

## 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 commis-

sioners 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 out 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

PRIVACY COMMISSIONERS CONTINUED ON PAGE 2



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

## 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 requires provinces to follow suit — either by adopting the bill or formulating similar legislation — within two years. CFP Editor Patrick Feng asked Ann Cavoukian, Information and Privacy Commissioner of Ontario, for her thoughts on the significance of the bill's passage.

**Patrick Feng:** How significant is Bill C-6's passage?

**Ann Cavoukian:** This is a big day for Canada. Bill C-6 will return control of personal data to individuals. It will give citizens the ability to choose what level of privacy they want. Also, it will level the playing field in terms of business: right now we have a few good actors who care about privacy, and without C-6 they may be at a comparative disadvantage because they are trying to do the right thing.

**PF:** How does this compare to other privacy or data protection legislation in other countries?

**AC:** It's comparable to other legislation such as the EU Data Directive. There are some differences, of course, but generally the bill is compatible with other countries' laws.

**PF:** Do you think that the passage of Bill C-6 will put pressure on the U.S. to now adopt comprehensive privacy legislation?

**AC:** I think it's too much to hope that pressure from Canada would be sufficient. However, there is more and more pressure being built up by fact that more countries — Canada, Hong Kong, Australia, European countries — are adapting data protection laws.

**PF:** Thank you very much.

**AC:** Thank you.

## CFP CELEBRATES US COURT DECISION

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 *E-commerce Law Weekly*. While the district court did not deny that source code was expressive, it concluded that the functional aspects of code overwhelm the expressive aspects.



“...THE 6TH CIRCUIT DID ARTICULATE THE IMPORTANT PRINCIPLE THAT CODE IS SPEECH” — MIKE GODWIN

The 6th Circuit disagreed. Citing a number of Supreme Court precedents, the appeals court noted that many non-traditional forms of speech such as "musical score[s] cannot be read by the ... public, but can be used as a means of communication among musicians. Likewise, computer source code, though unintelligible to many, is the preferred method of communication among computer programmers."

"The implications of this are immense, especially when you consider that forced speech is as 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 raise 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.

### What's Inside

CFP Year One .....	page 2
Birds of a Feather .....	page 3
Panel Updates .....	page 3
Interview with Adam White Scoville .....	page 4
Authentication .....	page 4

### Today's Weather

Partly Cloudy,  
Chance of Showers  
Hi 13°C 56°F  
Lo 2°C 34°F

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, WOWED 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 less formal legitimation acquired 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 new awareness of such issues on the part of the other party and, perhaps with moral suasion, could lead to changes in data practices in a non-confrontational manner.

Perhaps there is no surprise that the privacy commissioners classified themselves as pragmatists. 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.

## CFP IN THE NEWS

### THE FIRST CFP: THE BEGINNING OF THE END OF MUTUAL MISTRUST

ELIZABETH WEISE, USA TODAY  
APRIL 4, 2000

The first CFP was in 1991, in response to a nationwide series of very high-profile search-warrant raids of alleged computer by the Secret Service. Called Operation Sun Devil, the raids, not infrequently on teens, involved drawn guns, confiscated equipment and no arrests. The Internet, a much more technical and generally apolitical crowd then, went ballistic.

Enter Jim Warren, a longtime computer expert who'd become rich by creating the West Coast Computer Faire — and who also happened to be a motorcyclist who had "a whole bunch of friends who were motorcycle cops."

"I went on the Net and said, 'Well now, hold it, folks. These are just naive law enforcement people, and they just don't understand how we do things in cyberspace. Most of them are decent folks trying to do the right thing. All we have to do is explain how we do things in cyberspace,'" the genial, bearded Warren says.

To that end, he proposed a forum in which law enforcement and computer people could sit down and talk things through. Computer Professionals for Social Responsibility offered its nonprofit status to help make mailings affordable, and Warren promised to pick up the bill if the conference lost money. A program committee began to come together.

Warren made a cold call to Gail Thackeray, the Arizona assistant attorney general coordinating the Western regional portion of Sun Devil.

"I introduced myself and said, 'Ma'am, many of us were quite concerned about what was going on with the raids, and we'd very much like to have a face-to-face.' Her immediate response was 'If you can get the computer people there, I can guarantee I'll get the law enforcement people there.'"

Computer security expert Dorothy Denning came on board and got Laurence Tribe of Harvard Law School



JIM WARREN, CFP CHAIR '91

and William Bayse, director of the FBI's Technical Services Division with responsibility for the National Crime Information Center.

"We were reputable," Warren says. "Suddenly, flaming anarchist libertarian freedom zealots were being consulted by virulent butt-busting law enforcers — and we're helping them!"

Everyone came. "We had folks from the National Security Agency, the CIA, the FBI and the Department of Justice. There were federal, state and local high-tech criminal investigators and prosecutors and corporate security officers," Warren recalls. "On the other side, we had indicted computer crackers, convicted phone phreaks, leading civil liberties advocates and some of the world's leaders in privacy issues."

Each constituency had its own concerns about everyone else attending. But even so, Warren says, there was common ground: "During one of the luncheons, some FBI and NSA people were sitting at a table with some hackers. They were somewhat mutually distrustful, but after they got to talking, they agreed that the people who really frightened them all were the seven or so IRS agents at the next table over."

### CFP Newsletter Editorial Staff

#### EDITORS-IN-PANIC

ALEKSANDR GEMBINSKI  
ARI SCHWARTZ

#### ASSIGNMENT EDITORS

PATRICK FENG  
ESZTER HARGITAI  
HARRY HOCHHEISER  
CHRISTOPHER HUNTER  
ERNEST MILLER

#### STAFF WRITERS

WILLIAM ABBOTT  
ANNE ADAMS  
ALEXANDRE ALVAREZ  
BILL BONNER  
DOUG COKER  
KATE CRABTREE  
CHRISTIAN W. ERICKSON  
KATRINA HANNA  
MARK KERR

MATHIAS KLANG  
ALEXANDER MACGILLIVRAY  
LAUREN MATHESON  
MEGAN MCCORMICK  
ERNEST MILLER  
MARK HISSINK MULLER  
THOMAS NAUER  
NADIA OLIVERO  
NIKOLA OLIC  
ANDRIY PAZYUK  
NOAH ROMER

KAYVAN SAEGHI  
KURT M. SAUNDERS  
LINA TILMAN  
DAVID TODD  
MARC WALDMAN  
ALMA WHITTEN  
SARA WILFORD  
DIETER ZINNBAUER

SPECIAL THANKS TO  
JAMES DEMPSEY

Thursday April 6th, 2000

CHALLENGING THE ASSUMPTIONS

## 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 Frissell, 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: 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 PGP 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 Torto,  
Cryptorights, Executive Director  
Robert Guerra, Special Project Leader (Canada)

#### Viral E-mail 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 Duwaik, OptInk

#### April 2000: 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 Berry 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

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.

### Ben Franklin's Web Site

Privacy and Curiosity  
from Plymouth Rock  
to the Internet



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) argued for control by surveillance, in the preface to his *PANOPTICON*, whereby every person in a building is watched 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 odd individuals to 'keep the others on their toes'. Over the past 25 years Duncan Campbell has shown us the frightening realities 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 concerns what Duncan Campbell himself termed the, "lawless area of the surveillance of international communications." Specifically, a review is made of the ECHELON project, a highly automated system for processing global communication information. Duncan uncovered this project for the first time in 1988. In 1999 he produced a European report with the first documentary evidence for the continued existence of this system and its capabilities. This extensive system exists to access, intercept and process important global communications. Campbell suggested, at an interview during this conference, that the problem is that, "it is clearly only too easy in this new environment for the rivers of information to be accessed once the portholes are open." He also went on to add that now is the critical time to deal with these problems, "because if we don't get the right things... then our children and our children's children will turn round and say what was privacy."

This presentation also reviews the effectiveness of statutes for protecting privacy in the light of advances in automated surveillance technologies. As 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 show will take 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 leaching of information out of open communication systems."



CFP INTERVIEWS  
ADAM WHITE  
SCOVILLE

Although Adam White Scoville is currently concluding a clerkship with the Colorado Supreme Court, he has otherwise been involved with Internet law and policy issues since 1994, through stints working for the U.S. Senate Subcommittee on Technology and the Law and the Center for Democracy and Technology. He also founded one of America's first exclusively online legal journals, the Intellectual Property and Technology Forum at Boston College. last year, one digital signature drafter called Adam's article "Clear Signatures, Obscure Signs," "probably the best single analysis and evaluation of [digital signature legislation and electronic authentication tools] that I've come across so far."

CFP — Why did you come to CFP?

Adam — For my health. I came to CFP for the mountains... I was misinformed.

After a year of dealing with whether you can be put in jail for skiing out of control, a reemersion with the kind of issues discussed at CFP is just what the doctor ordered, especially since I hope to be working in the field after leaving Colorado.

## "WHO AM I AND WHO SAYS SO?" PANEL WILL EXPLORE DIGITAL AUTHENTICATION

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 even 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.

Whilst 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 authentication 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 parallel 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 sacrifice 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.