Lawful Access and Data Preservation/Retention: Present Practices, Ongoing Harm, and Future Canadian Policies

By Christopher Parsons[1]

Version 2.2 :: February 7, 2012

[1] PhD Candidate in the Political Science Department at the University of Victoria. Thanks to the various individuals who have generously offered comments on earlier drafts of this report and to Joyce Parsons for her editorial assistance. This report was prepared for British Columbia Civil Liberties Association (BCCLA), though its proposals should be attributed to me and do not necessarily reflect those held by the BCCLA. Comments/suggestions are welcome at parsons@uvic.ca.

Table of Contents

Introduction

Lawful access legislation enhances policing and intelligence powers. There are typically three types of access powers associated with such legislation: search and seizure provisions, interception of private communications powers, and production of subscriber data.[2] In Canada, the Martin Liberal and Harper Conservative governments both tabled lawful access legislation, though each government's legislation died on the Order Paper when elections were called or parliament prorogued.

In the last session of parliament, the Conservative Party of Canada (CPC) tabled a series of bills meant to enhance, extend, and create new policing and intelligence powers. With the fall of the government in March 2011, these bills - C-50, An Act to amend the Criminal Code (interception of private communications and related warrants and orders); C-51, An Act to amend the Criminal Code, the Competition Act and Mutual Legal Assistance in Criminal Matters Act; and C-52, An Act regulating telecommunications facilities to support investigations – died. The subsequent CPC campaign platform promised to reintroduce these bills, along with other law and order legislation, and pass them in an omni-

[2] CIPPIC. (2007). "What is "lawful access?" Last updated June 2, 2007. Online: <http://www.cippic.ca/en/lawful-access-faq#LA01>

bus law within the CPC's first hundred days in office.[3] Since the formation of a majority government, the Public Safety minister has stated an unwillingness to modify the forthcoming bills in response to public outcry.[4] Given lawful accesses' legislative past, and the current government's advocacy for its past iterations, Canadians can expect lawful access legislation to be a governmental priority.

This report examines the British and American implementations of lawful access laws. It specifically attends to the following, as appropriate: preservation, retention, and access of data; audit formats; and harm that these laws have caused individuals. Next, there is a brief discussion of lawful access laws that have propagated in other jurisdictions around the world and the consequences of these laws. The report then identifies generalized problems with lawful access legislation and suggests ways to alleviate those problems should similar legislation be tabled (again) in Canada.

United Kingdom

The UK passed the *Regulation of Investigatory Powers Act* (RIPA) to extend law enforcement's access to communications systems in 2000. Ostensibly, this access was meant to enhance efforts to combat criminal offences and terrorist-related actions. Since then the government has amended that Act and is presently engaged in further broadening the powers of law enforcement and intelligence services. These expansions are worrying given how extensively authorities use these surveillance powers, how extensively authorities commit common errors, and how significantly individuals can be harmed.

Preservation and Retention of Data

UK Internet Service Providers (ISPs) retain data based on a voluntary code of practice, titled "Retentions of Communications Data Under Part: 11: Anti-Terrorism, Crime & Security Act 2001 (Code of Practice)." The Code clarifies how "communication service providers can assist in the fight against terrorism by meeting agreed time periods for retention of communications data that may be extended beyond those periods for which their individual company retains data for business purposes." More specifically, providers must retain data for six to twelve months, depending on its type.[5] This code divides information (per RIPA) into the following categories:

1. **traffic data** – including telephone numbers called, email addresses, and location data etc.
2. **use made of service** – including services subscribed, etc.

[3] Conservative Party of Canada. (2011). "Here For Canada: Stephen Harper's Low-Tax Plan for Jobs and Economic Growth." Online: <http://www.conservative.ca/media/ConservativePlatform2011_ENs.pdf>
[4] S. Schmidt. (2011). "Toews won't bend on online surveillance laws," *The Montreal Gazette.* Published October 28, 2011. Online: <http://www.montrealgazette.com/technology/Toews+bend+online+surveillance+laws/5619707/story.html>
[5] The only deviations from this time period are Web activity logs, which are retained for four days.

3. **other information relating to the subscriber** – including installation address, etc.[6]

Per RIPA, traffic data means:

1. any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted,
2. any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted,
3. any data comprising signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of any communication, and
4. any data identifying the data or other data as data comprised in or attached to a particular communication, but that expression includes data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored.[7]

A voluntary data preservation system, which was used in the wake of 9/11 and other disasters, retained data such as "the content of email servers; email server logs; radius or other IP address to user resolution logs; pager, SMS and MMS Messages currently on the network's platform; content of voicemail platforms; call data records (includes mobile, fixed line, international gateways & VoIP) and subscriber records."[8] Data had to be retained because criminal investigations "will take many months and it is likely that the significance of specific communications data and current stored content will not become immediately apparent and there is a real risk that important evidence could be lost."[9]

Audit Formats

The "Retentions of Communications Data Under Part: 11: Anti-Terrorism, Crime & Security Act 2001 (Code of Practice)" required that the Code be evaluated three months after it received parliamentary approval. The evaluation had to: consider whether the Code led to improvements in investigative work; identify the number of requests made; determine if the voluntary system was working; clarify the percentage of communications providers who had adopted the Code of Practice; and ascertain if sectors not complying with the Code were enjoying unfair commercial advantages. Since the inception of the

[6] Home Office. (2003). "Retention of Communications Data Under Part 11: Anti-Terrorism, Crime & Security Act 2001 (Code of Practice)." United Kingdom Government. Online: <http://www.opsi.gov.uk/si/si2003/draft/5b.pdf>

[7] UK Government. (2000). "Regulation of Investigatory Powers Act 2000," *Legislation.gov.uk*. Online: <http://www.legislation.gov.uk/ukpga/2000/23/contents>

[8] T. Richardson. (2005). "Net industry urged to co-operate following London bombings," *The Register*. Published July 11, 2005. Online: <http://www.theregister.co.uk/2005/07/11/ispa_preservation>

[9] European Digital Rights (2005). "UK ISPs Voluntarily Preserve Internetdata," *ERDI-Gram – Number 3.14, 13 July 2005*. Online: <http://www.edri.org/edrigram/number3.14/preservation>

Code, the Interception Commissioner has issued yearly reports that evaluate law enforcement's and intelligence agencies' uses of the UK's extended surveillance laws.

The UK's membership in the EU imposes reporting requirements about data retention processes. While the state is required to provide the European Commission with regular reports, the European Union's Article 29 Working Party has found that retention policies across the EU lack heterogeneity and often fail auditing requirements. The Working Party argues that telecom providers cannot be expected to ensure proper compliance with law enforcement requests, on the grounds of the power differences between communications providers and law and intelligence services. While the Working Party is hostile towards required data retention, it stops short of demanding its abolition. Instead, it suggests that the following handover procedure should be adopted across the EU and that member-nations be required to submit yearly reports that include information based on the following data points of interest:

1. Single contact point at each service provider;
2. Single data handover format, including at least the following:
    a. User data; containing a known, finite number of fields related to service subscription and the terminals made available to users;
    b. Traffic data; containing known finite fields;
    c. Provider code containing a unique EU-wide ID to identify the communications provider and/or ISP
    d. LEA code to ID which LEA made the request
    e. Judiciary code to ID the judicial authority requiring the disclosure
    f. Timestamp and request number
    g. Request type, to specify the data request category (e.g. by serious crime or by amount of requested traffic data).[10]

Establishing a common framework would enable wide-scale comparative analyses of telecom surveillance. This would let EU Commissioners evaluate the actual usage of data retention powers and the regularity of their usage by particular law enforcement authorities (LEAs). It would also identify whether a variety of judges or very specific ones are approving disclosure requests. Further, a standardized system would permit the Interception Commissioner to engage in more granular analyses of retention and surveillance requests by authorities, which would enhance the caliber of the office's yearly reports.

Challenges and Harm

The Interception Commissioner provides a report each year that details interceptions of communications traffic for the proceeding year. In 2007 there were twenty-four interception errors and breeches; the Commissioner deemed this number to be "too high." Northern Ireland Office/Police Service Northern Ireland, Government Communications Head-

[10]Article 29 Data Protection Working Party. (2010). *Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive*. Adopted July 13, 2010. Online: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf>. Pp 15.

quarters (GCHQ), the Security Service, Her Majesty's (HM) Revenue and Customs, as well as Communications Service Providers were found to have committed errors, often stemming from technical deficits or human transcription mistakes. In the same year, there were a total of 519,260 requests for communications data from Communications Service Providers; 1,182 errors were found, with two-thirds attributable to public authorities and one-third to Service Providers.[11]

In 2008, there were fifty interception errors and breeches, though again the Commissioner notes in his report that they were accidental. Specifically, they were caused by "human error or procedural error or by technical problems and that in every case either no interception took place or, if there was interception, the product was destroyed immediately on discovery of the error." The Northern Ireland Office/Police Service Northern Ireland, GCHQ, the Security Service, HM Revenue and Customs, Serious Organized Crime Agency, Secret Intelligence Service, Scottish Government, National Technical Assistance Centre, and Communication Service Providers committed errors. In the same year, there were 504,073 requests for communications data from Communications Services Providers, with 595 reported errors. Roughly three-quarters of these errors are attributable to public authorities and the rest to Communications Service Providers and ISPs.[12]

In 2009, there were 36 interception errors and breeches that were attributed to GCHQ, the Security Service, HM Revenue and Customs, the Serious Organized Crime Agency, the Scottish Government, the Metropolitan Police Counter Terrorism Command and National Technical Assistance Centre. During the year, there were 525,130 requests for communications data that resulted in 661 reported errors.[13]

It is important to put these numbers in perspective; in 2008 there were an average of 1,381 requests for citizens' subscriber information and communication data, and against the 2006 numbers this represents a 45% increase in monitoring.[14] Further, there is often a distinction to be made between governmental and public representations of 'errors'. When one family was subject to excessive local council surveillance – 21 separate acts in 3 weeks – to ascertain the family's eligibility to send their children to a local school, the council's lawyer maintained that this act was "minimally invasive of privacy."[15] Another

---

[11] Interception Commissioner. (2008). *Report of the Interception of Communications Commissioner for 2007*. Published July 22, 2008. Online: <http://www.statewatch.org/news/2008/jul/uk-interception-of-comm-report-2007.pdf>

[12] Interception Commissioner. (2009). *Report of the Interception of Communications Commissioner for 2008*. Published July 21, 2009. Online: <http://www.statewatch.org/news/2009/aug/uk-interception-of-communications-2008.pdf>

[13] Interception Commissioner. (2010). *Report on the Interception of Communications Commissioner for 2008*. Published July 27, 2010. Online: <http://www.official-documents.gov.uk/document/hc1011/hc03/0341/0341.pdf>

[14] M. Kennedy. (2009). "Officials seek access to phone and email data 1,381 times a day," *The Guardian*. Published August 10, 2009. Online: <http://www.guardian.co.uk/uk/2009/aug/10/email-phone-intercept-requests-police>

[15] Daily Mail Reporter. (2009). "Only a 'minimal' invasion of privacy: Snooping council spied on family 21 times in 3 weeks," *The Daily Mail*. Published November 6, 2009. Online: <http://www.dailymail.co.uk/news/article-1225755/Snooping-council-claims-invaded-mothers-privacy-minimally-spying-family-21-times-weeks.html>

local council exercised RIPA-based powers when investigating cleaners who were arriving late to work, care assistants who claimed too much on travel expenses, people thought to be selling counterfeit goods on eBay, individuals who applied for false injury claims, and a retailer who sold furniture not meeting fire standards.[16] The usage of legislation for such minor offences seems out of scope with its intention to enhance efforts to combat serious criminal offences and terrorist-related threats.

It is in light of how local councils and law enforcement agencies have actually used RIPA that the Home Secretary is preparing to modify the law. Changes will prevent local councils from using RIPA without magistrate approval if the offence under investigation carries a minimum sentence of 6 months or less.[17] Given how local councils often use systems that invade privacy more than required to conduct investigations (e.g. using CCTV or other direct surveillance when other, less invasive, methods are available), the Information Commissioner noted in 2008 that there is "a continuing failure on the part of authorising officers properly to demonstrate that less intrusive methods have been considered and why they have been discounted in favour of the tactic selected."[18] In addition, the Home Office is planning to modify RIPA so that businesses that provide 'value added' services (e.g. behavioural advertising) will require the consent of both the sender and intended recipient of a communications prior to monitoring communications. This will change the present law, under which surveillance of communications can take place so long as a business (or other party) has 'reasonable grounds' to accept that parties have consented to have communications intercepted.[19]

Present surveillance capacities – and potential for harm – will likely be extenuated if next-generation surveillance practices are implemented. Intelligence agencies are calling for deep packet inspection – capable of monitoring and modifying communications data and content in near real-time[20] – to be deployed throughout ISPs' networks to maintain the surveillance capacities enjoyed during the Cold War. These technologies are included in the 'Interception Modernisation Programme' (IMP) and meant to facilitate "a massive repository of communications traffic data" as well as empower the real-time capturing of

---

[16] Lancashire Press. (2010). "Lancashire County Council uses snooping powers," *Lancashire Evening Post*. Published January 25, 2010. Online: <http://www.lep.co.uk/news/lancashire_county_council_uses_snooping_powers_1_134943>

[17] "Local Authorities Would Require Approval From Magistrates Before They Can Use RIPA Powers for Surveillance – Home Secretary," *eGovMonitor*. Published January 27, 2011. Online: <http://www.egovmonitor.com/node/40488>

[18] "Councils 'still abusing spy laws'" *BBC*. Published July 21, 2009. Online: <http://news.bbc.co.uk/2/hi/uk_news/politics/8162192.stm>

[19] Home Office. (2011). "Regulation of Investigatory Powers Act 2000: Proposed Amendments Affecting Lawful Interception – A Consultation. A summary of Responses." Online: <http://www.homeoffice.gov.uk/publications/consultations/ripa-effect-lawful-intercep/ripa-lawful-intercept-responses?view=Binary>

[20] For a detailed background on deep packet inspection, see: C. Parsons. (2009). "Deep Packet Inspection in Perspective: Tracing its lineage and surveillance potentials," *New Transparency Project Working Paper*. Online: <http://www.christopher-parsons.com/Academic/WP_Deep_Packet_Inspection_Parsons_Jan_2009.pdf>. See also: C. Parsons. (2011). "Is Your ISP Snooping On You?" in M. Moll and L. Shade (eds.). *The Internet Tree: The State of Telecom Policy in Canada 3.0*. Ottawa: Canadian Centre for Policy Alternatives. Pp. 83-92.

content traversing the Internet.[21] In a London School of Economics report, titled "Briefing on the Interception Modernisation Programme," the authors note that IMP does not *maintain* but instead *extends* surveillance practices into novel communications environments and systems.[22] Given the increasing volumes of Internet traffic, as well as fragmentation of communications protocols, hosts, and increasing use of data encryption, deep packet inspection will be of dubious value in the long term.[23] The programme calls for the retention of email and website destinations[24] and would be configured by GCHQ to permit wiretaps and communications data collection in near real-time.[25] The UK Information Commissioner's Office has publicly stated that "[o]n the face of it, the proposal seems disproportionate when any perceived benefits that might be gained from retaining this data are set against the risks to privacy involved."[26] This corresponds with earlier concerns raised by mobile ISPs.[27]

United States

In 1994, the US enacted the Communications Assistance for Law Enforcement Act (CALEA) that imposed interception capabilities on telecommunications service providers. Following its passage, the Federal Communications Commission (FCC) ruled that carriers must be CALEA compliant by June 30, 2002.[28] For the past decade, law enforcement has strongly advocated for the retention of communications content, with this issue recently (re)arising during Congressional hearings.[29] The history of US domestic surveillance is rife with problems: mass warrantless surveillance, misuses of national security letters, harassment of minority communities, and failures to properly audit how

---

[21] C. Williams. (2009). "Spy chiefs size up net snoop gear," *The Register*. Published April 21, 2009. Online: <http://www.theregister.co.uk/2009/04/21/imp_dpi/>

[22] Policy Engagement Network. (2009). "Briefing on the Interception Modernisation Programme," *London School of Economics and Political Science.* Online: <http://www.lse.ac.uk/collections/informationSystems/research/policyEngagement/IMP_Briefing.pdf>

[23] A. Ramos. "Deep packet inspection technologies," in Harold F. Tipton and Micki Krause (eds.) *Information and Security Management Handbook (Sixth Edition), Volume 3*. New York: Auerbach Publications.

[24] T. Whitehead. (2010). "Every email and website to be stored," *The Telegraph*. Published October 20, 2010. Online: <http://www.telegraph.co.uk/technology/news/8075563/Every-email-and-website-to-be-stored.html>

[25] C. Williams. (2010). "Green light for spooks' net snoop plan," *The Register*. Published October 20, 2010. Online: <http://www.theregister.co.uk/2010/10/20/imp_coalition/>, see also R. J. Aldrich. (2010). *GCHQ: The uncensored story of Britain's most secret intelligence agency*. Harper Press: London. Chapter 26 discusses the hopes and aspirations of GCHQ and its public discussions about IMP.

[26] Kable. (2010). "ICO concerned over interception modernisation programme," *The Register*. Published October 25, 2010. Online: <http://www.theregister.co.uk/2010/10/25/ico_concerned_about_net_data_storage>

[27] C. Williams. (2009). "Mobile networks line up to bash net snooping plan," *The Register Hardware*. Published December 22, 2009. Online: <http://www.reghardware.com/2009/12/22/mobile_imp/>

[28] D. Valiquet. (2006). "Telecommunications and Lawful Access: II. The Situation in the United States, the United Kingdom and Australia," *Library of Parliament, Parliamentary Information and Research Service*. Published February 28, 2006. Online: <http://www2.parl.gc.ca/Content/LOP/ResearchPublications/prb0566-e.html>

[29] J. Vijayan. (2011). "DOJ seeks mandatory data retention requirement for ISPs," *Computerworld*. Published January 25, 2011. Online: <http://www.computerworld.com/s/article/9206379/DOJ_seeks_mandatory_data_retention_requirement_for_ISPs?taxonomyId=17>

(and why) surveillance is being conducted. Together, these problems have caused individuals, and society more broadly, to experience harm.

Preservation and Provision of Data

Both governmental and private actions can force ISPs to preserve and provide data. Data preservation is required per the Digital Millennium Copyright Act (DMCA). Under the DMCA, private parties (e.g. agents of the Recording Industry Association of America) can contact ISPs to preserve subscribers' identifying information based on IP address logs. 'Preservation Requests' are typically the precursor to legal action.[30] Law enforcement can also request access to stored data under the Stored Communications Act, which lets law enforcement retrieve and examine stored records (e.g. email) and subscriber information. Requirements to access data under this Act range from probable cause search warrants (lacking notice requirements) to subpoenas (with notice requirements).[31]

In addition to accessing stored data, CALEA requires communications providers to make their systems intercept ready. Prior to CALEA's enactment, industry argued that compliance costs would be between $3 and $5 billion, with the FBI estimating costs between $500 million to $1 billion. Industry subsequently lowered estimates to $1.3 billion, though, at the time, this excluded VoIP-based communications. In evaluating costs, the U.S. Department of Justice, Office of the Inspector General Audit Division stated that it was "skeptical as to whether CALEA's implementation cost can be determined with any degree of specificity."[32] As of 2004, the Inspector General was unable to determine concretely how compliant carriers were with CALEA, though by the FBI's suggested numbers only 10 to 20 percent of wireline equipment was CALEA compatible, roughly one half of pre-1995 wireless switches were compliant, and 50 to 90 percent of wireless switches installed post-1995 were CALEA compliant.[33] These assertions were made without the FBI having an auditing system to ascertain CALEA compliance. The stated aim of CALEA was for the FBI to mandate an 'engineered capacity' capable of monitoring 10% of the nation's telephone lines.[34]

Under CALEA, transactional data content is commonly captured by law enforcement using pen registers or trap and trace devices. Whereas a pen register reveals outgoing phone information (e.g. numbers entered), a trap and trace captures incoming calling data that can be used to identify the "originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents

---

[30] Information Technology Security. (2010). "Notice to Students about P2P and File Sharing: Preservation Requests," Texas State University (San Marcos) IT Security Resources. Last Updated July 16, 2010. Online: <http://security.vpit.txstate.edu/awareness/digital_copyright_p2p_filesharing/notice_to_students-p2p.html#req>. For an example of a preservation letter, see: http://gato-docs.its.txstate.edu/vpit-security/awareness/Sample-Preservation-Request.pdf

[31] See 18 USC § 2703(b)(1) (2000 & Supp 2001)

[32] U.S. Department of Justice, Office of the Inspector General Audit Division. (2004). "Audit Report 04-19 - Implementation of the Communications Assistance for Law Enforcement Act by the Federal Bureau of Investigation," US Department of Justice. Online: <http://cryptome.org/calea-audit.htm>

[33] *Ibid.*

[34] W. Diffie and S. Landau. (2007). *Privacy on the Line: The Politics of Wiretapping and Encryption (Second Edition)*. Cambridge, Mass.: The MIT Press. Pp. 220-221.

of any communication."[35] Together, these devices let law enforcement identify "communications records in real time, such as phone numbers dialed, "to: and "from: information associated with email messages and the IP addresses of computers to which a suspect connects."[36] The uses of transactional capture processes have risen dramatically since their formal recordings of use in 1987. In 1987, there were 1682 pen register and 97 trap and trace orders; in 1998, there were 4886 pen registers and 2437 trap and traces; in 1999, there were 4949 pen registers and 1554 trap and traces; and, most recently, in 2009, there were 12,444 pen registers and 11,091 trap and traces.[37]

The FBI uses National Security Letters (NSLs) to access information without judicial review on national security grounds. NSLs are used to retrieve financial, telecommunications, and credit information and to limit recipients from disclosing their reception of the letter. With these letters, the FBI can collect "[h]istorical information on telephone calls made and received from a specified number . . . and local and long distance billing records"; "[e]lectronic communication transactional records (e-mails), including e-mail addresses"; "screen names"; and "billing records and method of payment."[38] NSLs do not permit the FBI access to the actual content of communications. Significantly, the USA PATRIOT Act modified the conditions under which the FBI can obtain information with NSLs. Today, NSLs can be used so long as information is relevant to an investigation aimed at preventing acts of terrorism or espionage. Further, any field office can issue these letters[39] and 'community of interest'[40] provisions were regularly added to the boiler language of NSLs.[41]

In late 2009, it was disclosed that a vast swathe of information was being released to authorities that was (likely) being excluded from the surveillance statistics that Congress requires law enforcement and intelligence agencies to maintain and make available. As examples, Sprint Nextel provided law enforcement with over 8,000,000 hits from its customers' Global Positioning System (GPS) information between September 2008 and October 2009, and Cricket Communications received 200 requests for data each day.[42] Since

---

[35] U.S. Legal Code. "Section 3127(3)." Online: <http://www.law.cornell.edu/uscode/18/3127(3).html>
[36] C. Soghoian. (2011). "Law Enforcement Surveillance Reporting Gap (Draft V. 1.1)," Online: <http://www.digitallymediatedsurveillance.ca/wp-content/uploads/2011/04/Soghoian-Surveillance-reporting.pdf>
[37] ibid.
[38] DOJ, *Office of the Inspector General, A Review of the Federal Bureau of Investigation's Use of National Security Letters* ("OIG Report on NSLs") x–xiv (Mar 2007). Online: <http://www.usdoj.gov/oig/special/s0703b/final.pdf>. From P. Ohm. (2008). "Reviving Telecommunications Surveillance Law," *University of Chicago Law Review, Vol. 75.*
[39] P. Ohm. (2008). "Reviving Telecommunications Surveillance Law," *University of Chicago Law Review, Vol. 75.*
[40] Circles of interest model groups of individuals in terms of their position in a social network. This position determines their status, and sometimes also predicts social capital – the ability to mobilize social resources and act – as well.
[41] [41] U.S. Department of Justice, Office of the Inspector General. (2010). "A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records," *Department of Justice*. Published January 2010. Online: <http://www.justice.gov/oig/special/s1001r.pdf>
[42] C. Soghoian. (2009). "8 Million Reasons for Real Surveillance Oversight," *slight paranoia (blog)*. Published December 1, 2009. Online: <http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html>

government reports address only the 'live' capturing of data using CALEA intercept equipment, there is no formal reporting about the stored data being collected by authorities from providers such as Google, Yahoo!, Microsoft, and other private communications providers.[43] This said, Facebook disclosed in 2009 that each day it received between 10-20 requests from law enforcement looking for data,[44] and AOL noted in 2006 that it received roughly 1,000 requests per month for data.[45] Google recently launched their "Transparency Reports," which tracks the number of requests from law enforcement to provide or take action on Google-stored data. Between January 2010 and July 2010, there were 4,287 data requests with only 128 being requests to remove content.[46] Reports do not include data that is captured under the warrantless wiretapping system operated by the National Security Agency (NSA) that 'listens in' on foreign and domestic communications utilizing digital systems.[47] Further, it is unclear how much public data is being used and combined with government-proprietary data or data accesses through other access requests; Homeland Security is known to have collected data from social networking sites in developing threat assessments for President Obama's inauguration[48] and 'fusion centers' regularly combine sensitive government data with publicly assessable data sets to derive inferences and actionable intelligence.[49] In aggregate, branches of the US government are significantly invested in the capture, interception, retrieval, and monitoring of American communications content and traffic data.

Audit Formats

In 1968, Congress passed the Omnibus Crime Control and Safe Streets Act. This Act required the Administrative Office of the US Courts to generate reports on wiretap usage by police forces. Reports providing detailed information had to be submitted to Congress each year. As noted by Soghoian, the reports reveal "the city or country, the kind of interception (phone, computer, pager, fax), the number of individuals whose communications were intercepted, the number of intercepted messages, the number of arrests and convictions that resulted from the interception, as well as the financial costs of the wiretap."[50] Wiretap requests have expanded dramatically, with only 637 in 1987 and 2,376 in

---

[43] *Ibid*. It is important to note that, since 2005, federal authorities do not require probably cause to track physical locations. See: http://arstechnica.com/old/content/2005/12/5823.ars.

[44] N. Summers. (2009). "Walking the Cyberbeat," *Newsweek*. Published March 1, 2009. Online: <http://www.newsweek.com/2009/04/30/walking-the-cyberbeat.html>

[45] S. Hansell. (2006). "Increasing, Internet's Data Trail Leads to Court," *New York Times*. Published February 4, 2006. Online: <http://www.nytimes.com/2006/02/04/technology/04privacy.html>

[46] Google. (2011). "Transparency Report." Online: <http://www.google.com/transparencyreport/governmentrequests/>

[47] J. Bamford. (2008). *The shadow factory: The ultra-secret NSA from 9/11 to the eavesdropping of America*. New York: Doubleday.

[48] Tech Talk. (2010). "Homeland Security Harvested Social Network Data," *CBS News*. Published October 14, 2010. Online: <http://www.cbsnews.com/8301-501465_162-20019629-501465.html>

[49] K. Dilanian. (2010). "'Fusion centers' gather terrorism intelligence – and much more," *Los Angeles Times*. Published November 15, 2010. Online: <http://articles.latimes.com/print/2010/nov/15/nation/la-na-fusion-centers-20101115>; see also R. Singel. (2009). "Newly Declassified Files Detail Massive FBI Data-Mining Project," *Wired*. Published September 23, 2009. Online: <http://www.wired.com/threatlevel/2009/09/fbi-nsac/>

[50] C. Soghoian. (2011). "Law Enforcement Surveillance Reporting Gap (Draft V. 1.1)," Online: <http://www.digitallymediatedsurveillance.ca/wp-content/uploads/2011/04/Soghoian-Surveillance-reporting.pdf>

2009. 96% of the wiretaps in 2009 were for mobile phones. With the detailed statistics that are provided, we know that a few jurisdictions are responsible for a considerable portion of the wiretaps that are requested; in 2006, California, New York, New Jersey, and Florida accounted for 59% of all wiretap orders.[51] Further, we know that while encryption is occasionally encountered whilst trying to wiretap a suspect, encryption has never prevented law enforcement from retrieving the plain text of communications.[52] The Administrative Office has regularly, and faithfully, provided their reports since required to by the 1968 Act.[53]

Reports have been less forthcoming about pen registers and trap and trace devices. While the Pen Register Act requires that a list detailing the period of interceptions authorized by order and number, duration, and extension of orders, along with the specific offence(s) under which the order(s) are given be published, this accounting has been performed irregularly. Between 1999-2003, there was a single document dump that failed to detail all the information required under the Pen Register Act, and there is no evidence that reports were filed for 2004-2006. All reports include *only* Federal activities; states' actions are not accounted for. If state uses of pen registers and trap and trace devices parallel the rise of state-drive wiretaps, it is possible that states are conducting more communications data-based surveillance (in aggregate) than the federal government.[54]

Even weaker audits exist for traffic data and communications content accessed under the Stored Communications Act. This act requires that when law enforcement demands access to data on grounds of exigent circumstances that the attorney general records such requests and provides a yearly exigent circumstances report to the House and Senate Judiciary Committee. Such reporting is meant to operate as a check against misuse of exigent provisions.

A recent report provided by the Oversight and Review Division of the Office of the Inspector General found that the FBI has grossly abused their surveillance-related powers. The Bureau has not kept adequate records, has misled the courts, and has violated the Electronic Communications Privacy Act (ECPA) over the course of exercising their surveillance powers. The report notes that the FBI only corrected errors in their processes "after the OIG found repeated misuses of its statutory authority to obtain telephone records through NSLs or the ECPA's emergency voluntary disclosure provisions." 'Sneak peaks', where agents of telecom companies provide warrantless access to databases and let FBI agents check records of phone numbers (and sometimes provide additional information about the telephone record), were pervasive and likely made more common by situating FBI agents alongside telecom companies' employees. Sneak peaks also led to

---

[51] P. Ohm. (2008). "Reviving Telecommunications Surveillance Law," *University of Chicago Law Review, Vol. 75.*

[52] C. Soghoian. (2011). "Law Enforcement Surveillance Reporting Gap (Draft V. 1.1)," Online: <http://www.digitallymediatedsurveillance.ca/wp-content/uploads/2011/04/Soghoian-Surveillance-reporting.pdf>

[53] *Ibid*.

[54] P. Ohm. (2008). "Reviving Telecommunications Surveillance Law," *University of Chicago Law Review, Vol. 75.*

telecom companies performing 'Community of Interest' analyses on the behalf of the bureau.[55]

Susan Landau has developed an excellent summary of the deficiencies concerning FBI usage of exigent circumstances, sneak peeks, and NSLs:

- Many exigent letters never received the required legal follow-ups and the FBI often failed to determine if existing NSLs covered cases where exigent circumstances were being used to quickly access records. As a consequence hundreds of telephone records were purged because there were no legal bases to request the information in the first place.
- Private data was often provided to the FBI without a formal legal request.
- Only 11% of exigent letters were suitably specific about what information was being requested.
- Community-of-interest software was often used without first determining if the information the tool provided was relevant to the investigation.
- Exigent letters were often unrelated to genuine emergencies.
- Sneak peeks were often used to determine what data was available about particular individuals and, where the information was of interest, exigent circumstances letters were then used to access the 'peeked' data.
- The FBI would submit information to the Foreign Intelligence Surveillance Court and claim that it had been obtained using NSLs that were obtained weeks after the information had actually been collected.[56]

While the Foreign Intelligence Surveillance Act (FISA) requires annual reports to Congress, they are of limited analytic usefulness because they note only (a) total numbers of applications for electronic surveillance; (b) total number of orders and extensions that are ordered, modified, or extended.[57] While numbers have expanded dramatically – from 748 orders in 1997 to 2,181 in 2006 – they compress physical and electronic searches and exclude the President Bush's warrantless wiretap system.[58]

Finally, there are Department of Justice processes such as "Hotwatches" – which let authorities track individuals in real-time via "credit card companies, rental car agencies, calling cards, and even grocery store loyalty programs" – that are seemingly excluded from any formal reporting or auditing mechanism.[59] So too are the 'data laundering' pro-

[55] U.S. Department of Justice, Office of the Inspector General. (2010). "A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records," *Department of Justice*. Published January 2010. Online: <http://www.justice.gov/oig/special/s1001r.pdf>
[56] S. Landau. (2011). *Surveillance or Security: The Risks Posed by New Wiretapping Technologies*. Cambridge, Mass.: The MIT Press. Pp. 193-195.
[57] 50 USC § 1807 (2000).
[58] P. Ohm. (2008). "Reviving Telecommunications Surveillance Law," *University of Chicago Law Review, Vol. 75.*
[59] R. Singel. (2010). "Feds Warrantlessly Tracking Americans' Credit Cards in Real Time," *Wired*. Published December 2, 2010. Online: <http://www.wired.com/threatlevel/2010/12/realtime>

cesses that intelligence authorities are reputed to utilize in compiling some dossiers on American and foreign citizens.[60]

Harm to Individuals

Harm to individuals is often challenging to identify; the US government has been loathe to admit wrongdoing and has often brushed aside opposition to its surveillance by invoking national security and/or state secrets privileges.[61] The Electronic Frontier Foundation (EFF) asserts that the warrantless wiretapping carried out by the NSA led to AT&T's customers having their privacy violated and that it infringed on constitutional rights.[62] The over collection of information about Americans was so pervasive that even former President Bill Clinton's personal emails were captured.[63]

From an investigation into the FBI's practices, we learn that the Bureau issued exigent letters to collect call data and transactional information about reporters and researchers working with the *New York Times* and *Washington Post*.[64] Such issuance ran contrary to existing policy. Non-exigent surveillance has been harmful to individuals. Specifically, the FBI monitored other reporters on grounds that the reporters may have received leaked information about confidential government activities.[65] Lawyers have also been subject to overzealous government surveillance authorized by post-9/11 surveillance laws, having their phone calls monitored, offices secretly searched, and home searched.[66] Further, the general conditions of CALEA – to require communications providers to make their systems intercept ready – operate as a persistent danger to individuals and society by introducing security and eavesdropping vulnerabilities into otherwise secure communications systems. IBM researcher, Tom Cross, raised such concerns when describing security vulnerabilities in Cisco's wiretapping architecture. These weaknesses would let a criminal "produce a request for interception that had a valid username and password, thus enabling him to get the fruits of a wiretap."[67]

The massive surveillance dragnets have also impacted the perceptions of minority communities in the United States.[68] In one documented case of bureaucratic error, the leaders

---

[60] J. L. Simmons. (2009). "Buying You: The Government's Use of Forth-Parties to Launder Information about 'The People'" *Columbia Business Law Review* Vol. 2009 (3), p. 950.
[61] See EFF. "NSA Multi-District Litigation." Online: <https://www.eff.org/cases/att#197>
[62] EFF. "NSA Spying FAQ." Online: <https://www.eff.org/nsa/faq>
[63] J. Risen and E. Lichtblau. (2009). "E-Mail Surveillance Renews Concerns in Congress," *The New York Times*. Published June 16, 2009. Online: <http://www.nytimes.com/2009/06/17/us/17nsa.html>
[64] U.S. Department of Justice, Office of the Inspector General. (2010). "A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records," *Department of Justice*. Published January 2010. Online: <http://www.justice.gov/oig/special/s1001r.pdf>. Pp. 92-95
[65] U.S. Department of Justice, Office of the Inspector General. (2010). "A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records," *Department of Justice*. Published January 2010. Online: <http://www.justice.gov/oig/special/s1001r.pdf>. Pp. 115-120.
[66] E. Lichtblau. (2006). "U.S. Will Pay $2 Million to Lawyer Wrongly Jailed," *The New York Times*. Published November 30, 2006. Online: <http://www.nytimes.com/2006/11/30/us/30settle.html?_r=2&oref=slogin&pagewanted=print>
[67] S. Landau. (2011). *Surveillance or Security: The Risks Posed by New Wiretapping Technologies*. Cambridge, Mass.: The MIT Press. Pp 196-7.
[68] S. Landau. (2011). *Surveillance or Security: The Risks Posed by New Wiretapping Technologies*. Cambridge, Mass.: The MIT Press. Pp. 207.

of an Islamic Charity were targeted by federal surveillance without warrant.[69] Concerns in minority communities about the use of surveillance are further exacerbated by reports that some fusion centers are increasing their states of alert based on the growing public tolerance of Muslims throughout the United States.[70] The worry is that, under such surveillance, members of these communities may be less willing or interested in integrating with the broader American community, or in assisting law enforcement or intelligence agencies if they suspect one of their members of being dangerous. To date, this circumstance has led to a high-profile refusal to meet with New York Mayor Michael Bloomberg because of racially-motivated surveillance of the city's Muslim population.[71] Thus, individuals are harmed (their dignity infringed upon) as is society (by ostracizing individuals who may help law enforcement in the case of a threat from the minority community and undermining constitutional rights of speech, protections from illegitimate searches, and freedom of association). Such massive surveillance neither protected rights and liberties nor did it make the community noticeably safer from serious criminal activity.

There is also widespread evidence showing that political interests are driving surveillance using both electronic processes and lawful access-style laws, as well as widespread use of human assets to survey peaceful organizations.[72]

Malta, India, France, and Canada in Brief

Lawful access, mandated interception, and data preservation/retention are policy issues that arise around the world. What follows is a brief sampling of the expanded surveillance laws that have arisen in a few countries outside of the UK and US. The intention behind this sample is to show how these laws are more broadly realized and/or expanded over time.

In Malta, police and secret services have rapidly expanded their use of lawful access requests. Whereas in 2008, there were 869 requests, this grew to 4,023 in 2009. Most of the requests were for mobile telephony traffic, with few requests about fixed line telephony or Internet data.[73] Malta's expanded use of surveillance powers corresponds with increases in surveillance actions more generally in countries that have adopted wide-ranging policing and intelligence surveillance laws. While Malta's system is characteristic of those

[69] EFF. "Al Haramain v. Bush," *EFF Cases*. Online: <https://www.eff.org/cases/al-haramain>
[70] North Central Texas Fusion System. (2009). "Prevent Awareness Bulletin." Published February 19, 2009. Online: < http://www.baumbach.org/fusion/PAB_19Feb09.doc>
[71] P. Harris. (2011). "New York Muslims to snub Bloomberg breakfast in surveillance protest," *The Guardian*. Published December 29, 2011. Online: <http://www.guardian.co.uk/world/2011/dec/29/new-york-muslims-snub-bloomberg> A letter from prominent members of the New York Muslim community that addressed city-mandated surveillance is online as well: <http://nobreakfastwithbloomberg.wordpress.com/2011/12/26/hello-world/>
[72] S. Lendman. (2010). "Lawless Spying in America to Obstruct First Amendment Freedoms," *Baltimore Chronicle and Sentinel*. Published October 7, 2010. Online: <http://baltimorechronicle.com/2010/100710Lendman.shtml>
[73] I. Camilleri. (2011). "Police requests for data soar," *Times of Malta*. Published April 19, 2011. Online: <http://www.timesofmalta.com/articles/view/20110419/local/Police-requests-for-private-data-soar.361295>

required by the EU's Data Retention Directive, India is moving toward a broader system, one akin to the UK's. Like the UK, the Indian government is imposing laws that would require communications providers and individuals to turn over decryption keys if so compelled by a lawful authority.[74] This has led the Indian government to pressure firms such as Research in Motion, Google, and Skype to locate some of their servers in India, thus putting the companies' services in a position to be accessible to authorities.[75] While Google continues to resist such demands,[76] RIM is attempting to appease Indian authorities by providing global keys for non-enterprise uses of BlackBerry smartphones (e.g. BlackBerry Messenger Service).[77] India's widespread use of wiretaps – with over one hundred thousand phone taps every year[78] - is regularly mishandled, with "hundreds of illegal wire taps" for every legal case.[79]

In France, there are efforts to expand the scope of communications captured under the Data Retention Directive. Most recently, this effort has seen the French government push for the Loi d'Orientation et de Programmation pour la Performance de la Sécurité Inté (LOPPSI) 2 bill, which includes provisions sanctioning state-backed trojans, the Pericles database that would retain French citizen data, and a requirement that ISPs begin blacklisting some websites.[80] Trojans would "observe, collect, record, save, and transmit" keystrokes and could be installed for four months, after which a judge would need to renew

---

[74] For background articles on UK's decryption key controversy, see: Out-Law.Com. (2007). "UK police and now force you to reveal decryption keys," *The Register*. Published October 3, 2007. Online: <http://www.theregister.co.uk/2007/10/03/ripa-decryption_keys_power/> and K. Fisher. (2007). "UK can now demand data decryption on penalty of jail time," *Ars Technica*. Published October 1, 2007. Online: <http://arstechnica.com/tech-policy/news/2007/10/uk-can-now-demand-data-decryption-on-penalty-of-jail-time.ars>. In the UK, this has been used to target an animal rights activist (J. Leyden. (2007). "Animal rights activist hit with RIPA key decrypt demand," *The Register*. Published November 14, 2007. Online: <http://www.theregister.co.uk/2007/11/14/ripa_encryption_key_notice/>) and ultimately to imprison a man recognized as a non-terror threat on general grounds of maintaining a right to silence throughout police interrogations (C. Williams. (2009). "UK jails schizophrenic for refusal to decrypt files," *The Register*. Published November 24, 2009. Online: <http://www.theregister.co.uk/2009/11/24/ripa_jfl/>

[75] L. Whitney. (2010). "India wants local servers from RIM, Google, Skype," *CNet News*. Published September 2, 2010. Online: <http://news.cnet.com/8301-1009_3-20015418-83.html>

[76] K. Parbat. (2010). "Google won't share encryption keys with Indian sleuths," *The Economic Times*. Published December 16, 2010. Online: <http://articles.economictimes.indiatimes.com/2010-12-16/news/27573679_1_encryption-communication-systems-gmail>

[77] B. Woods. (2011). "RIM security access appeases Indian authorities," *ZDNet UK*. Published January 14, 2011. Online: <http://www.zdnet.co.uk/news/security/2011/01/14/rim-security-access-appeases-indian-authorities-40091440/?s_cid=938>. For more on challenges facing communications providers such as RIM that offer encrypted systems, see C. Parsons. (2010). "Decrypting Blackberry Security, Decentralizing the Future," *Technology, Thoughts and Trinkets*. Published November 29, 2010. Online: <http://www.christopher-parsons.com/blog/technology/decrypting-blackberry-security-decentralizing-the-future/>.

[78] D. Mahapatra. (2011). "Over 1 [hundred thousand] phones are tapped every year," *The Times of India*. Published February 15, 2011. Online: <http://articles.timesofindia.indiatimes.com/2011-02-15/india/28545822_1_lakh-phones-subscriber-base-provider>

[79] A. Khetan, B. Vij-Aurora, and S. Unnithan. (2010). "The secret world of phone tapping," *India Today*. Published December 9, 2010. Online: <http://indiatoday.intoday.in/site/story/the-secret-world-of-phone-tapping/1/122693.html>

[80] N. Anderson. (2010). "Move over, Australia: France taking 'Net censorship lead," *Ars Technica*. Published February 17, 2010. Online: <http://arstechnica.com/tech-policy/news/2010/02/move-over-australia-france-taking-net-censorship-lead.ars>

the software's authorization.[81] French efforts to retain and gain access to data also (now) require service providers to retain customer information in a manner accessible to authorities for investigation purposes. ISPs must retain:

- Identifier of the connection (e.g. IP address);
- Identifier assigned to the subscriber (e.g. login name or pseudonym used to connect to the Internet);
- Identifier of the terminal used to access the Internet (e.g. the Media Access Control address);
- Dates and times of the beginning and end of the connection's use;
- Characteristics of the subscriber's line (e.g. Asymmetric digital subscriber line, call through the public switched network, etc.)

For hosts that provide public online communications, store information, writings, images, sounds or messages, they must retain:

- The identifier of the origin of the communication (originating IP address, or other relevant information such as the mobile phone number or International Mobile Subscriber Identity (IMSI) number of the subscriber);
- The identifier that the system assigns to the information content (uniform resource locator or location on a website's tree structure);
- Protocols that are used to connect to the service (file transfer protocol, MMS, SMS, etc);
- Nature of the operation (e.g. creation, modification, deletion);
- Date and time of the transaction;
- The identifier that the author used when creating or transmitting the content.[82]

France's actions constitute a significant expansion of law enforcement access to stored data that can identify subscribers, and they significantly parallel South Korea's proposed 'Zombie prevention' bill. This bill is intended to enhance computer security whilst permitting law enforcement to examine details of businesses, records, and documents without warrant.[83]

---

[81] N. Anderson. (2009). "Next up for France: police keyloggers and Web censorship," *Ars Technica*. Published May 19, 2009. Online: <http://arstechnica.com/tech-policy/news/2009/05/next-up-for-france-police-keyloggers-and-web-censorship.ars>

[82] C. Wisniewski. (2011). "French law requires service providers to store and surrender passwords," *Sophos Naked Security Blog*. Published April 8, 2011. Online: <http://nakedsecurity.sophos.com/2011/04/08/french-law-requires-service-providers-to-store-and-surrender-passwords/>; E. Freyssinet. (2011). "Enforcement Decree of LCEN on data retention by ISPs and hosters," *Digital Crime: Cybercrime, forensic analysis of digital systems*. Published March 4, 2011. Online: <http://blog.crimenumerique.fr/2011/03/04/decret-dapplication-de-la-lcen-sur-la-conservation-des-donnees-par-les-fai-et-hebergeurs/>

[83] M. Masnick. (2011). "South Korea Wants To Mandate Everyone Must Install 'Security' Software To Prevent 'Zombies'" *Techdirt*. Published March 23, 2011. Online: <http://www.techdirt.com/articles/20110321/00593813570/south-korea-wants-to#>

In Canada, proposals to enhance law enforcement and intelligence agencies' surveillance and data access powers have met with strong criticism. The Government of Canada is intentionally trying to limit resistance to new powers by separating powers into a variety of bills to reduce "the likelihood that privacy and civil society communities would join forces with the telecommunications industry in opposing lawful access."[84] The Government hopes to separate civil advocates, the federal privacy commissioner, and industry, thus limiting their combined capacity to affect significant changes to any lawful access legislation.[85] The Canadian Bar Association has also voiced

> strong concerns about the scope and potential impact of the various proposals. [Their] concerns focus on the profound impact on the privacy of individual Canadians, and particularly on the potential to destroy solicitor client privilege by seizing communications between lawyers and clients. … In our view, all "lawful access" measures must be defined to conform with legal protections and guarantees that safeguard Canadians' rights and freedoms, and be closely monitored to ensure conformity. Prior judicial authorization is central, and blanket consumer agreements without prior judicial authorization or oversight do not meet that test. A heightened level of care and scrutiny is imperative where the interception or search of such communication may infringe on solicitor client privilege.[86]

Given the usage of lawful access provisions in the United States to violate solicitor client privilege as well as to more generally infringe upon citizens' privacy, the Canadian Bar Association's concerns cannot be stated strongly enough. In addition to these parties, Canada's privacy commissioners, privacy advocates, academics, and members of the public have also written, and spoken, publicly about their concerns related to lawful access legislation.

Recommendations and Warnings

Canada may soon have its own lawful access provisions codified into law. In this section, I generalize some of the problems that have arisen as other jurisdictions have struggled with lawful access and data retention/preservation. After noting each problem, I suggest how to mediate subsequent harms or discuss why that facet of the lawful access/preservation policy should be excluded from Canadian law.

Access to Data

Inappropriate access to transactional and content data is a common problem in the UK and US. In the UK, inappropriate access is typically described as accidental or the result

---

[84] M. Geist. (2006). "Ottawa's Divide and Conquer Strategy for Net Surveillance," *Michael Geist Homepage*. Published October 30, 2006. Online: <http://www.michaelgeist.ca/content/view/1504/159/>

[85] The extent to which such division has manifest following the election of the majority Conservative party Government is uncertain. Advocates, academics, and privacy commissioners have been united in their opposition to lawful access legislation, though there have been relatively few industry voices that have publicly raised concerns.

[86] B. A. Tabor. (2006). "Letter concerning lawful access to Ministers Vic Toews, Stockwell Day, and Maxmime Bernier," Office of the President of the Canadian Bar Association. Published July 5, 2006. Online: <http://www.cba.org/CBA/submissions/pdf/06-31-eng.pdf>

of an error. The Interception Commissioner has noted that there are mistaken transmissions of information from communications providers to various branches of government and accidental switching or replacements of phone numbers. It is important to recognize that while such access (and broader surveillance of the population) is rarely noted as serious or a systematic breech of privacy, municipal councils have often been identified as inappropriately using surveillance capabilities to access data (e.g. using CCTV for directed surveillance, accessing communications data for minor infractions).

In the US, the problem is more significant. The US suffers from endemic inappropriate surveillance: the NSA reportedly runs/ran a warrantless wiretapping system with the assistance of major telecommunications providers like AT&T; the FBI has collected information inappropriately; and a large amount of surveillance that is conducted by state and federal authorities alike remains unreported. Without reports, it is challenging to determine if access was appropriate or necessary.

In both the UK and US, branches of government are advocating for stronger data access and preservation powers. While the Data Retention Directive has been largely implemented by the UK, the 'next step' of 'mastering the Internet' will entail massive deployments of surveillance systems throughout communications networks. These new systems will let intelligence and law enforcement authorities immediately access digital communications in real time.[87] Certain factions within the United States are continuing to advocate for systems like those of Europe; the Department of Justice continues to call for ISPs to retain data for two years regardless of whether business practices call for such extensive retention periods,[88] the Defence Department is developing wide-scale systems to monitor Internet traffic,[89] federal law enforcement is requesting extensions of CALEA to include all communications providers (e.g. Facebook, Skype),[90] and the Obama administration has indicated support for extending FBI access to transactional communications data without prior judicial approval.[91]

The American case demonstrates that law enforcement agencies are prone to accessing communications data inappropriately when there is unclear (or lacking) judicial over-

[87] The notion of 'mastering the Internet' initially emerged in the previous labor government (C. Williams. (2009). "Jacqui's secret plan to 'Master the Internet'," *The Register*. Published May 3, 2009. Online: <http://www.theregister.co.uk/2009/05/03/gchq_mti/> and has since been adopted by the present UK coalition government (J. Leyden. (2011). "Spooks want backdoor into your network," *The Register*. Published March 8, 2011. Online: <http://www.theregister.co.uk/2011/03/08/cyber_security_shake_up/>

[88] J. Vijayan. (2011). "DOJ seeks mandatory data retention requirement for ISPs," *Computer World*. Published January 25, 2011. Online: <http://www.computerworld.com/s/article/9206379/DOJ_seeks_mandatory_data_retention_requirement_for_ISPs?taxonomyId=17>

[89] A. Sternstein. (2011). "Defense is building a database to analyze all network traffic," *Nextgov: Technology and Business of Government*. Published January 27, 2011. Online: <http://www.nextgov.com/nextgov/ng_20110127_9318.php?oref=topstory>

[90] C. Savage. (2010). "U.S. Tries to Make It Easier to Wiretap the Internet," *The New York Times*. Published September 27, 2010. Online: <http://www.nytimes.com/2010/09/27/us/27wiretap.html>

[91] E. Nakashima. (2010). "White House proposal would ease FBI access to records of Internet activity," *The Washington Post*. Online: <http://www.washingtonpost.com/wp-dyn/content/article/2010/07/28/AR2010072806141.html?hpid=topnews>

sight. Further, it is *critical* that judges and magistrates are positioned to permit or refuse access to data – a system where magistrates are required to approve of surveillance if certain conditions are met regardless of the court's own judgment is a recipe for inappropriate data access, insofar as it limits actionable court oversight. The need for oversight is especially important where comprehensive content and transactional surveillance instruments are being forcibly installed into communications providers' infrastructures: such instruments lend themselves to whole-scale monitoring of communications traffic and may pose a significant danger to essential civil rights. Everything possible must be done to ensure that access to data is legitimate, adheres to publicly declared policies, and minimally infringes on constitutional and Charter rights and legal safeguards. Further, surveillance powers should not be used in the investigation of minor offences; clear delimitations of the kinds of crimes that can be investigated must be established to prevent the function creep evidenced in the UK, where local councils use RIPA to prosecute minor offences.

Audits

The UK and American examples, along with suggestions by the EU, indicate what kinds of data should be included in audits of surveillance powers. These examples also suggest the potential challenges in conducting the audits themselves. To begin, detailed records and yearly accounting of how and why surveillance laws are drawn upon by law enforcement and intelligence agencies offer insights into state actions. Such insights can assuage fears of improper use of surveillance instruments. In the case of the UK, regular reporting has shown routine improper interceptions of communications traffic data and traffic contents. While the Interception Commissioner's reports do note which bodies improperly access communications and offer a few examples to highlight the types of improprieties, it does not include detailed jurisdictional information that is associated with US Wiretap reports or that is called for by the Article 29 Working Group. Of note, the American wiretap reports also reveal where encryption is encountered and whether it prevents access to plain text communications (to date it has never prevented such access). It is important to retain this bit of information because a federal governmental report has cited encryption as a problem facing Canadian law enforcement.[92]

Unfortunately, the American situation is less positive when turning to pen registers, trap and trace devices, access to communications under the Stored Communications Act, issuance of National Security Letters, FISA reports, or so-called 'hotwatches.' In each of these instances, law enforcement regularly fails to provide reports with regularity or to issue reprimands for inappropriate or false submissions to auditors. Many of the flaws in the US environment may be attributable to problems that the EU's Article 29 Working Party is trying to overcome throughout the EU: a heterogeneity of access and retention/preservation policies accompanied by a variety of auditing requirements.

An optimal audit should provide the public with information about how and why police are exercising surveillance powers and information about which specific judges are au-

[92] Nevis Consulting Group Inc. (2003). "Summary of Submissions to the Lawful Access Consultation," Department of Justice, Canada. Published April 28, 2003. Online: <http://www.justice.gc.ca/eng/cons/la-al/sum-res/sum-res.pdf>

thorizing surveillance and the regularity with which policing bodies draw on these powers. Canada could adopt recommendations from the Working Party in establishing an audit regime by including at least the following in the Canadian audit framework:

1. Number of requests made throughout the year, segmented by month;
2. Number of requests made throughout the year, per province by month;
3. Number of requests made throughout the year, divided between federal, provincial, and municipal requests by month;
4. User data being accessed, containing a delimited series of predefined fields;
5. Traffic data being accessed, containing a delimited series of predefined fields;
6. Traffic content being accessed, containing a delimited series of predefined fields that indicate the kind of traffic being intercepted/accessed;
7. Number of requests made to each communications provider in Canada, as well as number of requests that were responded to, both in a by month format;
8. A code associated with each accessing party, along with the number of times each party has requested either access to, interception of, or preservation of data by month;
9. Judiciary code that identifies which judicial authority authorized the usage of surveillance powers;
10. Request type (e.g. exigent circumstances, interception, subscriber information, data preservation, etc.) along with whether the information led to a prosecution and, where a prosecution was made, the class of the prosecution.[93]

Before any surveillance method is authorized by parliament or instituted by authorities, that method should be situated within the existing audit structure or be a publicly introduced new element to that structure. This would avoid obfuscating novel surveillance practices that is a regular occurrence amongst American authorities. It is critically important to institute a uniform surveillance 'report card'. Such a report would enable the measurement and publication of the government's performance in the area of surveillance, as well as trace the surveillance practices' effects.[94] Soghoian suggests that the courts and companies themselves may take a leading role in providing data for such a report card[95] – or alternative reporting mechanisms – though the Article 29 Working Group worries that private regulation of surveillance reporting and regulation fails to recognize power divisions between communications providers and law enforcement/intelligence.[96]

---

[93] For an extensive 'privacy protective' framework for the sharing of information once it has been accessed, see Kenneally, E. E. and Claffy, K. (2009) "An Internet Data Sharing Framework for Balancing Privacy and Utility." In proceedings of Engaging Data: First International Forum on the Application and Management of Personal Electronic Information. Online: <http://senseable.mit.edu/engagingdata/papers/ED_SII_An_Internet_Data_Sharing_Framework.pdf>

[94] P. Ohm. (2008). "Reviving Telecommunications Surveillance Law," *University of Chicago Law Review, Vol. 75.pp. 310-315.*

[95] C. Soghoian. (2011). "Law Enforcement Surveillance Reporting Gap (Draft V. 1.1)," Online: <http://www.digitallymediatedsurveillance.ca/wp-content/uploads/2011/04/Soghoian-Surveillance-reporting.pdf>. pp. 24-5.

[96] Article 29 Data Protection Working Party. (2010). "Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive." *Europa*.

Imposing fines or other penalties for false or inadequate private reporting may address the Working Group's concerns and advance Soghoian's own proposal, while enabling the compilation of a general report card and report that is issued to the public.

Definitions of 'Transactional' and 'Content' Data

In all countries under discussion, 'transactional data' about the communication and the actual 'content' of the communication tend to be separated. The rationale is that the former provides less information about the individual or the specific nature of the communication – it's less privacy invasive – whereas the latter is intensely invasive. Thus, the former is often accessible without a warrant and the latter typically requires a warrant or statement of exigent circumstances.

Such a division is increasingly problematic. Transactional data is often used to map associations, identify key nodes in communications networks, ascertain the modes of communications, and evaluate geographic locations of conversation participants. Using traffic data, authorities can identify "social agents' status, capacity to mobilize social resources and act (i.e. social capital). This can be discerned via traffic analysis, yielding a map of the social network and position of actors within it."[97] Further, differentiating between content and transactional data can be highly variable, even when capturing the same 'type' of data. As an example, search engines can reveal considerable personal information when individuals perform searches, but these searches arguably only constitute transactional information.[98] Finally, by analyzing transactional information, analysts can determine content, or facts, about an association before its members themselves do. As noted by Strandburg, "[l]ong before there is a name for the association, a platform, or a membership list, the associational pattern is recorded in the relational data. Associations may be evident even before the participants are aware that they have formed a collective enterprise and certainly before participants have made this kind of intentional "joining" decision that is typical for traditional organizations."[99]

As a result of the potential to derive inferences from electronically captured transactional data that can precisely identify facets of a person's life, movement, and behavior, it is critical for authorities to explain to judges how the data will be used and what authorities hope to find prior to receiving permission to collect and analyze the data. It is possible that the scope or depth of the surveillance may require a stronger means of accessing data – perhaps a warrant – or riders to accompany the surveillance that delimit prospective and unplanned uses of the data.

Published July 13, 2010. Online:
<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf>

[97] G. Danezis and R. Clayton. (2008). "Introducing Traffic Analysis," in A. A. Acquisti, S. Gritzalis, C. Lambrinoudakis, and S. D. C. di Vimercati (eds.). *Digital Privacy: Theory, Technologies, and Practices*. New York: Auerback Publications. P. 99.

[98] L. Mitrou. (2008). 'Communications Data Retention: A Pandora's Box for Rights and Liberties', in A. Acquisti and S. Gritzalis (eds.). *Digital Privacy: Theory, Technologies, and Practices*. New York: Auerbach Publications. p 423. See also: C. Soghoian. (2003). "The Problem of Anonymous Vanity Searches'. *I/S: A Journal of Law and Policy for the Information Society* 3/2: 299-318.

[99] K. J. Strandburg. (2008). 'Surveillance of Emergent Associations: Freedom of Associations in a Network Society', in A. Acquisti and S. Gritzalis (eds.). *Digital Privacy: Theory, Technologies, and Practices*. New York: Auerbach Publications. P. 438.

Infrastructural Vulnerabilities

Requiring communications providers to be 'surveillance ready' is, in essence, requiring them to integrate known security vulnerabilities into their systems for law enforcement's later exploitation. Such requirements have led to data breeches at Google, Adobe, and other high-profile technology companies[100] and massive surveillance of Grecian politicians for months-long periods. Politicians including the prime minister and other top government officials were monitored and the perpetrators of the illegal surveillance action were never identified.[101] In essence, CALEA and RIPA require vendors and communications providers to intentionally weaken the security of their systems. Of particular worry are systems that are designed to capture and retain data *prior* to criminal actions taking place as opposed to dragnets deployed *after* an event. As noted by security expert Bruce Schneier, the "latter can work well, but for the former the costs are too high, both social and economic, and the benefits are negligible."[102]

Surveillance systems have regularly been exploited where the wiretapping or other surveillance process is a technically simple task. Economic and temporal costs that make wiretapping and state surveillance more challenging may offset the potential for function creep, as would imposing liabilities on communications carriers that do not ensure that interception or access requests are legitimate and within the scope of defined law.[103] In essence, some degree of friction must be built into the surveillance apparatus to limit an unchecked slide towards expanded uses.

General Dangers to Civil Liberties

Surreptitious government-mandated surveillance is damaging to civil liberties. The fear of being watched "can result in self-censorship. It is not the kind of harm that is easily offset by hypertechnical arguments about encryption and one-way hash functions."[104] Professor Judith Wagner DeCew, who has noted that "surveillance of normal, everyday activities can lead one to be distracted and feel inhibited,"[105] and Professor Julie Cohen, who has argued that pervasive monitoring inhibits choice and "threatens not only to chill the expression of eccentric individuality, but also, gradually, to dampen the force of our aspirations to it"[106] confirm Ohm's position. The Article 29 Working Party also recognizes that data retention, and broad-scale surveillance more generally, is damaging to individuals and society. They base this position on the fact that

---

[100] K. Zetter. (2010). "Google Hack Was Ultra Sophisticated, New Details Show," *Wired*. Published January 14, 2010. Online: <http://www.wired.com/threatlevel/2010/01/operation-aurora/>

[101] J. Kirk. (2007). "Greek Spying Case Uncovers First Phone Switch Rootkit," *PC World*. Published July 12, 2007. Online: <http://www.pcworld.com/article/134398/greek_spying_case_uncovers_first_phone_switch_rootkit.html>

[102] B. Schneier. (2006). *Beyond Fear: Thinking Sensibly About Security In An Uncertain World*. Springer. Pp. 249.

[103] S. Landau. (2011). *Surveillance or Security: The Risks Posed by New Wiretapping Technologies*. Cambridge, Mass.: The MIT Press. Pp. 237-243.

[104] O. Ohm. (2008). The rise and fall of ISP surveillance. *University of Illinois Law Review*. Pp. 1459.

[105] J. Wagner DeCew. (1997). *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithica, New York: Cornell University Press. Pp. 76

[106] J. Cohen. (2007). "Examined Lives: Informational Privacy and the Subject as Object," 52 Stanford Law Review 1373. Pp. 1426,

> the availability of traffic data allows disclosing preferences, opinions, and attitudes and may interfere accordingly with the users' private lives and impact significantly on the confidentiality of communications and fundamental rights such as freedom of expression. These scenarios are unfortunately likely to occur both because of intentional activities and on account of negligent mechanisms.[107]

The concerns around mass surveillance are also recognized by Breyer, who notes that data retention processes in particular violate Article 8 of the European Convention on Human Rights because a great deal of information about a person's private life is revealed when conducting such surveillance. Further, Article 10 (freedom of expression) is impacted if anyone fails to express him or herself for fear of the state's surveillance. Finally, if ISPs are obligated to modify their property to accommodate the state, their protection of property might be violated.[108] Similarly, Crump suggests that mandated data retention violates First and Fourth Amendment rights because the conditions of most data retention (and sometimes even data preservation) are so broad that they violate the principle of narrowly tailoring governmental infringements on speech rights and search protections.[109]

Conclusion

Based on how UK, US, and international lawful access and expanded surveillance powers have been and are being used, it is apparent that Canadian equivalents require strict access guidelines, strong audit functionality, extensive security audits, and considerable consultation with civil rights advocates and members of the judiciary. Access requirements should require judicial oversight and let judges evaluate whether mere 'transactional data' of communications or subscriber data is revealing enough that a full warrant should be required prior to accessing data. Where exigent circumstances are used to bypass typical oversight provisions, there must be strong post-hoc evaluation both of the validity of the claim of exigent circumstances and of how data accessed has been (and is planned to be) used. This is especially important given the FBI's noted usage of exigent circumstances to unjustifiably access otherwise protected data.

Audits must be vigorous and conducted regularly by a neutral third party that can bring punishment to bear if law enforcement, communications providers, or courts are slow to provide necessary information. Whether it would be best to adopt a UK model – creating surveillance and interception commissioners – or further empowering and resourcing existing government bodies is unclear based on comparisons between functional UK and

---

[107] Article 29 Data Protection Working Party. (2010). "Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive." *Europa*. Published July 13, 2010. Online: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf>. Pp. 6.

[108] P. Breyer. (2005). 'Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR'. *European Law Journal* 11: 365-375.

[109] C. Crump. (2003). 'Data Retention: Privacy, Anonymity, and Accountability Online'. *Stanford Law Review* 56/1: 191-229.

US auditing and reporting bodies. A centralized 'surveillance report card' should be provided each year that clearly details who requested access to information or a wiretap, whether it was provided, who authorized it, and what corporations were involved. More discrete information, as noted in the previous 'Audits' section must also be included. If, after the audit, the auditing commissioner finds that a communications provider has not exercised resources to ascertain the validity of a lawful access request, the commissioner should publicly levy a fine and detail the corporation's errors. Standardizing an audit methodology is particular important during a regulation-making stage that will follow the government's passage of lawful access legislation.

Before establishing the technical means of surveillance, experts should be consulted about whether surveillance capabilities may introduce vulnerabilities into the core communications infrastructures that are relied upon by all sectors of the economy, branches of government, and members of the citizenry. The potential for misuse or harm resulting from such a vulnerability must be proportional to the *actual* harm that the infrastructure alleviates – this may require a survey of costs and harm of deploying a surveillance-ready infrastructure after several years of the infrastructure's usage. Where the infrastructure is seen as potentially posing more harm than providing actual benefit, it should be dismantled. A similar audit should be performed to evaluate the prospective and actual impacts that a lawful access/preservation law has on civil liberties versus the harm that is actually resolved only through the use of the infrastructure. Where the infrastructure has only a secondary, or contributory, function in resolving *serious* crimes, it should be re-evaluated and potentially dismantled.

The prospective of lawful access legislation in Canada has regularly raised concerns, fears, and anxieties over how surveillance powers might be realized by law enforcement, intelligence agencies, and other organizations that could gain access to Canadians' communications. Any legislation must be carefully evaluated against those of Canada's allies and friends so we can avoid the pitfalls and problems that bedevil them, while simultaneously building on our allies' successful oversight practices and systems. Such an evaluation demands a slow and methodical development and implementation of new law, accompanied by audits not just of the surveillance subsequently undertaken but also of the law itself. Laws mustn't exist unto themselves after passing into legislation and a responsible government must ensure that no law is passed that citizens would be unwilling to independently pass upon themselves. Any surveillance law that is overbroad, facilitates overzealous enforcement of minor laws, and damages the free speech, search protections, and freedoms of association that are the lifeblood of a democracy is no law that a responsible citizenry could ever be expected to authorize or legislate of its own will. Any law that is so damaging to the fabric of a democracy must be either modified extensively or withdrawn. Such a modification and/or withdrawal process can only be alleviated or avoided if the government is slow, reflective, and inclusive in the consulting, auditing, and modification processes associated with introducing any new surveillance-enabling lawful access legislation.

Appendix I – Listing of Acronyms

BCCLA – British Columbia Civil Liberties Association
CALEA – Communications Assistance for Law Enforcement Act
CCTV – Closed Circuit Television
CPC – Conservative Party of Canada
DMCA – Digital Millennium Copyright Act
ECPA – Electronic Communications Privacy Act
EFF – Electronic Frontier Foundation
EU – European Union
FBI – Federal Bureau of Investigation
FCC – Federal Communications Commission
FISA – Foreign Intelligence Surveillance Act
GCHQ – Government Communications Headquarters
GPS – Global Positioning System
IMP – Interception Modernisation Programme
IMSI - International Mobile Subscriber Identity
ISP – Internet Service Provider
LEA – Law Enforcement Authority
LOPPSI - Loi d'Orientation et de Programmation pour la Performance de la Sécurité Inté
NSA – National Security Agency
NSL – National Security Letter
OIG – Office of the Inspector General
RIPA – Regulation of Investigatory Powers Act
SMS – Short Message Service
MMS – Multimedia Messaging Service
UK – United Kingdom
US – United States
USA PATRIOT Act – Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act
VoIP – Voice over Internet Protocol