lexinformatica
technology.law.society

Cybercrime and Lawful Access

What's New?

- Canadian gov't sneaks production order power into Bill C-46 read more... text of C-46 see also excerpt from Hansard
- Canadian gov't releases summary of public consultation submissions, also in [pdf]
- Australian ISP Association releases cybercrime code [MS Word] read more...
- Opposition seeks disclosure on anti-terror surveillance read more...
- Cisco to embed "lawful interception" capability in routers read more...
- Solicitor-General ignoring legal requirment to publish statistics on electronic surveillance read more...
- Federal gov't releases report under FOI on policy implications of high-tech crime... [pdf]
- Vancouver conference presentations from BC FIPA [pdf], Bell Canada [pdf] and the DOJ [pdf] now available.

Table of Contents

Introduction

On August 25, 2002, the Canadian Department of Justice, Solicitor-General and Industry Canada released a **consultation document** which proposes to amend several Canadian statutes, including the *Criminal Code* and the *Competition Act*, in preparation for ratifying the Council of Europe's *Convention on Cyber-crime*.

The proposal discusses new investigatory powers for law enforcement, which would be excercised under lower judicial standards than those now applied to search & seizure warrants and intercepts under the *Criminal Code*; a requirement that telecommunications and Internet service providers make their networks "wiretap" compliant; mechanisms for providing subscriber and service provider information to law enforcement; and, the creation of new criminal offences for virus production and dissemination.

The proposal is almost as interesting for what it does not discuss as for what it does. For example, the aforementioned cybercrime convention contemplates assistance orders for disclosure of encryption keys, and new criminal offences for commercial copyright infringement, child pornography, etc., although these things are not mentioned in the lawful access consultation paper. Some states, including Australia, Japan, the United S tates and the United Kingdom have already drafted new legal intruments to address cybercrime issues. Unfortunately, the range of language and effects in these foreign instruments provides few clues as to what measures the Canadian government will be likely to adopt.

The Department of Justice, the lead federal sponsoring agency on the lawful access issue, held meetings with concerned civil society groups and with other industry and law enforcement stakeholders throughout the Fall of 2002. The civil society roundtables - held in Ottawa, Montreal and Vancover - were coordinated by stakeholders whose information can be found at the bottom of this page. By all accounts, every roundtable was well-attended. As a result of this dialogue, the DOJ extended the public comment submission deadline to 16 December 2002.

According to the DOJ, the federal government received over 300 submissions in response to the Lawful Access consultation, although over 200 of these are terse and pointed e-mails from individuals responding to what Justice described as an inaccurate online article about the proposals. Fifty submissions came from law enforcement agencies and associations, most of which were simply letters of support for the submission of the Canadian Association of Chiefs of Police (CACP). Fourteen civil society organizations filed submissions; twelve came from industry associations; ten from individual companies; and five from a miscellaneous group including the Library Association, the Bar Association and universities. On August 6, 2003, the DOJ released a **summary** of the collected submissions. A number of the original submissions are also available on this site (see below).

The department has apparently heard the message that more details are needed and more consultation necessary, and the focus is now on how best to address these demands. That being said, it will still be up to the Ministers to decide what the next step will be, and that decision is not likely to be taken until after the official summary is released. One suggested possibility is that the departments hold further informal pre-drafting consultations with key stakeholders; this could be a middle ground between moving straight to legislation at one end of a spectrum and, at the other end, sharing and consulting with stakeholders on draft legislation and regulations. The Department of Justice emphasized that no decision has been taken in this respect, but that the request for more details is certainly "being factored into the system".

Proving that this debate has really only just begun, the Collectif sur la surveillance electronique, a coalition of Quebec-based public interest groups, launched a public campaign on January 22 against the Lawful Access proposal and ratification of the Convention on Cyber-crime without further public debate. The collective’s declaration and backgrounder places the lawful access proposal in the context of other anti-terrorism measures adopted by the federal government since September 11, 2001 and argues that the case for increased surveillance powers for law enforcement and national security organizations has not been made.

This directory contains resources relating to the "lawful access" debate in Canada and cybercrime issues, generally. It is maintained by Jason Young, a law student at Queen’s University in Kingston, Ontario, Canada, with assistance from many individuals and civil society groups, including Privaterra, the Public Interest Advocacy Centre, the Electronic Privacy Information Centre, and others.

News

*Recommended articles marked with an **

- APEC furthers plans to combat cybercrime *Computerworld* 09 August 2003 - the APEC e-Security Task Group last week agreed that all APEC economies (including Canada) need to criminalize unauthorized access to computer systems and causing damage to computer systems; allow law enforcement to collect electronic evidence; and encourage greater international cooperation in investigating and prosecuting cybercrime. See conference schedule [pdf].
- Civil liberties group slams Internet ID proposal *Australian Reseller News* 07 August 2003 - proposal to require all Internet subscribers to identify themselves before receiving service.
- Easier wireless snooping worries watchdogs *Toronto Star* 07 August 2003 - senior DOJ official acknowledges that "lawful access" consultation document was not detailed enough and that more public consultation is necessary.
- Privacy, business groups fear Ottawa's plan to modernize surveillance law *CANOE* 07 August 2003 - reporting that the DOJ summarizes public responses to the consultation document as stating that it failed "to show that the current provisions in law are inadequate to allow effective access to data communications services in Canada or that investigations and prosecutions have been unsuccessful due to lack of technical capability." See also Globe & Mail
- * Australian ISP Association releases cybercrime code *News.com (Australia)* 07 July 2003 - self-regulatory cybercrime code governs relationships between ISPs and the police, including access to records and the collection and retention of data. See IIA Code [MS Word]
- * Ottawa urged to issue annual report on C-36 *National Post* 23 April 2003 - opposition critiques delay in releasing anti-terror surveillance statistics.
- * Inside Cisco's eavesdropping apparatus *News.com* 22 Apr 2003 - Cisco embeds "lawful interception" capability into its routers.
- Powers snoop more, explain why less *Toronto Star* 24 Mar 2003 - FOI reveals Solicitor-General not forthcoming with statistics on electronic surveillance.
- FBI, Justice Dept. Increase Use of Wiretaps, Records Searches *Washington Post* 24 Mar 2003 - "national security letters" allow FBI to compel electronic records without prior judicial review.
- Child porn surfers belong in jail: Canada *ZDNet (UK)* 15 Mar 2003 - new provisions would criminal ize knowingly viewing child pornography on Internet.
- Federal document worries privacy advocates *CBC Ottawa* 11 Mar 2003 - lawful access proposals one strand in a growing mesh of surveillance. See also *CBC Montreal* article.
- Surveillance proposals under attack *Montreal Gazette* 11 Mar 2003 - lawful access will have 'chilling effect' on freedom of expression and thought; leverages private sector as law enforcement spies.
- Alberta appoints cybercrime prosecutor *Edmonton Journal* 28 Feb 2003 - first crown prosecutor assigned to work full-time on cybercrime cases.
- Mafiaboy opened eyes to computer crime *Montreal Gazette* 23 Feb 2003 - evidence of cybercrime often volatile.
- * Lawyers: Hackers sentenced too harshly *Business Week* 22 Feb 2003 - U.S. national association of defence lawyers concludes study finding that sentences for cybercrimes frequently exceed seriousness of crime and rely on easily inflated damage figures. Read study here [pdf].
- * What's a cybercrime and what's not *India Times* 16 Feb 2003 - low reporting, lack of police

training and specialized resources contribute to cybercrime; article includes definition of "cybercrimes" in Indian Penal Code.

- Porn Hunters Unwelcome in Canada? *Wired* 12 Feb 2003 - Bill C-15 would make it unlawful for civilian volunteers to track child porn on the Internet simply by criminalizing knowingly viewing child pornography.
- Former Solicitor-General speaks out against lawful access proposal *World Forum on Community Networking* 10 Feb 2003 - Warren Allmand, former S-G of Canada, argues that lawful access proposal is both overbroad and will be ineffective in achieving stated goals.
- U.S. Cyber-security plan counts on private sector's input *eWeek* 4 Feb 2003 - latest draft of National Strategy to Secure Cyberspace will call for response system that relies on broad public-private information-sharing.
- EU proposes agency to combat cybercrime *Globe & Mail* 11 Feb 2003 - EU head office proposes to set up an agency to coordinate Internet security efforts across the Union.
- Rights groups slam antiterror proposals *Globe & Mail* 10 Feb 2003 - ....
- Cybercrime, they just don't mention it *Melbourne Age* 29 Jan 2003 - security experts claim cybercrime rising "exponentially"; police admit problems lie in lack of resources, including appropriate forensic tools, and low reporting. Same story in the *New York Times* here.
- Police struggle to fight child porn *CBC* 16 Jan 2003 - Toronto police identify lack of resources and national strategy as primary issues in fighting child porn on Internet.
- * Proposed law sparks privacy concerns *ComputerWorld Canada* 14 Jan 2003 - KPMG consultant argues that most ISPs are already "more than cooperative" in law enforcement investigations.
- Police launch online survey about cybercrime *Calgary Herald* 13 Jan 2003 - public education and awareness an important component of fighting cybercrime.
- Security breaches of police system worry privacy activists *WorldNetDaily* 31 Dec 2002 - audit of crime database shows significant private abuse by those who have legitimate public access.
- EPIC joins Canadian civil libertarians in criticizing 'Lawful Access' proposal *BNA Privacy Law Watch* 30 Dec 2002 - Washington, D.C.-based public interest group joins in criticism of Canadian "lawful access" proposal.
- Bush Administration to Propose System for Monitoring Internet *New York Times* 20 Dec 2002 - upcoming report national strategy to secure cyberspace will recomme nd centralized monitoring of ISP users.
- Rethink urged over net snooping laws *BBC* 19 Dec 2002 - UK police acknowledge current data retention requirements contravene human rights legislation.
- Snooping system is illegal, say police *The Guardian (UK)* 18 Dec 2002 - senior law enforcement representative says current cybercrime system illegal under human rights law and leaves industry exposed to civil action.
- BC Privacy Commissioner: new lawful access powers not justified *OIPC/BC*, 16 Dec 2002 - submission argues no demonstrable need for new powers; existing judicial pre-authorization standards should apply; creation of centralized subscriber database worrisome.
- BC Freedom of Information and Privacy Association *FIPA*, 16 Dec 2002 - argues email attracts a high expectation of privacy; proposals would increase law enforcement intercept capability; consultation document too vague and insufficient justification for new powers given.
- Privaterra sees lawful access as 'slippery slope', unjustified *Privaterra*, 16 Dec 2002 - new investigatory powers unjustified; holistic approach more sensitive to constitutional rights; reasonable expectation of privacy in traffic data; judicial pre-authorization should apply; too much law enforcement discretion discriminatory.
- ISPs spell out true cost of data retention *ZDNet (UK)*, 12 Dec 2002 - industry testifies costs of retention much higher than gov't forecast; legal, technical and administrative obstacles to simply p

roviding retained data.

- UK law may be updated to cover denial of service attacks *ZDNet (UK)*, 11 Dec 2002 - concerns that some types of hacking might not be covered by the UK's *Computer Misuse Act* could prompt changes to the law, following strong lobbying from industry.
- Ontario Privacy Commissioner critiques lawful access proposal *IPC/ON*, 10 Dec 2002 - 3-point letter highlights lack of oversight, needs determination for new investigatory powers and the flawed logic of applying old standards on new methods of surveillance.
- First e-crime congress meets *VNUNet.com (UK)*, 10 Dec 2002 - charter pledges include: enquiries will be carried out to minimise disruption to business; all exchanges of information will be kept confidential; information 'sanitized' before disclosure to 3d parties; sources will remain confidential; cybercrime unit will share intelligence bulletins with industry; active support for risk assessment procedures.
- UK Police unveil cybercrime confidentiality charter *VNUNet.com (UK)*, 10 Dec 2002 - charter formalises the cybercrime investigation process in a business setting and attempts to limit disruption to a company's day-to-day operations and minimise damage to corporate reputations in the event of an attack.
- Insecure networks targeted by paedophiles *ZDNet (UK)*, 9 Dec 2002 - head of UK's high-tech crime unit claims pedophiles hacking corporate servers.
- Crime 'more serious online than off' *ZDNet (UK)*, 9 Dec 2002 - head of UK's high -tech crime unit declares cybercrime aggravated variant of traditional crime. *Cf.* Prof. Susan Brenner's take on 'cybercrime' here.
- Cybercrime cop hails Cauchon bill *The Montreal Gazette*, 6 Dec 2002 - law prof calls Ottawa's draft kiddie porn law balance between freedom of expression and child protection. View proposed amendments/adoptions here.
- Privacy delays cybercrime code *AustralianIT*, 6 Dec 2002 - Australia's Internet Industry Association's cybercrime code delayed because of concerns raised by Privacy Commissioner; will be ready within weeks.
- We'll All Be Under Surveillance *The Village Voice*, 6 Dec 2002 - media grok on DARPA's total information awareness.
- * Home Office: We got data retention wrong *ZDNet News*, 5 Dec 2002 - UK gov't admits that voluntary data retention code was ill-advised; will try again next year.
- Internet Hate-Speech Ban Called 'Chilling' *PC World*, 2 Dec 2002 - hate speech protocol viewed as incompatible with U.S. free speech protections.
- * Is Privacy Dead? *The Globe & Mail*, 2 Dec 2002 - editorial surveys recent privacy challenges, including Homeland Security, CCRA air passenger database, national ID, and lawful access; notes privacy easier to defend in the abstract.
- *Ottawa's data dig *ITWorld Canada*, 29 Nov 2002 - raises questions of scope of lawful access proposal, cost implications, qualitative difference of traffic data.
- * International Chamber of Commerce decries EU data retention *Europemedia*, 29 Nov 2002 - business uers/providers argue privacy conerns are not going away; differing data retention laws will harm competitiveness; and, law enforcement can already get all the info they need from existing subscriber and traffic records.
- Editorial: Target terror not privacy *The Toronto Star*, 28 Nov 2002 - state-sponsored intrusions on privacy become points of departure for new intrusions.
- Department to store data on citizens for four years *The Irish Times*, 28 Nov 2002 - modeled after controversial UK RIP Act, draft bill would require retention of 'deep data' for 2 - 4 years.
- CIPS calls for Lawful Access watchdog *ITBusiness.ca*, 28 Nov 2002 - analyst disagrees with CIPS contention that gov't requires special legislation

- Man, 20, charged in Web luring of girl *The Globe & Mail*, 5 Dec 2002 - Toronto man charged with new 'Internet luring' provision in *Criminal Code*.
- * IT association warns of flaws in lawful access proposal *Canadian Information Processing Society*, 28 Nov 2002 - believes Canadians have right to anonymity on the Internet; makes several recommendations, including: personal information should not be shared with other countries unless approved by a superior court judge, audit trails of all accesses, software that collects browsing traffic data should be banned. Full submission here.
- Southeast Asian nations endorse 'holistic approach' to cybercrime *Help Net Security*, 27 Nov 2002 - pilot project stresses holistic (technological, administrative, legal) approach, including best practices for protecting privacy and IP; recommends establishment of 24x7 monitoring for tracking cyber-criminals and extraterritorial cooperation in prosecution of offences.
- Harmonizing cyberspace regulations usually means dumbing them down *Vancouver Sun*, 27 Nov 2002 - lawful access proposal raises barriers to competition.
- Watchdog denounces cyber-snooping plan *The Toronto Star*, 26 Nov 2002 - commissioner argues that invading the privacy of Canadians through lawful access should not be convenient; more work needs to be done on pro posal; some groups contemplate boycott of consultation.
- Verizon files suit over new rules *The Everett Herald*, 26 Nov 2002 - telecom challenges WA state utilities commission rules prohibiting sale of customer calling records or using them to market anything but telecommunication services.
- Commissioner says proposed laws are a needless intrusion *The Ottawa Citizen*, 26 Nov 2002 - proposals go far beyond existing practices and threaten to make e-mail messages subject to a lower level of protection than telephone calls or letters; government has not made a sufficient case; preservation and production orders have no non-cybercrime analogue and are inappropriate.
- Lawyers fear misuse of cyber murder law *The Register*, 25 Nov 2002 - *Homeland Security Act* creates life sentence for hackers who "knowingly or recklessly" attempt to cause death; some lawyers feel it will be used to compel plea bargains while others think it will be an unused curiousity on the books.
- Finland proposes extensive data retention *EFFI* 25 Nov 2002 - Finnish police can already demand data retention if they have a valid reason to suspect a crime; proposed extension would require logging traffic data consisting almost entirely of ordinary communications between citizens.
- * Privacy Commissioner comments on 'Lawful Access' proposal *Privacy Commissioner* 25 Nov 2002 - suggests that proposal will create unprecedented scrutiny of our use of the Internet and that; cybercrime investigations should be s ubject to same procedural safeguards as traditional investigations. Full text of letter to Justice Minister.
- Signing Homeland Security bill, Bush appoints Ridge as secretary *The New York Times* - new dept. will bring together nearly 170,000 workers from 22 agencies with widely varying histories and missions.
- Government has lost 'moral compass': privacy under attack *The Toronto Star* 24 Nov 2002 - privacy commissioner asks PM to direct mind towards implications of increased surveillance post-9/11.
- Pentagon Weighed, but Discarded, Plan Reconfiguring the Internet *The New York Times* 21 Nov 2002 - eDNA proposal to divide Internet into secure "public network highways," where a computer user would have needed to be authenticated, and "private network alleyways," which would not.
- * How Ottawa is selling out our privacy *The Toronto Star*, 19 Nov 2002 - the Liberal's search for largely illusory security is stripping citizens of privacy; criminal investigation is moving from the specific (probable cause) to the general (panopticism).
- Internet Provisions in Security Bill *The New York Times*, 19 Nov 2002 - CSEA allows law

enforcment to trace e-mails and other Internet traffic during cyber attacks without obtaining prior judicial authorization; "good faith" enough to attract safe harbor for invasions of privacy.

- Senate Passes Homeland Security Bill *The Washington Post*, 19 Nov 2002 - new act creates new agency responsible for domestic security and will allow any government entity (federal, state, or local) to request email and voicemail from service providers without a warrant or probable cause.
- * Ottawa's planned Big Brother should be dissected *The Toronto Star*, 18 Nov 2002 - observes the lack of Parliamentary debate on lawful access and the notable absence of the federal privacy commissioner; Vint Cerf thinks Carnivore ok.
- * George Bush's Big Brother Orwell would recognize the plan to monitor citizens using databases *The Los Angeles Times*, 17 Nov 2002 - historically, practical barriers rather than constitutional ones protected our civil liberties; in the last decade, these practical barriers to gov't abuse have fallen to technology.
- Mounties claim cybercrime up 65 per cent this year *Network World Canada*, 15 Nov 2002 - poor information security increases criminal opportunities.
- Big Brother Goes To Washington *MSNBC*, 15 Nov 2002 - Interview with EPIC's Rotenberg over p roposed U.S. *Computer Security Enhancement Act* which would get rid of prior judicial authorization for ISP subscriber records.
- You Are A Suspect *New York Times*, 14 Nov 2002 - op-ed by W. Safire on the DARPA's proposed 'Total Information Awareness' data-mining project.
- New Zealand gov't introduces lawful access bill *New Zealand Herald*, 13 Nov 2002 - new bill sets aside money for modifying telecom networks, but not ISPs
- Council of Europe adopts protocol to cybercrime treaty *EurActiv*, 8 Nov 2002 - new protocol requires members to criminalise the intentional dissemination of racist and xenophobic material, threats, denials or gross minimisation through computer systems
- Federal proposal to increase capacity for interception of private communications *Observ@tions*, 8 Nov 2002 - definition of 'service provider' would embrace health networks; data available to interception is quantitatively and qualitatively different than in analog networks. Aussi disponsible en francais.
- * On privacy patrol: look who's watching now *ITBusiness.ca*, 8 Nov 2002 - Canadian privacy czars silent in LA debate
- We Spy *ITBusiness.ca*, 7 Nov 2002 - suffering from info overload, intelligence agencies don't have capacity to analyze the surveillance they receive already
- Stage Set for Homeland Security Act *Wired*, 6 Nov 2002 - amendments will make it easier for law enforcement to request e-mail from ISPs without warrant
- FBI's Cybercrime Crackdown *MIT Technology Review*, 6 Nov 2002 - interview with FBI cyberagent underscores new focus on cybercrime
- Acquittal on heroin charges 'mind-boggling' *Vancouver Sun*, 5 Nov 2002 - wiretap evidence inadmissible: police did not follow terms of authorization and failed to establish lack of less invasive means of obtaining evidence
- FBI Struggling to stop cybercrime *PCWorld*, 1 Nov 2002 - lack of cooperation between law enforcement and industry hindering cybercrime prevention
- Europe's cops can't collar cyber-criminals *News.com*, 1 Nov 2002 - lack of cooperation and resources hindering cybercrime prevention in Europe; mentions new Europol anti-cybercrime coordinating body
- * Protection from the protectors *Globetechnology.com*, 1 Nov 2002 - notes that objective justification for new LA powers lacking
- "Lawful Access" will give spooks sweeping powers *ITBusiness.ca*, 1 Nov 2002 - "journalist" completely misses the point and claims that lawful access would simply "level the pl aying field"

- * Big Brother is becoming a reality *Montreal Gazette*, 31 Oct 2002 - good overview of LA issues
- Internet tattle-tale law may threaten privacy *Hamilton Spectator*, 30 Oct 2002 - incorrectly focuses on cost of data retention, which is not contemplated by LA proposal
- Proposal to fight cyber-crime costly, invasive study says *Toronto Star*, 30 Oct 2002 - incorrectly focuses on cost of data retention, which is not contemplated by LA proposal
- NDP Introduces ISP Licencing Bill *Lex Informatica*, 27 Oct 2002 - poorly-drafted bill has lessons for government
- * UK ISPs say no to 'data retention' *The Guardian* (UK), 22 Oct 2002 - lack of objective justification for data retention prompts UK ISPs to refuse to collect subscriber data voluntarily
- Eye-spy online *ITBusiness.ca*, 18 Oct 2002 - argues that departure from 'reasonable & probable' standard for search & seizure is a slippery slope
- Report Calls for Plan of Sharing Data to Prevent *New York Times*, 7 Oct 2002 - report by leading information and security experts recommends increased data-sharing between law enforcement and the private sector.
- Is Big Brother tracking your e-steps? *ITBusiness.ca* 4 Oct 2002 - general overview of LA proposal and fear that new laws could leave door open to abuse by law enforcement
- Legislation targets cybercrime *London Free Press*, 4 Oct 2002 - [*No longer available online*]
- * Federal proposal tells only part of cybercrime story *Globe & Mail* 3 Oct 2002 - breaks down four main points of proposal; notes lack of detail in proposal, though convention is given as impetus for amendments; notes lack of objective justification for ratification; and, mentions multilateral assistance treaties/obligations under convention
- Canada's Cyber-Snooping Plans Raise Ire *Reuters*, 25 Sep 2002 - [*No longer availble online*]
- White House Issues Cyber-security plan White House *Press Release*, 20 Sep 2002 - adjunct to Homeland Security Act, strategy discusses increased cooperation and info-sharing to prevent cybercrime, see also "The National Strategy to Secure Cyberspace" [pdf]
- Patrolling the Cybe r-borders *eWeek*, 16 Sep 2002 - discusses the U.S. "National Strategy to Secure Cyberspace" and some of the international implications of the U.S. administration's strategy
- Ottawa poised to become Big Brother *Globe & Mail*, 3 Sep 2002 - federal privacy commissioner reviewing proposal and will make comments; hints that some ISPs have built "elaborate security features" to reassure their customers
- * P. Piazza, "Wanted: Tools, expertise to fight cybercrime" *Security Management* 45:9 (September 2002) 41 - study reports need for new investigatory tools to facilitate data collection, map of the network, import and organize log files and lower the expertise needed to intercept real-time data communications | Read the study by the Institute for Security Technology Studies and RAND
- Canada preps Internet snoopers charter *The Register*, 28 Aug 2002 - skeptical that Canada, as permanent CoE observer, is required to sign or ratify cybercrime convention
- * Will Canada's ISPs become spies? *News.com*, 27 Aug 2002 - notes similarities between proposal and U.S. CALEA, but also observes that proposal may be broader in scope
- Government of Canada to Review Lawful Access Laws Dept. of Justice *Press Release*, 25 Aug 2002 - press release on consultation document

Older News

- UK RIP Act gives law enforcement bodies access to personal data retained for national security purposes ZDNet, 31 Jul 2002
-
- "Data retention" scheme marches forward in European Parliament European Parliament, 27 Jun 2002

- International cybercrime treaty finalized *News.com*, 22 Jun 2002
- Carriers must be alert to provisions of new anti-terrorist legislation, lawyer warns *Decima Publishing*, 25 Mar 2002 (pay access)
- Civ libs ask Council of Europe about secret "Second Protocol" ACLU, 1 Mar 2002
- B. Freedman, "Cybercrime treaty open for signature" *Lawyers Wkly.* 21:43 (Mar. 2002) 13.
- "World's Leaders Unite to Battle Cybercrime" *Toronto Star*, 15 May 2002
- Council of Europe drafts secret "Second Protocol" *Politech*, 20 Feb 2002
- Council of Europe approves "cybercrime," "hate speech" treaty *Wired.com* 13 Nov 2001
- Council of Europe "cybercrime" treaty marches forward Council of Europe and CDT, 20 Sep 2001
- Privacy International asks South Africa to block wiretap bill Privacy International, 14 Aug 2001
- FBI's Mueller refuses to commit to independent Carnivore review U.S. Senate, 3 Aug 2001
- 2600 Australia assails "cybercrime" legislation 2600 Australia, 24 Jul 2001
- Council of Europe panel OKs controversial "cybercrime" treaty *Politech*, 25 Jun 2001
- Multi-nation cybercrime pact gets OK *ZDNet*, 22 Jun 2001
- Privacy groups try to rally opposition to "cybercrime" treaty GILC, 9 Jun 2001
- Update on Echelon, cybercrime treaty, FBI's Operation Cyber Loss *e-Legality Bulletin*, 5 Jun 2001
- Cops at "cybercrime" summit complain about unhelpful businesses *Wired.com*, 1 May 2001
- U.S. Chamber of Commerce opposes "cybercrime" treaty U.S. Chamber of Commerce, 9 Dec 2000
- Council of Europe treaty may not include privacy protections *Wired.com*, 8 Dec 2000
- U.K. police want power to keep email, phone records for 7 years *London Observer*, 3 Dec 2000
- Netherlands is adopting controversial Council of Europe treaty *IDG*, 1 Dec 2000
- Carnivore, anonymity, Council of Europe treaty *EPIC*, 30 Nov 2000
- Council of Europe "cybercrime" treaty being reworked *Wired.com*, 14 Nov 2000
- Civil lib groups oppose CoE treaty, OECD "cybercrime" f orum *Financial Times*, 18 Oct 2000
- French proposed anti-anonymity law requires "identity escrow" *Politech*, 19 Jun 2000
- Slate privacy roundtable (#3) police searches and seizures *Slate.com*, 10 Jun 2000
- International update: Australia, Switzerland, G8 summit *Politech*, 26 May 2000
- G8 update: Global Internet Project report, more news from Paris *Politech*, 19 May 2000
- Cybercrime Forum Touted For Canada *Globe & Mail*, 18 May 2000
- G8 nations bar public from debate, Europeans want 1-year records *CBC*, 15 May 2000
- G8 complains of digital havens; French hate "unfettered freedom" *Yahoo.com*, 15 May 2000
- G8 officials meet in Paris this week to discuss computer crime *Politech*, 15 May 2000
- Draft treaty shows weakness of Euro-privacy laws - Bill Stewart *Politech*, 5 May 2000
- Planned global Net-treaty hands police more power, limits privacy *Wired.com*, 3 May 2000
- Justice Dept FAQ on encryption: We need access to plaintext! U.S. Dept. of Justice, 10 Mar 2000
- US-Europe cybercrime treaty ha ppening in secret - M.Wessling *Slashdot*, 13 Jan 2000
- Janet Reno proposes "cybercrime" crackdown, new databases *Reuters*, 28 Nov 1998

Public Consultation Background and Fora

Between October 21 and November 2, 2002, the Department of Justice, the Solicitor-General and Industry Canada held public consultation roundtables with civil society groups in Ottawa, Montreal and Vancouver. Private meetings between the sponsors and industry and law enforcement groups were also held during the fall. Background material from the civil society roundtables can be found here.

Ottawa - October 21 | Agenda | Attendees | Presentation: Access to Subscriber Info | Notes

#1 | Notes #2

Vancouver - November 2 | Notice | Agenda | Presentation: Legal Context of Proposal

Montreal - (no information available)

Early in the public consultation, the federal government indicated they did not intend to publish the submissions received, except in summary. However, submissions from a broad cross-section of individuals and organizations have been collected on this site and are available below.

Civil Society

- Submission by the BC Freedom of Information and Privacy Association on the consultation paper.
- Submission by the Civil Liberties Association, National Capital Region, on the consultation paper.
- Submission by the Electronic Frontier Foundation/Electronic Frontier Canada on the consultation paper.
- Submission by the Electronic Privacy Information Center on the consultation paper.
- Submission by the Public Interest Advocacy Centre on the consultation paper.
- Submission by la Ligue des droites et libertes (en francais).
- Submission by Privaterra/Computer Professionals for Social Responsibility on the consultation paper.
- Submission by Telecommunities Canada on the consultation paper.
- Submission by Vancouver Community Networks on the consultation paper.

Individuals

- Letter from Professor Ian Kerr, University of Ottawa Faculty of Law, to the Ministers responsible.
- Submission by Chris Brand, computer professional, on the consultation paper.
- Sub mission by Matthew Skala, University of Waterloo, on the consultation paper.
- Submission by Russell McOrmond, small Internet Service Provider, on the consultation paper.
- Submission by Tom Trottier, computer professional, on the consultation paper.
- Submission by Bill Bonner, University of Calgary, on the consultation paper.
- Submission by Keith Risler, private citizen, on the consultation paper.

Industry and Industry Associations

- Letter from the Canadian Wireless Telecommunications Association letter to Min. of Justice on lack of disclosure in public consultation.
- Letter from the Canadian Association of Internet Providers calls on gov't to provide more detail on draft legislation and regulations.
- Submission by the Canadian Wireless Telecommunications Association on the consultation paper.
- Submission by the Information Technology Association of Canada on the consultation

paper.

- Submission by the Computer Technology Industry Association (CompTIA) on the consultation paper.

Law Enforcement

While only one submission from the law enforcement community is available here, many of the submissions received by the government from the law enforcement community reportedly supported the CACP document.

- Submission by the Canadian Association of Chiefs of Police (CACP) on the consultation paper.

Privacy Commissioners

- Letter from the Privacy Commissioner of Canada to the Ministers responsible.
- Letter from the Ontario Information and Privacy Commissioner to the Ministers responsible.
- Letter from the British Columbia Information and Privacy Commissioner to the Ministers responsible.
- Submission by the Commission d'acces a l'information du Quebec on the consultation paper (en francais).
- Submission by the Alberta Information and Privacy Commissioner on the consultation paper.

Other Background Materials

During the Ottawa roundtable on October 21, 2002, several attendees expressed concern that the consultation document was too vague and did not provide enough information upon which to give informed comment. This refrain was repeated at other meetings with civil society and industry and can be found in many of the written public submissions above. In response, government representatives promised to release more background material relating to the proposed ratification of the Council of Europe *Convention on Cyber-crime*. However it was not until February 28, 2003, that additional background material was released and then only in response to freedom of information requests to the DOJ and Industry Canada.

- Access to information request [pdf] to DOJ (20 Nov 2002) for relevant background material on proposed ratification of the cybercrime convention and the "Lawful Access" public consultation; identical request [pdf] to Industry Canada.
  - Response from Industry Canada (28 Feb 2003) [pdf]
  - Response from Department of Justice (06 Mar 2003) [pdf]
  - An Analysis of International Iniatives on High-Tech Crime: A Review of the Implications for the Canadian Policy Environment [pdf].
- Access to information request [pdf] to DOJ (04 Mar 2003) for consultant's summary of public submissions made to lawful access sponsoring agencies and a list of groups with whom the sponsoring agencies met to discuss the lawful access proposal; identical request [pdf] to Industry Canada.
  - Response from the Department of Justice (11 Mar 2003) [pdf]

- Access to information request [pdf] to the Solicitor-General (04 Mar 2003) for s. 195 report on applications for authorization to intercept private communications and intercepts actually executed from 1995 to date. Additional request for data on intercepts granted under s. 185 and s. 188 of the *Criminal Code* but not executed by the authorized peace officer for lack of technical capability to do so.
  - Response from Solicitor-General (11 Mar 2003) [pdf]
  - Reply to Solicitor-General (18 Mar 2003) [pdf]
  - Kevin Sorenson, MP, Canadian Alliance Justice Critic, questioning Solicitor-General Hon. Wayne Easter on delay in tabling the s. 195 report
  - Wayne Easter, Solicitor General of Canada, responding to letter sent to the Speaker of the House of Commons, Peter Milliken, regarding the failure to disclose electronic surveillance statistics in a timely fashion. [pdf]

Public Fora

Since the August 25, 2002 release of the lawful access consultation document, there have been several public presentations or debates on the lawful access issue, including the following:

- Seminar Discussion Notes [pdf] - notes made at Queen's Law faculty seminar led by Professor Ian Kerr of the University of Ottawa on the DOJ's proposed lawful access amendments. Discussion on 'agent of state' doctrine and fiduciary duties as applied to ISPs.
- Professor Ian Kerr's keynote at the 3rd Annual CACR/IPC Privacy and Security Workshop and his powerpoint from that presentation.
- BC FIPA Exec. Dir. Darrell Evans' presentation on Lawful Access to the Fr ontiers of Privacy and Security Conference in Vancouver, 13-14 Feb 2003 [pdf]
- Ass't Gen. Counsel, Bell Canada, David Elder's presentation on Lawful Access [pdf].
- DOJ lawyer Paul Pierlot's summary of the public consultation process [pdf]
- Declaration by the Collectif sur la surveillance electronique against the lawful access proposal and ratification of the cybercrime convention. See also Backgrounder.

Statutory and Other Instruments

- Convention on Cybercrime **Author:** Council of Europe
  Date: November 2001
  Type: HTML
  Abstract: The Convention has three primary purposes: 1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime; 2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form; 3) setting up a fast and effective regime of international co-operation.

- Criminal Code of Canada **Author:** Canada
  Date: November 2001
  Type: HTML
  Abstract: Unlike some federations, notably Australia and the United States, criminal law in

Canada is solely federal in jurisdiction, although it is administered provincially. Part VI of the Criminal Code is concerned with state invasions of privacy. Part XV deals with special procedures and powers, including what law enforcement requires to obtain a search warrant (s. 487).

- Bill C-20: An Act to amend the Criminal Code (protection of children and other vulnerable persons) and the Canada Evidence Act **Author:** Canada
  Date: (introduced) 5 December 2002
  Type: HTML
  Abstract: In response to Supreme Court ruling, bill tailors definition of "child pornography" to make it an offence to possess written material whose dominant theme is the description of illegal sex acts with persons under 18 years of age, regardless of motive of accused. Also creates new offences of voyeurism by mechanical or electronic means and knowingly distributing or otherwise making available voyeuristic recordings to the public. View comparison of proposed amendments.

- Regulation of Investigatory Powers Act (UK) **Author:** Home Office, United Kingdom
  Date: 28 July 2000
  Type: HTML
  Abstract: Compels assisted disclosure of encrypted data and passwords. Passed in response to U.K. law enforcement's claim that new technologies were inhibiting investigations. Targeted at child pornography, human trafficking, etc.

- Communications Assistance for Law Enforcement Act (US) **Author:** U.S. Government
  Date: October 1994 (implementation through 2000)
  Type: HTML
  Abstract: CALEA requires telecommunications carriers to ensure that their equipment, facilities, and services are able to comply with authorized electronic surveillance. The CALEA definition of "telecommunications carrier" does not include ISPs, although the PATRIOT Act largely eliminates the distinction.

- USA PATRIOT Act of 2001 (U.S.) **Author:** U.S. Government
  Date: October 24, 2001
  Type: HTML
  Abstract: USA PATRIOT is an acronym standing for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism". It is a 342-page omnibus that amends 15 different statutes, but only a few provisions relate to online activities. In particular, s. 212 of the act allows ISPs to voluntarily hand over all "traffic" data to law enforcement without need for a court order or subpoena. Sections 210 and 211 expand the records that the government may seek with a subpoena and without judicial review to include records of session times and durations; dynamic IP addresses; and means and source of payments, including credit card or bank account numbers. Section 217 expands surveillance powers against suspected computer trespassers with no need for court order. Wiretaps are now allowed for suspected violations of the *Computer Fraud and Abuse Act*. The Electronic Frontier Foundation has provided a helpful analysis of the act as it relates to online activities.

- Homeland Security Act (U.S.) **Author:** U.S. Government
  Date: November 19, 2002

Type: HTML
Abstract: HSA creates new department-level agency charged with implementing and overseeing the U.S. domestic security apparatus. The Department of Homeland Security will absorb several other agencies, including the Federal Emergency Management Authority, Border Patrol, Customs, and the Transportation Security Agency. The *Computer Security Enhancement Act* (CSEA) was rolled into the HSA and abrogates judicial pre-authorization for investigations of telecommunications and Internet service provider subscriber records and other traffic data. Read EPIC's letter to the House sub-committee on Crime, criticizing the (then) bill.

- Cybercrimes Act of 2001 (Australia) **Author:** Commonwealth of Australia
  Date: September 27, 2001
  Type: HTML
  Abstract: This act implements some provisions of the Convention on Cyber-crime through amendments to a number of different Australian federal laws. Section 477 creates absolute liability offences for unauthorized modification of data to cause impairment and impairment of electronic communication. Section 478 creates the offence of possession or control and production and supply of data with intent to commit a computer offence. The definition of "data" includes software, but the s. 478 offences are not restricted to onl y software that could be used to commit substantive computer offences; the law does not recognize that much of the software in this provision has legitimate testing uses. Schedule 2 relates to law enforcement access to electronically stored data and creates assistance orders which require persons to hand over passwords to secure systems and encrypted data. Electronic Frontiers Australia (EFA) has a variety of materials on the act and its implications.

- Directive on Privacy and Electronic Communications 2002/58/EC **Author:** European Parliament
  Date: May 30, 2002
  Type: PDF
  Abstract: This directive repeals and replaces an earlier directive, 97/66/EC, which translated, for the telecommunications sector, the principles set out in the European Directive on Privacy and Data Protection 95/46/EC. The replacement directive proscribes data retention requirements for information and communications services. EU countries have until October 31, 2003 to implement the Directive. Some of them (e.g., Belgium, France, Great Britain, Spain) have already provided for the retention of electronic communications data.

Academic Literature

Alphabetized by author's last name, then title.

"Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication", 110 *Harv. L. Rev.* 1591 (1997).

H. Axelrod et al., "Crime and punishment in cyberspace: dealing with law enforcement and the courts" (27th Annual ACM SIGUCCS conference on User services: Mile high expectations, Denver, 1999) 11.

S. Baker, "Technological Innovation & Legal Tradition: Enduring Principles For Changing Times" (1998) 4 *Tex. Rev. L. & Pol.* 53.

C . Barrett, "FBI Internet Surveillance: The Need For A Natural Rights Application of the Fourth Amendment to Insure Internet Privacy" (2002) 8(3) *Rich. J.L. & Tech. 16.* [html] [pdf]

L. BeVier, "The Communications Assistance for Law Enforcement Act of 1994: A Surprising Sequel to the Break Up of AT&T" (1999) 51 *Stan. L. Rev.* 1049.

S. Brenner, "State cybercrime legislation in the United States of America: a survey" (2001) 7(3) *Rich. J. L. & Tech.* [html]
___________ "Is There Such a Thing as "Virtual Crime"?" (2001) 4 *Cal. Crim. Law Rev.* 1. [html] [pdf]

J. Broberg, "From CALEA to Carnivore: How Uncle Sam Conscripted Private Industry in Order to Wiretap Digital Telecommunications" Case comment *U.S. Telecom Ass'n* v. *FCC*, 227 F.3d 450 (D.C. Cir. 2000) (2001) 77 *N.D. L. Rev.* 795.

J. van Buuren, *Making up the rules: Interception versus privacy*, (Amsterdam: Jansen & Janssen, 2000). [html]

M. Clifford, "Communications Assistance for Law Enforcement Act (CALEA)" (2002) 36-APR Prosecutor 22.

L. Coacher, "Permitting systems protection monitoring: when the government can look and what it can see" 46 *Air Force L. Rev.* 155. [html]

C. Cohn, "EFF Analysis of the Provisions of the USA PATRIOT Act That Relate to Online Activities" (2002) 701 PLI/Pat 1201. [html]

M. Colombell, "The Legislative Respon se to the Evolution of Computer Viruses" (2002) 8(3) *Rich. J. L. & Tech.* [html] [pdf].

J. Dempsey, "Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy", (1997) 8 *Albany L.J. of Sci. & Tech.* 1.

G. Eddie, "E-mail, the police, and the Canadian Charter of Rights and Freedoms: retooling our understanding of a reasonable expectation of privacy in the cyber age" (2000) 14(1) *Int. Rev. of L. Comp. & Tech.* 63.

P. Georgiton, "The FBI's Carnivore: how federal agents may be viewing your personal e-mail and why there is nothing you can do about it" (2001) 62(6) *Ohio State L. J.* 1831.

N. Giallonardo, "Steve Jackson Games v. United States Secret Service (36 F.3d 457 (5th Cir. 1994)): the government's unauthorized seizure of private e-mail warrants more than the Fifth Circuit's slap on the wrist" (1995) 14 *John Marshall J. of Comp. & Info. L.* 179.

T. Greenberg, "E-mail and voice mail: employee privacy and the federal wiretap statute" (1994) 44 *Am. U. L. Rev.* 219.

A. Hamdani, "Who's liable for cyberwrongs?" (2002) 87(4) *Cornell L. Rev.* 901.

R. Hubbard, P. deFreitas and S. Magotiaux, "The Internet - Expectations of Privacy in a New Context" (2002) 45 *C.L.Q.* 170.

D. Jackson, "Protection of privacy in the search and seizure of e-mail: is the United States doomed to an Orwellian future?" (1999) 17(2) *Temple Enviro. L. & Tech. J.* 97.

C. Manchester, "Obscenity in the mail" (1983) *The Criminal Law Review* 64.

G. North, "Carnivore in Cyberspace: Extending the Electronic Communications Privacy Act's Framework to Carnivore Surveillance" (2002) 28 *Rutgers Computer & Tech. L.J.* 155. [html]

D. Ormerod, "Protection o f Children Act 1978, s.1(1)(a)- Making an Indecent Pseudo-Photograph of a Child- Mens Rea- Whether Opening of an E-mail Attachment Containing Indecent Photographs "Making a Photograph"- Whether Downloading of Indecent Images from the Internet to Computer Screen "Making an Photograph"- Whether Intention to Store and Intention for Future Retrieval of Material Requisite Mens Rea for Commission of Offense Under Section 1(1)(a)" (2002) 2002 *The Crim. L. Rev.* 659.

A. Pascual, "Access to 'traffic' data: when reality is far more complicated than a legal definition" (Global Community Networks 2002, Montreal, 11 October 2002) [unpublished]. [ppt]

A. Pascual and I. Hosein, "Understanding Traffic Data and Deconstructing Technology-neutral Regulations" (7 March 2002) [unpublished] [pdf].

A. Orr, "Marking Carnivore's Territory: Rethinking Pen Registers on the Internet" (2001-2002) 8 *Mich. Telecomm. & Tech. L. Rev.* 219. [pdf]

R. Plesser et al., "USA PATRIOT Act for Internet and Communications Companies" (2002) 19 No. 3 *Computer & Internet Law* 1. [html]

M. Rotenberg, "Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)" 2001 *Stan. Tech. L. Rev.* 1. [html] [pdf]
___________ "Privacy and Secrecy After September 11" (2002) 86 *Minn. L. Rev.* 1115.

M. Rustad, "Private enforcement of cybercrime on the electronic frontier" (2001) 11(1) *So. Cal. Interdiscipli nary L.J.* 63.

D. Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy" (2002) 75 S. Cal. L. Rev. 1083. [pdf]

L. Surtees and W. Chaisatien, "Caught in the Web: Ottawa's Implementation of Cyber-crime

Treaty Requires Online Surveillance by xSPs" IDC Canada.

H. Tavani, "Defining the boundaries of computer crime: piracy, break-ins, and sabotage in cyberspace" (2000) 30(3) ACM SIGCAS Computers and Society 1.

P. Taylor, "Issues Raised by the Application of the Pen Register Statutes to Authorize Government Collection of Information on Packet-Switched Networks" (2001) 6 *Va. J.L. & Tech.* 4. [html]

G. Tufaro, "Will Carnivore Devour the Fourth? An Explanation of the Constitutionality of the FBI Created Software" (2002) 18 *N.Y.L. Sch. J. Hum. Rts.* 305.

J. Vandermause, "You've got indecent e-mail!" (1999) 1999(6) *Wis. L. Rev.* 1259.

J. Yeates, "CALEA and the RIPA: The U.S. and the U.K Responses to Wiretapping in an Increasingly Wireless World" (2001) 12 *Alb. L.J. Sci. & Tech.* 125.

P. Young, "The Case Against Carnivore: Preventing Law Enforcement From Devouring Privacy" (2001) 35(1) *Ind. L. Rev.* 303.

Resources

- Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Needs Assessment *Institute for Security Technology Studies*, Sept 2002 - study reports need for new investigatory tools to facilitate data collection, map of the network, import and organize log files and lower the expertise needed to intercept real-time data communications.
- The Solicitor-General is required, by law, to annually publish a report on electronic surveillance in Canada. The report indicates that the number of applications made for audio and video authorizations and renewals has fallen since 1995, but does not explain the trend. Actual intercepts have also fallen. Emergency authorizations under s. 188 represent a miniscule number of the total: only six were granted in the five-year period 1995-1999. See 2001 Report, 2000 Report, 1999 Report.
- U.S. Administration's Cyber-Security Plan | Excerpts
- Electronic Privacy Information Center (U.S.) Data Retention Archive
- StateWatch (UK): EU-FBI Telecommunications Surveillance Archive
- Privacy International's Cybercrime Index
- G8 Principles on the Availability of Data Essential to Protecting Public Safety, including a list of log details related to some services that may be available to an Internet service provider.
- Illegal and Offensive Content on the Internet: The Canadian Strategy to Promote Safe, Wise and Responsible Internet Use
- Sem inar Discussion Notes - notes made by Jason Young at Faculty seminar led by Professor Ian Kerr of the University of Ottawa on the DOJ's proposed lawful access amendments. Discussion on 'agent of state' doctrine and fiduciary duties as applied to ISPs. See also Ian Kerr's keynote at the 3rd Annual CACR/IPC Privacy and Security Workshop and his powerpoint from that presentation.
- Council of Europe releases results of traffic data questionnaire - a comprehensive

snapshot of traffic data retention law and policy throughout Europe.

- ABA International Cybercrime Project -
- Council of Europe releases results of "traffic data" questionnaire - read more...
- U.S. National Association of Defence Lawyers comment on sentencing finds that cybercrimes are frequently punished more severely than comparable non-computer-related offences. [pdf].
- National Hi-Tech Crime Unit - UK's first-ever national crime fighting force; mandate to combat computer crime, provide specialized assistance to local law enforcement agencies, and liase with international counterparts.
- An Analysis of International Initiatives on High-Tech Crime: A Review of Implications for the Canadian Policy Environment - report commissioned by the federal gov't in preparation of ratification of cyber-crime convention; released [pdf] under access to information [pdf] on February 27, 2003.
- Slides from Matt Skala's presentation on lawful access to the University of Toronto's Info Rights Salon.

Stakeholders

The following information was released [pdf] on May 9, 2003, in response to an access to information request [pdf] filed on March 4, 2003.

- List of consultations held with organizations in respect of the lawful access proposal.
- Organizations represented at the lawful access consultation meetings.
- Organizations which made written submissions in response to the lawful access consultation document.
