THE FIRST TIME THAT CFP WAS COVERED BY THE NY TIMES.
• THE FBI “INVITED” ONE OF THE CONFEREES TO THEIR OFFICES FOR AN INTERVIEW. THEY THOUGHT HE WAS KEVIN MITNICK, BUT WERE WRONG.
• OUR KEYNOTE SPEAKER, SIMON DAVIES, WOVED THE AUDIENCE AT HIS DINNER KEYNOTE SPEECH WITH AN ENTRANCE OF FLASHING LIGHTS AND MUSIC AND DRESSED AS THE POPE!”
— GEORGE TRUBOW, CFP CHAIR ’94

PRIVACY COMMISSIONERS CONTINUED FROM PAGE 1
‘business case’ for developing systems with privacy in mind and therefore appeals to the motivation of businesses.

There was also considerable consensus among the commissioners on the need to be pragmatic, needing to recognize and work within the subtleties of any given situation. The successful influence of a commissioner depends to a large degree on their judicious consideration of when and how they are most likely to be effective, now and in the future. While commissioners possess legislative legitimation, they also possess a considerable degree of formal power ascribed through the status of their offices. This individual status can facilitate less official discussions on privacy issues that arise. Privacy concerns raised through such discussions could lead to an awareness of such concerns raised through such discussions or actions.

Perhaps there is no surprise that the privacy commissioners classified themselves as pragmatic. This pragmatism did not come across as a limiting factor. Rather, with a focus on the privacy value, this pragmatism appears to lead to the creation of innovative strategic means through which the value can be promoted. The formal powers of the offices and the potential use of the media are only two specific devices in the repertoire available to the commissioners. Overuse of these particular tools could potentially lead to a diminishment of the ability of privacy commissioners to effectively promote and encourage the protection of privacy values by making the process antagonistic, rather than being cooperative and promoting self-reflection.

The commissioners believe that the selective use of their formal tools as well as the strategic use of their considerable repertoire of less formal tools will more effectively promote the privacy value in the longer term.

The successful influence of a commissioner, however, will depend on the commissioner’s ability to explain how things could be different, while being pragmatic, needing to recognize and work within the subtleties of any given situation. The successful influence of a commissioner depends to a large degree on their judicious consideration of when and how they are most likely to be effective, now and in the future. While commissioners possess legislative legitimation, they also possess a considerable degree of formal power ascribed through the status of their offices. This individual status can facilitate less official discussions on privacy issues that arise. Privacy concerns raised through such discussions could lead to an awareness of such concerns raised through such discussions or actions.

Perhaps there is no surprise that the privacy commissioners classified themselves as pragmatic. This pragmatism did not come across as a limiting factor. Rather, with a focus on the privacy value, this pragmatism appears to lead to the creation of innovative strategic means through which the value can be promoted. The formal powers of the offices and the potential use of the media are only two specific devices in the repertoire available to the commissioners. Overuse of these particular tools could potentially lead to a diminishment of the ability of privacy commissioners to effectively promote and encourage the protection of privacy values by making the process antagonistic, rather than being cooperative and promoting self-reflection.

The commissioners believe that the selective use of their formal tools as well as the strategic use of their considerable repertoire of less formal tools will more effectively promote the privacy value in the longer term.
COMMON INTERESTS, DEEPER DISCUSSIONS

BOFS OFFER MORE INTERACTION
THURSDAY APRIL 6TH 9:30 PM — 12 AM

Freeing the Law: Universal Access to Legal Research Materials
Location: Pier 7
This session will focus on the mission of the Free Law Consortium (FLC), which is to provide sophisticated access to legal research materials for free. At present, efficient and easy access to such materials is controlled by the duopoly of Westlaw and Lexis. The Internet was supposed to change all this, but hasn't yet. Westlaw claims that the Internet never will change this substantially. This session will analyze how the Internet can be used to make legal information readily accessible and easily searchable and why the Westlaw emperor has no clothes. Lawyers, librarians, and researchers especially welcome.
Organizers: Ernest Miller, Yale Law School
Mark Kerr, Yale Law School

Internet Voting: Prelude to the Debate
Location: Harbour Ballroom
See story below for more information.

TechnoLibertarianism — Threat or Menace?
Location: Pier 8
Organizer: Duncan Frussel, Offshore.com

Health Information Privacy
Location: Dockside II
Organizer: Marcia Weiss, Point Park College

Infomediaries, Privacy, and Trust
Location: Pier 9
Organizer: Tom Maddox, PrivacyPlace Magazine

CryptoRights Root Key Ceremony
Location: Location: Pier 4
“If you’ve been reading about “Public Key Infrastructures” (PKIs) in the media but don’t really know what they are or how they work, this is a rare opportunity for you to come learn about public key cryptography from some very experienced crypto people (who are also involved in human rights work), and to be present at the Birth of a new root key and a new PKI. This will be a PGK root key, not an X.509 root key, so the newly-generated CRF “root” key, which will be used as the certifying Meta-Introducer key in the CRF’s PKI, will also be split (using a cryptographic technique to protect it from misuse), and signed by everyone present who has a PGP key, in order to give it validity (and stature) in the global Web of Trust. Representatives of the CRF will also be generating their personal Trusted Introducer keys, which will be signed in front of everyone by the Meta-Introducer key.

If this paragraph didn’t make much sense to you now, then you should definitely come to the ceremony and listen to the Tutorial immediately preceding the Ceremony. Please join us for this very special (and educational!) birth.”
Organizers: Dave Del Toro, Cryptorights, Executive Director
Robert Guerra, Special Project Leader (Canada)

Viral Email Marketing vs Spam
Location: Dockside IV
Who Should Attend?: “Advertisers and marketers”
Why?: “There’s a fine line between viral marketing (customers referring their friends and family to your product) and spam, i.e. what happens when you incentivize your customers to spam your friends and family.”
Organizers: Jad Dowdik, OptIn

A Turning Point for Kids’ Online Privacy
Location: Dockside III
Organizer: Alison Pohn, The FreeZone Network

The Developing Caselaw of Privacy: A Survey and Discussion
Location: Pier 5
Organizer: Keith Enright, Entelechy

INTERNET VOTING
NEW THURSDAY BOF & CHANGES ON FRIDAY
There are some speaker changes for the session on Friday at 9:30 on Internet voting chaired by Lance Hoffman of The George Washington University. Hans von Spakovsky from the Voting Integrity Project is replacing Deborah Phillips, and Joe Mohen, CEO of election.com, is replacing Marc Strassman from that firm. Also, David Jefferson of Compaq, chair of the technical committee for the California Secretary of State’s Internet Voting Task Force, will join the panel along with previously announced members Paul Craft from the Florida Secretary of State’s office and Perry Schoenmakers of the University of Eindhoven.

There is a new Birds of the Feather session Thursday evening at 9:30 p.m. in the Harbour Ballroom. Entitled Internet Voting: Prelude to the Debate, it will be led by David Jefferson (see above). Also expected to attend are Jim Adler, CEO of VoteHere; representatives of election.com; and many of the panelists who will participate in the debate Friday morning. This BOF will provide more of an opportunity than possible in the limited time Friday morning to recount war stories of elections past and present and to examine in gory detail the various technical and organizational aspects of public computer-based elections.

Hans A. von Spakovsky serves on the Board of Advisors of the Voting Integrity Project, a national nonpartisan organization concerned with protecting the integrity and security of the voting process. He is Vice President and General Counsel of the Strollo Group, a government relations and public affairs firm. He is also Vice Chairman of the Fulton County Board of Registration and Elections (this includes Atlanta). He is a graduate of MIT and of Vanderbilt Law School.

CFP CELEBRATES 25 YEARS OF THE PRIVACY JOURNAL
Ben Franklin’s Web Site
Privacy and Curiosity from Plymouth Rock to the Internet

Robert Ellis Smith graced CFP2000 with the humorous letters that he has received after 25 years of publishing one of the most well-known privacy publications, the Privacy Journal. Smith’s new book, entitled Ben Franklin’s Web Site: Privacy and Curiosity from Plymouth Rock to the Internet, which explores American History to discover the tug between our yearning for privacy and our insatiable curiosity, is on sale all week in the Harbour Ballroom.

Robert Ellis Smith
DUNCAN CAMPBELL OFFERS MORNING KEYNOTE

GLOBAL SURVEILLANCE AND EVIDENCE FOR ECHELON

ANNE ADAMS

The use of surveillance to curtail our freedom so as to control and manipulate socially unacceptable behavior is not a modern day invention. Jeremy Bentham (1832) authored a 2,000 page treatise on the subject, which he termed panoptican. The concept was to monitor every person in a building from a central tower. Although people were not watched all the time, they maintained their standards of behavior for fear of being watched. Fear would be maintained by examples being made of old individuals to ‘keep them off their toes’. Over the past 25 years Duncan Campbell has shown us the frightening potential of modern day surveillance technologies. With the automation of surveillance technologies there are far more powerful possibilities available to unscrupulous individuals, organizations and governments. Relevant intelligence information can be provided on diplomatic, economic and scientific developments.

This presentation also reviews the effectiveness of surveillance in the light of advances in automated surveillance technologies. Campbell argues, “there is no law controlling the international snooping of communications.” He presents, in this talk, evidence indicating that governments are routinely exploiting communication intelligence for commercial gain.

Finally, when asked what he believed attendees would leave the talk remembering Campbell suggested, “I think that what I have to say and what I’ll take to most people to places that they didn’t dream existed”. He added that he hoped he would be able to share with his audience the “scale and the capacity of international surveillance” and that this should “underscore what people should do in terms of organizational and self- protection in terms of leading of information out of open communication systems.”

SARA WILFORD

How do you prove you are who you say you are? How do you know that someone is legitimate in his or her dealings with you? It is difficult enough to verify someone’s identity in the tangible world with forgery, impersonation and credit card fraud to name just a few of the potential problems of authentication. The world of cyberspace has even more difficulties of identification and verification due to its remote and electronic nature. Basically, you just never know who you are dealing with or if the goods or services you are attempting to buy exist. This is why the “digital signature” and other authentication systems are being developed in order to alleviate the problems of identity. Identity is however, not only important between individuals and organizations and from person to person, but also to promote trust in Internet companies and verify their legitimacy.

While the need for verification to promote e-commerce is relatively clear, the needs of business and governments in verifying identity must be carefully considered in the light of individual privacy and the increasing requirement that individuals reveal more and more details about their personal lives. Are we in danger of becoming so transparent to the data banks that the privacy of the individual is only to be found inside one’s own skull? The amount of unique data that will be required to verify identity will need to be carefully protected to ensure that such potentially sensitive personal information does not enter into the public domain.

The act of signing a document to guarantee its legitimacy is made less useful in the light of fears of tampering and hacking particularly when transactions are made electronically. The use of cryptography and keysigning is perhaps one way that verification of identity can be assured, but the recent moves attempting to limit its use or at least to control it, means that privacy and civil liberties may be undermined at every juncture.

As consumers, we need to be assured that our credit card details do not go astray, and that only those documents with our authorization and verification will be acted upon. The idea that someone may use our identity for their own means, or that third parties may access sensitive information is of concern to many, thus making the use of authentication and security more vital.

The problems associated with authentications are not just related to the verification of identity but also involve greater public policy issues, which includes the amount and kind of data required to confirm the identity of someone. The use and access to such data is also an issue of major importance. This is due to its potential for abuse by organizations seeking to maximize profits by using the data for marketing purposes. Therefore the confirmation of individual identity becomes an emotive issue which requires much debate and setting of boundaries of implementation and the need to identify the potential use made of information, beyond its initial purpose.

THE PRESS AND PRIVACY: FRIENDS OR FOES?

BRETT BURNEY

Which is more important — our freedom of speech or our right to privacy? This is the main topic for conversation at The Media and Privacy panel session on Thursday, April 6, 2000. Ann Cavoukian, the Information & Privacy Commissioner of Ontario, will moderate the discussion on the media’s right to inform the public contrasted with an individual’s right to a private life.

To get a good idea of the topic, Commissioner Cavoukian has a short paper printed in the proceedings. She asks: “is the strength of our presumption of privacy equal to the forces promoting freedom of speech?” She declares that “any media intrusions into the private world of an individual should have to be justified on some legitimate grounds involving true public interest, and not just because it’s a ‘good story’.”

Raymond Wacks, another panelist for the session, also writes a paper in the proceedings that points out the pivotal issue: We demand immediate news today. The Internet allows the media to provide immediate news. But do we want the individual’s right to privacy when news stories flash on our screens before an individual has a right to respond or react to such news?

Wacks eloquently sums up the current view that is generally shared about the media and privacy: “only wimps are for privacy … tough guys go for free speech.”

This session will discover whether the wimps or the tough guys will prevail in the end.