Digital Traffic Cops*: Recommendations for the Canadian Cybercrime Initiative*[1]

Jason Young
Gowling LaFleur Henderson Fellow
LL.M. (Candidate) in Technology and Law
Faculty of Law - University of Ottawa
jyoung@lexinformatica.org
PGP KeyID 0x46E11518

[1] This paper is adapted from an earlier, more comprehensive work *Surfing While Muslim: Privacy, Freedom of Expression and the Unintended Consequences of Cybercrime Legislation* (forthcoming *McGill L.J.*, 2004), http://www.innovationlaw.org/pages/swm_jyoung.doc. I remain indebted for the assistance and criticism of many. In particular, I would like to thank the Canadian Social Sciences and Humanities Research Council Anonymity Project for its generous financial support.

"It may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing… by silent approaches and slight deviations from legal modes of procedure."[2]

Introduction

The preamble to the Council of Europe's *Convention on Cyber-crime* sets the stage: new technologies of digitization and networking threaten the traditional means that law enforcement and intelligence agencies have used to catch 'bad guys'.[3] Moreover, now that the bad guys are moving into cyberspace along with everyone else, they have invented new crimes – cybercrimes – which demand new methods to investigate and prosecute. The Main Street 'cop on the beat' has never had it so tough, so the argument continues.[4] Gone are the days of Canter and Siegel's USENET Green card spamming,[5] these new breed of cyber-criminals aren't two-bit lawyers, but crackers, techno-savvy pedophiles and terrorists who thumb their noses at cyber-cops from foreign jurisdictions or behind techno-pseudonymity, and disappear without leaving a trace.

Ostensibly, global cybercrime initiatives are predicated on designing new investigatory powers to maintain the *status quo* for law enforcement. The stated public policy objective of the *Convention* as well as its national subsidiaries in countries such as Canada, the United States and the United Kingdom, is to maintain lawful electronic

---

[2] *United States* v. *Bach*, (18 November 2002), No. 02-1238 (8th Cir. 2002) (Brief of *Amicus Curaie* Electronic Privacy Information Centre at 4) (citing *Boyd* v. *United States*, 116 U.S. 633 at 636 (1886)).
[3] Council of Europe, Committee of Ministers, 109th, *Convention on Cyber-crime*, ETS No. 185. (2001), preamble [*Convention*], Canada, Dept. of Justice et al., *Lawful Access: Consultation Document* (Ottawa: Justice, 2002) at 3 [Lawful Access].
[4] *See e.g. Convention*, Lawful Access, Canadian Association of Chiefs of Police, *Response To Government Of Canada's Lawful Access Consultation Document*, (Toronto: CACP, 2002) at 32.
[5] P. Lewis, "Sneering At a Virtual Lynch Mob" *The New York Times* (11 May 1994) D7.

surveillance capabilities in the face of new technologies which are making it more difficult for the old tools to work, while preserving and protecting citizens' privacy and other rights and freedoms.[6]

However, these initiatives fail to recognize that the same technologies which make it more difficult for cyber-cops to catch cyber-criminals, also have the potential to become a more encompassing form of social control. In democracies, the efficacy of electronic surveillance is the very rationale for adopting stringent procedural safeguards on its use. As more of our daily activities become instantiated by technology, a society which exposes us, at the whim of the state, to the risk of having a permanent electronic record made every time engage in online activities might be superbly equipped to fight crime, but it would be one in which privacy and freedom of speech no longer had any meaning.[7]

The Canadian government's response has been both short-sighted and, from an international perspective, typical. Under the guise of the *Convention*, the federal government has sought to adopt new requirements to force Internet and telecommunications service providers to authenticate the identity of their subscribers, to make their networks 'surveillance-friendly' and to compel them to produce subscriber 'traffic data' under lower standards than that now required for other types of state surveillance, such as wiretaps and warrants.

This proposal – dubbed "lawful access" – is a case-study in unintended consequences. Applying traditional rules of lawful access – or worse, rules subject to lower standards – to the persistent, pervasive and permanent information realm of

[6] Lawful Access, *supra* note 3 at 6.
[7] *R.* v. *Duarte*, [1990] 1 S.C.R. 30 at 44 (La Forest J.) [*Duarte*].

cyberspace does not simply maintain the *status quo*, but rather introduces unique and dangerous implications for our constitutional rights and freedoms.

Part I of the paper illustrates that legal definitions of "traffic data" in the Canadian lawful access proposal and, by extension, global cybercrime initiatives, fail to adequately recognize the nature of the data actually caught by these definitions. Part II argues that certain characteristics of the Internet lead cyber-citizens to believe they enjoy more privacy than they actually do, and makes concerns about these rights more poignant. Part III suggests that the rationale of the Canadian lawful access proposal is ill-defined, the public policy objectives poorly-constructed and the potential unintended consequences both numerous and unconstitutional. The paper concludes with recommendations for improving the proposal.

Part I: What is "traffic data"?

There is no international consensus on a definition for traffic data. Instead, each country or organization has adopted their own definition, some more broad than others.[8] The Canadian cybercrime proposal uses "telecommunications associated data" to mean any data "pertaining to the telecommunications functions of dialing, routing, addressing or signaling…" and seeks to justify a lower expectation of privacy in this data using a tautological argument: "the standard for Internet traffic data should be more in line with that required for telephone records and dial number recorders in light of the lower

[8] *See e.g. Convention*, *supra* note 3, Art. 1, *Regulation of Investigatory Powers Act 2000* (U.K.), 2000, c. 23, *Communications Assistance for Law Enforcement Act*, 47 U.S.C. §§ 1001-1010 (1994).

expectation of privacy in these types of data."[9] However, a consideration of the types of data often included in the definition of "traffic" and the nature of digital communications, generally, should cast serious doubt on any argument that it should not attract a reasonable expectation of privacy.

The following example illustrates traffic data in an analog context.

Figure 1: Traffic data on a plain old telephone system (POTS)

20021021070824178 165 0187611205 **6139574222** ----------001------003sth 46 **5145281768**-----0013 1410260

Caller at (613) 957-4222 makes a phone call at 7:08:24 AM on October 21, 2002 to recipient at (514) 528 1768 for 3 minutes and 20 seconds.

The two following examples[10] illustrate, digital traffic data can reveal categories of information wholly unrelated to the routing and addressing of the message.

Figure 2: Traffic data from two callers on a wireless network (~GSM)

time GMT=20010810010852 Cell ID=115 MAC ID=**00:02:2D:20:47:24 (A)**
time GMT=20010810010852 Cell ID=115 MAC ID=**00:02:2D:04:29:30 (B)**
time GMT=20010810010852 Cell ID=115 MAC ID=00:60:1D:21:C3:9C
time GMT=20010810010853 Cell ID=129 MAC ID=00:02:2D:04:29:30
time GMT=20010810010854 Cell ID=129 MAC ID=00:02:2D:1F:53:C0
time GMT=20010810010854 Cell ID=129 MAC ID=**00:02:2D:04:29:30 (B)**
time GMT=20010810010854 Cell ID=129 MAC ID=**00:02:2D:20:47:24 (A)**
time GMT=20010810010856 Cell ID=41 MAC ID=00:02:2D:0A:5C:D0
time GMT=20010810010856 Cell ID=41 MAC ID=00:02:2D:1F:78:00
time GMT=20010810010900 Cell ID=154 MAC ID=00:02:2D:0D:27:D3

On August 10, 2001 at 1:08:52 AM, cellphone user A was in radio cell 115 (Dorval Airport) with cellphone user B and both traveled together at 01:08:54 am to cell 129 (Hilton Hotel).

[9] Lawful Access, *supra* note 3 at 12.
[10] Adapted from 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], online: <http://www.it.kth.se/~aep/private/cnglobal2002-escuderoa.ppt> (date accessed 19 Oct 2002).

Figure 3: Traffic data from a user connecting to a web server

295.47.63.8 - - [05/Mar/2002:15:19:34 +0000] "GET/cgi-bin/htsearch?config
=htdigx&words=startrek HTTP/1.0"20 2225
295.47.63.8 - - [05/Mar/2002:15:19:44 +0000] "GET/cgi-bin/htsearch?config
=htdig&words=startrek+avi HTTP/1.0"200x
215.59.193.32 - - [05/Mar/2002:15:20:17 +0000] "GET/cgi-bin/htsearch?config=
htdig&words=Modem+HOWTO …
192.77.63.8 - - [05/Mar/2002:15:20:35 +0000] "GET/cgi-bin/htsearch?config
=htdig&words=conflict+war HTTP/1.0"200
211.164.33.3 - - [05/Mar/2002:15:21:32 +0000] "GET/cgi-bin/htsearch?confi
g=htdigx&words=**STD**+**clinic**+**Kingston**…
211.164.33.3 - - [05/Mar/2002:15:21:38 +0000] "GET/cgi-
bin/htsearch?go=1&do=nw&ct=NA&1y=US&1a=**1234**+**Main**+**Street**
&1p=&1c=**Kingston**&1s=**ON**&1z=**K7L**+**3H4**&1ah=&2y=US&2a=**300**+**1st**+**Avenue**&2p=&2c=
Kingston&2s=**ON**&2z=**K4E**+**4T5**&2ah=&lr=2&x=83&y=10
211.164.33.3 - - [05/Mar/2002:15:22:05 +0000] "GET/cgi-bin/htsearch?config
=htdigx&words=**taxi**+**info**
82.24.237.98 - - [05/Mar/2002:15:25:29 +0000] "GET/cgi-bin/htsearch?confi
g=htdigx&words=blind+date HTTP/1.0

On March 5th 2002, Internet surfer at IP 211.164.33.3 searched for information on Kingston STD clinics, driving directions from 1234 Main St., Kingston, ON K7L 3H4 to 300 1st Avenue, Kingston, ON K4E 4T5 and taxi info.

It should be obvious that the privacy implications of the data collected in *Figure 1* compared to that collected in *Figures 2* and *3* are potentially considerably less serious; there is simply less information available to inappropriately collect, use and disclose. However, the data in all three figures would be captured by most legal definitions of "traffic data", despite the fact that they are contextually very different. Insofar as a label or an analogy reinforces the idea that "traffic data" is separate from and different than "content" it ignores the fact that in digital communications the line between what is merely traffic and what is content blurs considerably.

Canadian courts have yet to address the traffic/content dichotomy, but U.S. courts have had the opportunity in a number of instances and found it a false one. In *Doubleclick*,[11] a district court considered how traffic and content information could be

[11] *In re Doubleclick, Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 514 (S.D.N.Y. 2001) [*Doubleclick*] ("GET information is submitted as part of a Web site's address or 'URL,' in what is known as a 'query string.' For example, a request for a hypothetical online record store's selection of Bon Jovi albums might

one and the same thing. In *Pharmatrak*, the U.S. 1st Circuit Court of Appeals unequivocally found that data of the kind captured by the "GET" method in *Figure 3* was content[12] under the federal wiretap statute.[13]

Canadian courts at the highest levels have found a reasonable expectation of privacy in information which tends to reveal intimate details of the lifestyle and personal choices of an individual,[14] even if disclosed to third parties,[15] or regardless of the nature of the information if the individual had demonstrated an expectation of privacy in it by his or her actions.[16] Standing doctrine suggests, therefore, that digital traffic data could be subject to a reasonable expectation of privacy, as that concept has been defined under s. 8 of the *Charter of Rights and Freedoms*.

Part II: Implications of the 'Collapse of the Digital Moment'[17]

Our activities in cyberspace are qualitatively different than many of their offline counterparts in three respects. First, every activity in cyberspace is instantiated by technology such that wherever we go online and whatever we do, we leave behind a trail

---

read: http://recordstore.hypothetical.com/search?terms=bonjovi. The URL query string begins with the '?' character meaning the cookie would record that the user requested information about Bon Jovi.").

[12] *Pharmatrak*, *supra* note 25 at 19-20 ("Transmissions of completed forms, such as the one at Pharmacia's Detrol website, to [Pharmatrak, Inc.] constitute electronic communications… 'contents' when used with respect to any electronic communication includes any information concerning the substance, purport or meaning of that communication. This definition encompasses personally identifiable information such as a party's name, date of birth, and medical condition."); at 11-12 ("Pharmacia used the 'get' method to transmit [*inter alia* names, dates of birth, and medical conditions] from a rebate form on its Detrol website").

[13] 18 U.S.C. § 2510(4) ("'intercept' means the aural or other acquisition of the *contents* of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.").

[14] *R.* v. *Plant*, [1993] 3 S.C.R. 281 at 293 [*Plant*].

[15] *Schreiber* v. *Canada (Attorney General)*, [1998] 1 S.C.R. 841 at 854 [*Schreiber*].

[16] *R.* v. *Shearing*, 2002 SCC 58 at paras. 167 and 112, *R.* v. *Law*, 2002 SCC 10 at para. 16.

[17] With apologies to S. Vaidhyanathan, *Copyrights and Copywrongs*, (New York University Press: New York, 2001) c. 5.

of data. This data are recorded, often aggregated and linked to create profiles of us as visitors, consumers or members of virtual communities. This persistence, pervasiveness, and permanence of traffic data about our activities in cyberspace changes the nature of the information itself, independent of what individual datum represent.

Second, our widespread techno-illiteracy about what actually takes place behind the screen encourages us to make false assumptions about the capabilities and the extent of surveillance we may be exposed to when engaging in online transactions. The new Panopticon's strength is that we participate voluntarily, seeing only the obvious advantages – convenience and choice – not the less tangible and more complex disadvantages.[18]

Other structural characteristics of the Internet lend themselves to this misperception. In most cases, our email addresses and pseudonyms reveal little or nothing of our age, gender, nationality, background or geographical location and these proxies give us a certain sense of anonymity. As the caption to the now famous *New Yorker* cartoon reads, "On the Internet, no one knows you're a dog,"[19] or so many would believe.

We need passwords to get on the Internet, to check our email, to participate in online forums and e-commerce and these safeguards give us a certain sense of security. In *U.S.* v. *Maxwell* a U.S. court found that a subscriber had an expectation of privacy in his email because only he could access his password-protected account and there was

[18] Canada, *Annual Report Privacy Commissioner 1998-99* (Ottawa: Office of the Privacy Commissioner, 1999) (Commissioner: B. Phillips) at 1-2.
[19] P. Steiner, *The New Yorker* 69:20 (5 July 1993) 61.

little risk that any messages he sent would be retrieved or read by anyone other than the intended recipients for the same reason.[20]

Opinion polls consistently show that Canadians and Americans are concerned about their privacy in cyberspace,[21] but because most possess a poor appreciation of what actually takes place 'behind the screen',[22] these concerns are not operationalized and actions remain unmitigated.[23] Many times, individuals engage in trust relationships simply because trust is a difficult thing to judge online.[24] In so doing, people assume that the interface protects them from prying eyes and that they enjoy more privacy in visiting Playboy.com from a laptop in the physical solitude of their living rooms than if they were to pick up the magazine in the local corner store.[25]

Third, "traffic data" is an arbitrarily defined legal label designed to classify information as separate from and different than the content of a message. As *Figures 2*

---

[20] [1995] 42 *M.J.* 568, 576 [*Maxwell*].
[21] *Trust and Privacy Online: Why Americans Want to Rewrite the Rules*, (Washington, D.C.: Pew Internet & American Life, 2000), online: Pew <http://www.pewinternet.org> (date accessed: 29 March 2003). *see also* Electronic Privacy Information Center, Public Opinion on Privacy, online: <http://www.epic.org/privacy/survey/default.html> (date accessed: 29 March 2003).
[22] *See* S. Turkle, *Life on the Screen: Identity in the Age of the Internet* (New York: Simon & Schuster, 1995).
[23] *See* EC, Commission, *Legal Aspects of Computer-Related Crime in the Information Society* (Wurzburg: EC, 1998) at 25, online: Europa <http://europa.eu.int/ISPO/legal/en/comcrime/sieber.html> (date accessed: 12 May 2003) [*Sieber Report*] ("One of the main dangers of computer crime is caused by the fact that many private users do not know the threats that they are actually or potentially exposed to.").
[24] *See e.g.* S. Jarvenpaa and S. Grazioli, "Surfing among sharks: How to gain trust in cyberspace" *National Post*, (7 August 2001) M2 (in most cultures, confidence is fostered by close contact between parties, but reputation and size are harder to convey and close customer relationships more difficult to develop in cyberspace than in a traditional physical setting).
[25] *Blumofe* v. *Pharmatrak*, *Inc*. (*In re* Pharmatrak Privacy Litig.),No. 02-2138, 2003 U.S. App. LEXIS 8758 at 11-12 (1st Cir. May 9, 2003) [*Pharmatrak*] (Pharmatrak, Inc., recorded the personal information of 197 visitors to Pharmacia, Inc.'s Detrol.com, a website on bladder control medication, including names, addresses, telephone numbers, email addresses, dates of birth, gender, insurance status, education levels, occupations, medical conditions, medications, and reasons for visiting the particular website. Pharmatrak collected the information in contravention of explicit contractual conditions and in contrast to its own representations); the third-party collection, which was invisible to the data subject, was also in contravention of Pharmacia's own privacy policy which stated that "[p]ersonally identifiable information [would] not be sold, rented or exchanged outside of Pharmacia unless the user [was] first notified and expressly consent[ed] to such transfer.", online: Internet Archive <http://shorl.com/hinudryfrestoma> (last updated: February 2001).

and *3* illustrate, it relies on an obsolete analogy. The line between traffic and content is a not a bright one and, frequently, not even the technology experts know where it lies.[26]

American courts have adopted the notion that "what a person knowingly exposes to the public" he or she cannot logically expect to be protected within the sphere of a reasonable expectation of privacy.[27] In *U.S.* v. *Hambrick*,[28] the court found that in knowingly disclosing non-content information to a third party, the defendant lost any expectation of privacy in that information. In that case, "non-content" actually referred to subscriber information as opposed to traffic data, although the latter was clearly contemplated.[29] Similarly, the 6th Circuit Court of Appeals found in *Guest* v. *Leis*, that subscribers do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person, the system operator.[30]

However, the determination of reasonable expectation has not often turned on that point in Canadian law. Instead, as articulated in *Schreiber*, the Supreme Court has chosen to focus the analysis on how "closely linked to the effect that a breach of that privacy would have on the freedom and dignity of the individual."[31]

The Canadian cybercrime initiative echoes the *Convention* in suggesting that because the search and seizure or surveillance would take place without intruding on the physical sanctity of the subject's home, it would be less invasive.[32] However, this ignores

---

[26] *Ibid.*
[27] *See e.g. Smith* v. *Maryland*, 442 U.S. 735, 744 (1979) ("[P]etitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record. In these circumstances, petitioner assumed the risk that the information would be divulged to police…") [*Smith*].
[28] 2000 U.S. App. LEXIS 18665 (4th Cir., 2000).
[29] *Ibid* at 11-12 (citing interpretation in *Smith*, *supra* note 27 at 741-742 that since pen registers do not acquire the contents of communications, they do not attract Fourth Amendment protection; petitioner had no expectation of privacy in traffic data).
[30] 255 F.3d 325, 335-336 (6th Cir., 2001).
[31] *Schreiber* v. *Canada (Attorney General)*, [1998] 1 S.C.R. 841 at 854 [*Schreiber*].
[32] Explanatory Report to the *Convention on Cyber-crime* at para. 171; *Lawful Access*, *supra*, note 3 at 11.

the fact that technology has inverted the proximity of personal information to the subject to such an extent that invasions of privacy rarely ever take place within the confines of one's house or person, but more often through the complicity of third party holders of personal information. Breakthroughs in technology in the 1970's and 80's have made it possible for the private sector to collect, combine, store, manipulate, and exchange vast amounts of data quickly and at ever-diminishing cost.[33] By the early 1980s, the private sector overtook the state as the primary threat to privacy, upsetting Orwell's dystopic vision of one Big Brother in favour of many little ones.

Canadian courts have found that a reasonable expectation of privacy is not founded on the location of the information in which the expectation is held.[34] Records that "could reveal incredibly intimate and personal details about his preferences, habits, opinions, hopes and activities" were deemed to attract a reasonable expectation of privacy despite the fact they were held by third parties in remote locations.[35]

Part III: The unintended consequences of a legislated approach

There is a presumption that governments introduce legislation to remedy specific problems. Unfortunately, a foundation criticism of the Canadian cybercrime proposal must be the lack of empirical – or anything beyond anecdotal – evidence that the

[33] C. Berzins, "Protecting Personal Information in Canada's Private Sector: The Price of Consensus Building" (2002) 27 *Queen's L.J.* 609 at 616.
[34] *Del Zotto* v. *Canada (Minister of National Revenue)* (1997) 147 D.L.R. (4th) 457 (SCC).
[35] *Ibid* at 478.

legislative amendments proposed are actually required to solve a specific market failure.[36]

Stanford law professor Lawrence Lessig has observed that more than law alone enables legal values, and law alone cannot guarantee them.[37] In cyberspace, and in cybercrime investigations, frequently code and technical standards are as important as law. The Canadian proposal claims that technology lies at the root of many of the difficulties now faced by law enforcement and national security agencies in their efforts to investigate and prosecute crime in cyberspace. However, empirical surveys of the impediments which law enforcement faces support a different conclusion: that improved *technological* and *administrative* solutions would substantially address the public policy objectives of lawful access.[38]

There is a metaphorical parallel to the dilution of judicial oversight, which can shed light on potential consequences. Under highway safety legislation in many Canadian provinces and U.S. states, the thresholds for vehicular search and seizure have been lowered in a manner similar to that now proposed in the Canadian and other cybercrime initiatives. Police officers can conduct random roving stops of motorists anywhere and at anytime. There is no need for law enforcement to justify a stop nor can judicial oversight be effective because there is no objective criteria against which a judge can measure an officer's belief that such action was justified.

---

[36] Section 195 of the *Criminal Code* requires the Solicitor-General to annually publish reports on authorizations for interceptions of private communications (s. 185), authorizations given for emergency interceptions without reasonable diligence (s. 188), and interceptions made in the preceding year. However, the Solicitor-General has failed to table this report to Parliament for over two years, *see* T. Hamilton, "Powers snoop more, explain less" *The Toronto Star* (24 Mar 2003).
[37] L. Lessig, "The Law of the Horse: What Cyberspace Might Teach" (1999) 113 *Harv. L. Rev.* 501.
[38] M. Vatis, "The Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Needs Assessment" (Hanover, NH: Institute for Security Technology Studies, 2002) at 10-12, online: Dartmouth College <http://www.ists.dartmouth.edu/lep/lena.htm> (date accessed: 24 October 2002).

To a greater degree than in Canada, courts and commentators in the United States have acknowledged that unlimited police discretion to stop and search will result in the harassment of racial or cultural minorities or be used as a pretext for investigation of unrelated criminal activity. A lower threshold encourages individual police officers to make subjectively-based assessments which can, in turn, too easily mask discriminatory conduct. This has been widely acknowledged by the courts, in academic literature, social science data and the media in both Canada and the United States.[39] Second, a lower threshold precludes effective judicial and public oversight of inevitable constitutional violations. Some Canadian courts have more recently acknowledged that the lack of judicial oversight is problematic and have sought to read down discretionary powers for investigatory detentions.[40] Contrary to this growing awareness, the Canadian cybercrime initiative proposes broad investigatory powers under lower thresholds and, in so doing, ignores the lessons learned from investigative detentions in North America.[41]

Reduced judicial oversight and the natural predilection of even the most fair-minded person to prejudge their perceptions has, in the context of highway safety, led down a slippery slope of subjectivity that many Black North Americans euphemistically call "DWB", the offence of "Driving While Black".[42] The reality is that while discretion is the hallmark of individualized justice, it can easily contain the seeds of inequity.

---

[39] *See e.g. R.* v. *Landry* (1986), 25 C.C.C. (3d) 1 at 30 (S.C.C.), *Brown*, *infra* note 40 at para. 94; *see also* "Police Target Black Drivers" *The Toronto Star* (Oct 20 2002), "The Story Behind the Numbers" *The Toronto Star* (19 Oct 2002), "Treatment Differs By Division" *The Toronto Star* (Oct 19 2002).
[40] *See e.g. Brown* v. *Durham Regional Police Force*, (1998), 138 C.C.C. (3d) 1 (Ont. C.A.).
[41] Lawful Access, *supra* note 3 at 11 (claiming production orders "less invasive", contemplating lower expectation of privacy in traffic data), 12 (interpreting *Plant* to suggest that some types of data should not require judicial authorization).
[42] *See* D. Harris, Driving While Black: Racial Profiling On Our Nation's Highways (Special Report) (New York: ACLU, 1999), online: ACLU <http://www.aclu.org/profiling/report> (date accessed: 9 Nov 2002); K. Meeks, *Driving While Black: Highways, Shopping Malls, Taxicabs, Sidewalks: How to Fight Back if You are a Victim of Racial Profiling* (New York: Broadway Books, 2000); G. Webb, "DWB" Esquire 131:4 (April 1999) 118.

Without procedural safeguards, discretion will often be exercised in a manner not consonant with the goals and spirit of valid legislative objectives.[43]

In the present political atmosphere and in the context of Canadian cybercrime proposal, it does not take much foresight or even creativity to interpolate 'driving' with 'surfing' and 'Black' with 'Muslim' to imagine that reduced judicial scrutiny could lead to a new cyber-offence, in North America, of "Surfing While Muslim".[44] Salient interests might include a Muslim-sounding name, an IP address from an Arab country or organization, an online purchase of the most recent book by Muslim authors Irshad Manji, Salman Rushdie or any number of others as defined by the personal biases of the individual investigator. Similar discretion could just as easily be applied to any number of groups frequently stereotyped as exhibiting undesirable behaviour, including youths, and the full spectrum of political causes. Legal control becomes a more all-embracing form of social control.

Recommendations

The Canadian cybercrime initiative fails to account for the nature of the technology it seeks to regulate and, in so doing, sets a dangerous precedent in Canadian law. Unfortunately, the Canadian situation is not unique. Many nations, including the

[43] *See e.g.* K. Lunman, "Muslims 'threatened' by new law, group says" *The Globe & Mail* (15 May 2003) A7 (Muslim group argues discretionary powers under the *Anti-terrorism Act*, S.C., 2001, c. C-41 used to profile Muslims citizens.).
[44] J. Young, "Surfing While Muslim: Privacy, Freedom of Speech and the Unintended Consequences of Cybercrime Legislation" *McGill L. J.* (forthcoming spring 2004).

United States, have already started down this road. The following recommendations speak to a more thoughtful approach.

First, policymakers must recognize that new technologies collapse old distinctions and sometimes create new ones. A long, broad approach to technology regulation – a certain humility – would likely do much to improve legislated responses.

Second, policymakers must recognize that there is a synergy between the market, technology, law and policy that precludes looking at the individual components out of context. Failure to do so will result in, at least, unintended consequences and, at worst, exacerbation of the problem the regulations seeks to address.

Third and finally, constitutional rights should never be abrogated for anecdotal or anything less than clearly identified market failures. This is particularly true in the technology space, where pundits frequently confuse hyperbole with fact and code plays an ever more important role in the construction of legal rights and norms.