SURFING WHILE MUSLIM: PRIVACY, FREEDOM OF EXPRESSION & THE UNINTENDED CONSEQUENCES OF CYBERCRIME LEGISLATION

A Critical Analysis of the Council of Europe Convention on Cyber-crime
& the Canadian Lawful Access Proposal

By Jason M. Young[†]

ABSTRACT

The Canadian government's *Lawful Access* discussion paper fails to provide empirical – or anything beyond anecdotal – evidence that the legislative amendments proposed are actually needed. Evidence derived from U.S. law enforcement agencies suggests that technological and administrative impediments – more than legal ones – are the cause of most difficulties experienced in cybercrime investigations and prosecutions, specifically: insufficient basic record keeping by telecommunications and Internet service providers; inability to effect data preservation extraterritorially; inability to circumvent encryption; and, a lack of common data-sharing protocols.

Under the guise of international obligations, the government seeks to adopt new legal investigatory tools, the effect of which would be a dilution of judicial oversight for the production of digital "traffic data" in criminal investigations. These initiatives fail to address the fact that value is inherent in all technology and must be factored into the application of laws which seek to regulate new technologies. Unlike the analog analogue, digital traffic data will often reveal a great deal about one's lifestyle, intimate relations or political or religious opinions. Canadian courts have unequivocally found that information of this nature is subject to the highest constitutional protections, particularly in the criminal investigation context.

The *Lawful Access* consultation paper misinterprets the Supreme Court's standard for finding a 'reasonable expectation of privacy', by failing to distinguish between the nature of information contained in the various categories of traffic and the label "traffic data", which is otherwise legally meaningless. 'Traffic data' should attract a reasonable expectation of privacy under the *Plant* doctrine if it passes within the permeable walls of the biographical core or, under the *Shearing* and *Law* doctrines, if the owner of the information held a subjective reasonable expectation of privacy in the data, regardless of its content. Such an expectation could flow *inter alia* from the nature of the relationship between a subscriber and a provider.

By their nature, packet-mode communication intercepts are liable for massive infringement of third party Charter rights, which the Supreme Court held in *Thompson* can be determinative of constitutionality. Further, investigatory tools for packet-mode communications

[†] B.A., LL.B., LL.M. Although all errors are my own, I remain indebted to many people for their assistance and criticism in the drafting of this paper: Lemma Eljallad, Fred Carter, Alan DeKok, Gus Hosein, Mr. Justice Stephen Hunter, Russell McOrmond, Matt Skala, John Swaigen, Clare McCurley and Professors Arthur Cockfield, Colin Bennett and Ian Kerr. I would also like to thank the University of Dayton School of Law, the University of Toronto Centre for Innovation Law and Policy and the Social Sciences and Humanities Research Council Anonymity Project for their generous financial support and the editors of the *International Journal of Communications Law & Policy*, Boris Rotenberg, Simone Bonetti and Nimrod Kozlovski for their valuable feedback on the drafts of this paper, and for their patience.

cannot separate traffic and content data, necessitating a high reasonable expectation of privacy standard for both.

The government's discussion paper claims that production orders – executed by third party telecommunications or Internet service providers – would be less invasive than traditional search warrants. This arguments overemphasizes the physical aspect of a search and fails to recognize that § 8 of the Charter of Rights and Freedoms protects people, not places or things against unreasonable search and seizures.

The history of investigatory detentions under highway safety legislation shows that subjectively-based assessments can too easily mask discriminatory conduct by law enforcement. Contrary to popular understanding, discrimination is a corollary of discretion, not a synonym for racism. It is not a 'dirty word', but simply an accepted condition that must be factored into the administration of the law. Diluted judicial oversight in the context of cybercrime investigations expands law enforcement and third party discretion to discriminate and could lead to the *de facto* offences of, for example, 'surfing while Muslim', or belonging to any negatively-stereotyped group in cyberspace.

Applying traditional rules of *Lawful Access* to the persistent, pervasive and permanent information realm of cyberspace introduces new and unique implications for privacy and freedom of expression. The efficacy of electronic surveillance is such that it has the potential to annihilate any expectation that our communications will remain private. A society which exposes us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we send an email or visit a web site might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning. Consequently, proposed legal 'solutions' to what are often technological or administrative dilemmas may not be the most equitable approach for extending effective policing and intelligence authority to cyberspace. To the extent that governments choose legal tools to investigate and prosecute 'cybercrimes', great care must be taken that they do not abrogate existing constitutional protections.

In theory there is no difference between practice and theory, in practice there is.

– Yogi Berra

I. INTRODUCTION

On 25 August 2002, the Department of Justice, Solicitor-General and Industry Canada issued *Lawful Access*, a public consultation document which proposed amendments to several important federal statutes including the Criminal Code.[1]

Among other measures, the proposals sought to introduce several new investigatory powers which would grant law enforcement, regulatory and national security agencies access to telecommunications and Internet service provider ("ISP") subscriber and "traffic data", under a lower threshold than that now required for search warrants.

The Criminal Code and other statutes generally provide that state agencies cannot obtain documents or information without first establishing a factual foundation of 'reasonable and probable' grounds that an offence has been or will be committed. This requirement serves two purposes: first, it is a check against the unfettered discretion of law enforcement to look for and

[1] DEPARTMENT OF JUSTICE, ET AL., LAWFUL ACCESS: CONSULTATION DOCUMENT (2002) *available at* http://canada.justice.gc.ca/en/cons/la_al/law_access.pdf (last visited 1 Dec. 2004).

collect evidence of crime at the expense of individuals' Charter rights; and, second, it creates a record of accountability subject to audit of abuse of authority and defects in the law.

This discussion begins with a consideration of some of the impediments faced by law enforcement in the investigation and prosecution of "cybercrime."

The paper next addresses the question of what are Canada's obligations under the Council of Europe's Convention on Cyber-crime, on the assumption that the government will ratify the treaty.

The analysis of the procedural amendments can be separated into five areas of consideration. First, what is the rationale for judicial scrutiny of electronic surveillance? Second, what are the implications of assuming a lower expectation of privacy in digital "traffic data"? Third, what is the nature of the relationship between a subscriber and a service provider with regards to expectations of individual privacy? Fourth, what are the constitutional implications of imprecise surveillance tools? Finally, what lessons can we apply in the context of *Lawful Access* from the adoption of less rigorous investigatory standards in a seemingly unrelated field: highway safety legislation?

II. IMPEDIMENTS TO CYBERCRIME INVESTIGATIONS ADDRESSED BY THE LAWFUL ACCESS INITIATIVE

As a preliminary matter, it should be noted that the *Lawful Access* document did not provide sufficient background for proper assessment of impediments to the effective investigation of cybercrime. There is a presumption that governments introduce legislation to remedy specific problems. It should be easy enough then, to find evidence that the amendments proposed in the *Lawful Access* document are indeed required to remedy specific problems. Unfortunately, a foundation criticism of the *Lawful Access* document and the public consultation, generally, is that it lacked empirical – or anything beyond anecdotal – evidence that the legislative amendments proposed are actually needed.[2] As Professor Michael Geist comments: "[T]he proposal merely points to the need to comply with the cybercrime treaty as the primary rationale for many of the reforms."[3] This observation was repeated by individuals at civil society consultations held in Ottawa, Montreal and Vancouver in the fall of 2002.

The Solicitor-General's *Annual Report on the Use of Electronic Surveillance* for 2001, the latest year for which figures have been released, show that applications for authorization

[2] Section 195 of the Criminal Code requires the Solicitor-General to annually publish reports on authorizations for interceptions of private communications (§ 185), authorizations given for emergency interceptions without reasonable diligence (§ 188), and interceptions made in the preceding year. However, the Solicitor-General had failed to table this report to Parliament for more than two years, *see* Tyler Hamilton, *Powers Snoop More, Explain Less*, THE TORONTO STAR, 24 Mar. 2003, at D1.

[3] Michael Geist, *Federal Proposal Tells Only Part of Cybercrime Story*, THE GLOBE & MAIL, 3 Oct. 2002, at B16. *See also* Declan McCullagh, *Will Canada's ISPs Become Spies?*, CNET NEWS.COM, 27 Aug. 2002, *available at* http://news.com.com/2100-1023-955595.html (last visited 1 Dec. 2004).

have decreased between 1996 and 2003.[4] However, the report sheds little light on the reason for the decrease,[5] nor was any representative from either the Department of Justice or the Solicitor-General able to explain the trend when questioned during the consultation phase. Indeed, the Solicitor-General does not even collect statistics on the frequency for which intercepts are authorized but not executed for lack of technical ability to do so.[6]

The lack of basic empirical data demonstrating a need for new surveillance powers – particularly under diluted judicial oversight – is disturbing. While many of the proposals in the consultation document may appear cosmetic, it should never be enough to abrogate constitutional protections by anecdote[7] or for anything less than reasons which are demonstrably justifiable in a free and democratic society.[8] As the U.S. Supreme Court recognized over one hundred years ago, "[i]t 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."[9]

Empirical data from sources outside the consultation suggest that technological and administrative solutions would be more appropriate than legal ones. In June 2002, the Institute for Security Technology Studies at Dartmouth College released a so-called 'needs assessment' on the technological impediments facing cybercrime investigators.[10] To assemble the data and prepare its findings, the ISTS conducted a national survey, held a workshop with key

---

[4] *See generally* SOLICITOR GENERAL OF CANADA, ANNUAL REPORT ON THE USE OF ELECTRONIC SURVEILLANCE 2003, at 6 (indicating that the number of applications made for authorizations to intercept and renewals has fallen: 263 (1995), 162 (1999) to 146 (2001)), *available at* http://dsp-psd.pwgsc.gc.ca/Collection/JS43-2-2001E.pdf (last visited 1 Dec. 2004).

[5] This despite the fact that § 195(3)(b) of the Criminal Code, *infra* note 28, requires the report to set out a general assessment of the importance of interception of private communications for the investigation, detection, prevention and prosecution of offences in Canada. Criminal Code, R.S.C. ch. C-46, § 195(3)(b).

[6] Letter from Duncan Roberts, ATIP Coordinator, Solicitor-General, to Jason Young (11 Mar. 2003), *available at* http://www.lexinformatica.org/cybercrime/pub/solgen_s195.pdf (last visited 30 Mar. 2003).

[7] *See, e.g.*,, CANADIAN ASSOCIATION OF CHIEFS OF POLICE, RESPONSE TO GOVERNMENT OF CANADA'S LAWFUL ACCESS CONSULTATION DOCUMENT 32 (2002), *available at* http://www.lexinformatica.org/cybercrime/pub/cacp_la.pdf (last visited 12 Jan. 2003) [hereinafter CACP] (Appendix A contains a number of anecdotal examples of instances in which law enforcement investigations have been impeded by technology. While interesting, this type of information does little to illuminate the larger justification for abrogating constitutional protections).

[8] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, enacted as Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11, § 1 [hereinafter *Charter*].

[9] Brief of Amicus Curiaie Electronic Privacy Information Centre at 4, United States *v.* Bach, 310 F.3d 1063 (8th Cir. 2002) (citing Boyd *v.* United States, 116 U.S. 633, 636 (1886)).

[10] MICHAEL VATIS, DARTMOUTH COLLEGE: INSTITUTE FOR SECURITY TECHNOLOGY STUDIES, THE LAW ENFORCEMENT TOOLS AND TECHNOLOGIES FOR INVESTIGATING CYBER ATTACKS: A NATIONAL NEEDS ASSESSMENT (2002), *available at* http://www.ist§dartmouth.edu/lep/lena.htm (last visited 24 Oct. 2002).

stakeholders in the law enforcement community, and interviewed law enforcement personnel, including investigators and prosecutors, in seven U.S. states and the District of Columbia.[11]

While the purpose of the assessment was to identify technological impediments and not necessarily legislative or regulatory ones, it is difficult to divorce the two in cyberspace. As Stanford law professor Lawrence Lessig explains, "[t]he *code* of cyberspace – its architecture and the software and hardware that implement that architecture – regulates life in cyberspace generally. Its code is its law."[12]

Many lawmakers and law enforcers suggest that technological problems can and should be addressed by Draconian legal sanctions, even for *de minimis* infractions.[13] Ironically, the Dartmouth assessment seems to suggest that the technological imperative could be a surrogate for legislative and regulatory responses: "Laws, regulations, treaties, and other policy instruments have not evolved to match the new realities facing cyber-attack investigators . . . [t]herefore, the struggle to stay technologically up-to-date promises to become a permanent feature of the law enforcement landscape."[14]

The assessment identified a number of non-technical (or more correctly hybrid) issues commonly impeding cybercrime investigations, namely: insufficient record keeping by ISPs;[15] an inability to effect data preservation extraterritorially;[16] encryption circumvention techniques;[17] and a lack of common data-sharing protocols.[18]

---

[11] *Id.* at 10-12.

[12] LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 35 (2001).

[13] *See, e.g.,*, JASON YOUNG, DIGITAL COPYRIGHT REFORM IN CANADA: REFLECTIONS ON WIPO AND THE DMCA (unpublished manuscript), *available at* http://www.lexinformatica.org/dox/digitalcopyright.pdf (last visited 3 Jan. 2005). *See also* WIPO Copyright Treaty, 20 Dec. 1996, 36 I.L.M. 65. The treaty's preamble recognizes "the need to introduce new international rules and clarify the interpretation of certain existing rules in order to provide adequate solutions to the questions raised by . . . technological developments."

[14] VATIS, *supra* note 10, at 10.

[15] *Id.* at 28-30.

[16] *Id.* at 30.

[17] *Id.* at 34. I enumerate this as a non-technical issue because routine circumvention of encryption by law enforcement would employ largely non-technical methods, *i.e.*, warrants for remote key-logging, legal compulsion of passwords, etc.

[18] *Id.* at 24. This complaint is ironic given that the greatest threat to network neutrality is the desire by law enforcement and commercial actors to build intelligence into the network. Here, the latter recognizes the value that neutral protocols have for development, seemingly wish to emulate that success for investigatory data-sharing, but also seek to optimize the network for one set of uses, namely: authentication, integrity and non-repudiation. *See, e.g.,*, James Speta, *A Common Carrier Approach to Internet Interconnection* 54 FED. COMM. L.J. 274-75 (2002) ("[B]uilding complex functionality into a network implicitly optimizes the network for one set of uses while substantially increasing the cost of a set of potentially valuable uses that may be unknown or unpredictable at design time. The number of new applications developed for the Internet . . . is a testament to that system's flexibility." (Citations omitted).

The impediments were also relatively elementary (*i.e.*, requirements for data collection tools that can parse information from multiple formats, automated and expert data collection tools to minimize requirements for investigator training, databases of subject experts in various jurisdictions, clearinghouses for tools and techniques, investigative tools specifically designed for law enforcement, etc.), suggesting that many of the difficulties investigators now face would be more appropriately addressed in Silicon Valley than in Parliament, Congress or Brussels.[19]

III. CANADA'S LEGAL OBLIGATIONS UNDER THE CONVENTION ON CYBERCRIME

In February 1997, the Council of Europe created a committee to draft "a binding legal instrument" dealing with the creation of new computer-related offences, substantive criminal law, the use of national and international coercive powers and jurisdiction.[20] The first public draft was not released until April, 2000, and was immediately criticized by civil society groups as being both incomplete and not responsive to privacy concerns.[21] The final text was released in June 2001 and opened for signature in September of that year.

On November 23, 2001, Canada, along with 30 other nations, signed the Council of Europe's Convention on Cyber-crime,[22] The stated purpose of the Convention is threefold: to harmonize the domestic criminal substantive law elements of offences and connected provisions in the area of cybercrime; to provide for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means

---

[19] VATIS, *supra* note 10, at 52 ("The entities that develop technological solutions to the obstacles outlined in this study have a singular opportunity. Since the existing technology does not meet cyber-attack investigators' needs, the solutions that are developed may become widely adopted by the law enforcement community."). *See, e.g.*,, Declan McCullagh, *Inside Cisco's Eavesdropping Apparatus*, CNET NEWS.COM, 21 Apr. 2003, *available at* http://news.com.com/2010-1071-997528.html?tag=nl> (arguing that more precise surveillance capabilities in routers would help protect non-targeted third party traffic) (last visited 21 Apr. 2003).

[20] *See* Press Release, Council of Europe, First International Treaty to Combat Crime in Cyberspace Approved By Ministers' Deputies (19 Sept. 2001); COUNCIL OF EUROPE, EXPLANATORY REPORT TO THE CONVENTION ON CYBERCRIME ¶¶ 7-15 (2001).

[21] The first public draft was number 19; the real-time collection of traffic data provision did not reappear until draft 27; *see* GUS HOSEIN, ET AL., ZERO KNOWLEDGE SYSTEMS, AN ANALYSIS OF INTERNATIONAL INITIATIVES ON HIGH-TECH CRIME: A REVIEW OF IMPLICATIONS FOR THE CANADIAN POLICY ENVIRONMENT 17 (2001), *available at* http://www.lexinformatica.org/cybercrime/pub/perrin.pdf (last visited 3 Jan. 2005); *see also* Letter from the American Civil Liberties Union, the Electronic Privacy Information Center and Privacy International to the U.S. Dept. of Justice and the Council of Europe (7 June 2001) (objecting to the "non-transparent manner in which this Convention has been developed.") (on file with the author).

[22] Council of Europe, Convention on Cybercrime, European Treaty Series (ETS) no. 185, *opened for* signature Nov. 23, 2001, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (last visited Feb. 20, 2004) [hereinafter Convention on Cybercrime].

of a computer system; and to create an efficient and effective regime of international cooperation.

A. The Structure of the Convention

The Convention contains four chapters: (1) definitions; (2) substantive and procedural measures to be taken at domestic level; (3) international co-operation; and (4) final clauses.

The Convention's treatment of the substantive law offences stipulates criminal sanctions for child pornography, unauthorized access to a computer and other such offences. These measures are both uncontroversial and largely already found in the Criminal Code. However, the more problematic treatment of procedural measures is the subject of the rest of this essay.

B. Procedural Provisions

Section 2 of Chapter II of the Convention establishes broad procedural powers for the purpose of criminal investigation of the offences established in Section 1, Articles 2 through 11. However, the procedural powers are not limited to only those offences or even to 'cybercrimes' generally.[23] The Convention is directed at any criminal offence committed by means of a computer system and the collection of evidence of any criminal offence where that evidence is in electronic form.[24]

There are two exceptions to the scope of application. First, Article 21 provides that the power to intercept content data shall be limited to a range of serious offences to be determined by domestic law. Second, a party may reserve the right to apply the measures in Article 20 (real-time collection of traffic data) only to specific offences or categories of offences.[25]

The Explanatory Report cautions against adopting the Article 20 reservation, based on the importance of real-time tracing to law enforcement and on the grounds that "the collection of traffic data alone does not collect or disclose the content of the communication" and is therefore subject to a lower expectation of privacy.[26]

---

[23] *See generally* Susan W. Brenner, *Is There Such a Thing as "Virtual Crime"?*, 4 CAL. CRIM. LAW REV. 1 (2001) (concluding that most of the activity currently characterized as "cybercrime" is nothing more than the commission of conventional crimes by unconventional means), BRUCE SCHNEIER, SECRETS & LIES: DIGITAL SECURITY IN A NETWORKED WORLD 15 (2000) (arguing that the threats in the digital world mirror the threats in the physical world). *See also* Scott Berinato, *The Truth About Cyberterrorism*, CIO MAGAZINE, 15 Mar. 2002, *available at* http://www.cio.com/archive/031502/truth.html (last visited 15 May 2003) (use of term "cyberterrorism" is fear-mongering); Albert I. Aldesco, *contra Note: The Demise of Anonymity: A Constitutional Challenge to the* Convention *on Cybercrime*, 23 LOY. L.A. ENT. L. REV. 81, 85 (2002) (author fantastically equates computer viruses with Ebola, one of the most virulent and lethal viruses known to science, with a mortality rate between 50%-90%).

[24] Convention on Cybercrime, *supra* note 22, Art. 14(2)(a-c).

[25] EXPLANATORY REPORT, *supra* note 20, at ¶¶ 142-43 (explaining that the article 20 reservation is subject to the exception that the reservation cannot be narrower than the powers reserved under article 21).

[26] *Id.*

The Dartmouth needs assessment identified real-time traffic data collection as one of the most effective methods of catching cyber criminals.[27] According to the *Lawful Access* document, real-time search of traffic data was already permissible in Canada under either § 487.01 or Part VI of the Criminal Code[28], but it suggested that the standard for intercepting Internet traffic data should be more in line with that required for telephone records and dial number recorders:

> [I]n light of the lower expectation of privacy in a telephone number or Internet address, as opposed to the content of a communication … [a] specific production order could be created under a lower standard in order to allow for the production of telecommunications associated data, that extends beyond the telephone numbers already covered by section 492.2 of the Criminal Code, historic traffic data or real-time collection of traffic data.[29]

Again, the *Lawful Access* document did not provide any background as to why a lower standard was required, but from other sources we learned that the argument was premised on a number of inter-related themes: traffic data is of great evidentiary value to law enforcement and rapid collection is crucial to ensuring availability and integrity of the data; it is often difficult to collect this data; and many parties believe that it should attract a lower expectation of privacy than content data.

Clearly, the evidentiary value of traffic data is an important piece of the cybercrime puzzle. However, when it comes to addressing the best method of getting this evidence into the hands of law enforcement while maintaining adequate protections for privacy, the consensus among stakeholders breaks down.

The *Lawful Access* document suggested that the problem was a lack of legal access to the requisite data, but provides no reasoning for this conclusion. Meanwhile, the Dartmouth needs assessment identified the primary impediments to real-time collection of traffic data as technological (*i.e.*, investigatory tools not specifically tailored to law enforcement needs) and administrative (*i.e.*, lack of coordination between jurisdictions).

Arguably, the most contentious aspect of the Convention and the focus of much of the rest of this paper is found in Article 18, requiring signatories to adopt "production orders" to compel individuals or service providers to produce, respectively, "specified computer data" or "subscriber information" in their possession or under their control.[30] Specified computer data

---

[27] VATIS, *supra* note 10, at 30.

[28] Criminal Code, R.S.C. 1985, ch. C-46, §§ 183-184, 342.1, 342.2, 430.

[29] LAWFUL ACCESS, *supra* note 1, at 11-12; *see also* Provision of Subscribers' Telecommunications Service Provider Identification Information To Law Enforcement Agencies, Order CRTC 2001-279 ¶ 11 (30 Mar. 2001), *available at* http://www.crtc.gc.ca/archive/ENG/Orders/2001/O2001-279.HTM (finding that LSPID information does not reveal intimate details of the lifestyle or personal choices of subscribers, but can only be provided to law enforcement under certain conditions); Bell Canada – Customer Name and Address, Telecom Decision CRTC 2002-52 ¶ 17 (30 Aug. 2002), *available at* http://www.crtc.gc.ca/archive/ENG/Decisions/2002/dt2002-52.htm (information in a reverse-directory is non-confidential; value of warrantless access outweighs the privacy concerns in providing the information).

[30] Convention on Cybercrime, *supra* note 22, Art. 18(1)(a-b).

means any information in a computer, including software applications.[31] Subscriber information includes the type of the communication service used, the subscriber's identity, address, telephone or other access number, period of service and billing and payment information.[32] This provision is circumscribed in Article 15 by a proportionality principle and such conditions and safeguards appropriate in view of the nature of the power or procedure concerned including, *inter alia*, judicial or other independent supervision, grounds justifying application, and limitation on the scope and the duration of such power or procedure.[33]

The *Lawful Access* document identified Article 18 as one of the key amendments required in Canadian law in order to ratify the Convention and proposed the adoption of several types of production orders, including general and specific production orders, subscriber information orders, assistance orders, anticipatory orders, and data preservation orders. This paper will only address the implications relating to general and specific production orders for Internet traffic data, as the most obnoxious to our constitutional notions of privacy and freedom of speech and as the most frequently justified by fallacy.

C. Key Problems

1. A lower threshold for electronic surveillance would be unconstitutional

In the case of serious crime, information is sometimes collected using electronic surveillance. In Canada, as in other democratic countries, this aspect of police investigations occurs under a well-established and rigorous legal framework for the lawful interception of private communications, subject to the principles of the Charter of Rights and Freedoms and strict procedural safeguards in the Criminal Code, not the least of which requires that law enforcement receive prior approval from the courts to engage in such activities.

The rationale for this framework is so obvious that in democratic societies it is sometimes taken for granted. In the words of one Supreme Court justice, "a society which exposes us, at the whim of the state, to the risk of having a permanent electronic recording made of our activities in cyberspace might be superbly equipped to fight crime, but it would be one in which privacy no longer had any meaning."[34] The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private.[35] Ergo, it is unacceptable in a free society that law enforcement be allowed to invade citizens' privacy at their sole discretion or that they be allowed to circumscribe rights through technology that they could not in law.[36]

The Supreme Court recognized the appropriate standard in one of the first cases decided under the Charter of Rights and Freedoms:

---

[31] *Id.* Art. 1(b).
[32] *Id.* Art. 18(3).
[33] *Id.* Art. 15.
[34] R. *v.* Duarte, [1990] 1 S.C.R. 30 at 44 (La Forest J.).
[35] *Id.*
[36] *See, e.g.,*, Kyllo *v.* United States, 533 U.S. 27 (2001); R. *v.* Tessling, 2004 SCC 67.

> The state's interest in detecting and preventing crime begins to prevail over the individual's interest in being left alone at the point where credibly-based probability replaces suspicion. History has confirmed the appropriateness of this requirement as the threshold for subordinating the expectation of privacy to the needs of law enforcement.[37]

Consequently, the Criminal Code generally prohibits law enforcement from obtaining documents or information without first establishing a factual foundation of 'reasonable and probable' grounds that an offence has been or is being committed. This requirement serves two purposes: first, it is a check against the "unfettered discretion"[38] of law enforcement to look for and collect evidence of crime at the expense of individuals' Charter rights; and, second, it creates a record of accountability subject to audit of abuse of authority and defects in the law.

In *R. v. Duarte*, La Forest J. acknowledged Parliament's careful efforts to circumscribe state use of electronic surveillance:

> Law enforcement must always seek *prior judicial authorization* before using electronic surveillance. Only a superior court judge can authorize electronic surveillance, and the legislative scheme sets a high standard for obtaining these authorizations. A judge must be satisfied that other investigative methods would fail or have little likelihood of success, and that the granting of the authorization is in the best interest of the administration of justice… this latter prerequisite imports as a *minimum requirement* that the issuing judge must be satisfied that there are reasonable and probable grounds to believe that an offence has been or is being committed and that the authorization sought will afford evidence of that offence. [T]he provisions and safeguards of the *Code* have been designed to prevent the agencies of the state from intercepting private communications on the basis of mere suspicion.[39]

i. Production Orders

The *Lawful Access* document proposes the creation of a specific production order which would grant law enforcement access to "traffic data" under a lower threshold than that now required for a search warrant or authorization to intercept. Where a new threshold might lie is not made clear, though in their submission in response to the lawful access consultation the Canadian Association for Chiefs of Police suggests the following:

> Procedural safeguards are required in order to ensure that production orders are appropriately employed. Such orders ought to be issued by either a judge or justice who is satisfied by information on oath or solemn affirmation that the officer applying for the order is engaged in the *bona fide* execution of a lawful duty and that the order is reasonable [sic] required in order for this duty to be carried out.[40]

No expectation of privacy exists in traffic data *vis à vis* the recipient of the message. However, traffic data can be obtained from sources besides the recipient of an Internet communication. For example, traffic data is also recorded at the server that uploads the message

[37] Hunter *v.* Southam, [1984] 2 S.C.R. 145, 166-67.
[38] *Duarte*, *supra* note 35, at 32.
[39] *Id.*, ¶ 45 (emphasis added).
[40] CACP, *supra* note 7, at 17.

from the sender, at the computers that pass the packets along from the sender and at the server that reformulates and stores the message until it is downloaded by the recipient.

The Supreme Court has ruled that an order for the production of documents[41] is a seizure within the meaning of § 8 of the Charter of Rights and Freedoms, as is the power to make copies of documents.[42] Therefore, an order for the production of third party records made pursuant to the Code would fall under the ambit of § 8 of the Charter.

The *Lawful Access* document suggested that a lower threshold for production orders was justified because these orders would be less intrusive than a search warrant, "as there would be no entry into and search by law enforcement of the premises of a third party."[43] In *United States v. Bach*, the U.S. 8th Circuit Court of Appeals adopted a similar argument in accepting that civilian searches are sometimes more reasonable than searches by police officers.[44] For example, a search by a civilian software expert could be more reasonable than a search by an officer because the latter lacked the knowledge to differentiate a trade secret from a legitimate computer software program.[45] In *R. v. Plant*, the court found that:

> [t]he place and manner in which the information in the case at bar was retrieved also point[s] toward the conclusion that the appellant held no reasonable expectation of privacy with respect to the computerized electricity records. The police were able to obtain the information on-line by agreement of the [Calgary Utilities] Commission. Accessing the information did not involve intrusion into places ordinarily considered private….[46]

This argument suffers four serious limitations.

First, it overemphasizes the purely physical aspect of a search and seizure at the expense of the impact on the individual to whom the search was targeted and the seized information pertained. In *R. v. Edwards*,[47] the Supreme Court held that "an interpretation of the degree of intrusiveness is not a matter of where the information in question is located, but to what extent disclosure of that information would impact the reasonable expectation of the individual's privacy."[48] It is a well-established principle – and one which is reflected in the court's analysis in *Plant* despite the passage above – that § 8 protects "people, not places or things".[49]

I note the apologetic reminder of the Court in *R. v. O'Connor*:

---

[41] *See, e.g.*,, Thomson Newspapers Ltd. *v.* Canada (Dir. Of Invest. And Research, Restrictive Trade Practices Comm'n), [1990] 1 S.C.R. 425, 517-18; R. *v.* McKinlay Transport Ltd., [1990] 1 S.C.R. 627.

[42] *See, e.g.*,, Comité Paritaire de L'Industrie de la Chemise *v.* Potash, [1994] 2 S.C.R. 406.

[43] LAWFUL ACCESS, *supra* note 1, at 11.

[44] 310 F.3d 1063, 1067 (8th Cir. 2002).

[45] *Id.* (citing Schalk *v.* State, 767 S.W.2d 441, 454 (Tex. Ct. App. 1988)).

[46] R. *v.* Plant, [1993] 3 S.C.R. 281, 295.

[47] [1996] 1 S.C.R. 128, ¶ 34.

[48] *Id.*; *see also* Del Zotto *v.* Canada (Minister of Nat'l Revenue), [1997] 147 D.L.R. (4th) 457, *infra* note 127 and accompanying text.

[49] *See* R. *v.* Colarusso, [1994] 1 S.C.R. 20, 60 (*per* La Forest J.); *see also Plant*, *supra* note 46, at 291; *Hunter*, *supra* note 37, at 158, citing Katz *v.* United States, 389 U.S. 347 (1967); and R. *v.* Dyment, [1988] 2 S.C.R. 417, 428-29.

> Although it may appear trite to say so, I underline that when a private document or record is revealed and the reasonable expectation of privacy therein is thereby displaced, the invasion is not with respect to the particular document or record in question. Rather, it is an invasion of the dignity and self-worth of the individual, who enjoys the right to privacy as an essential aspect of his or her liberty in a free and democratic society.[50]

Second, the argument assumes that the third party search would be more reasonable *because* it is less intrusive. Clearly, there will be situations in which a third party search is not less intrusive and perhaps unreasonable by that aspect. *Bach* itself provides an example: according to intervenor Yahoo!, ISP technicians do not selectively choose or review the contents of the named account, they simply hand over the entire contents in response to a subpoena.[51] This can hardly be seen as less intrusive, given that if the search had been conducted by law enforcement, the execution would be restricted to the terms of the warrant. Unfortunately, the court declined to find on this point.

The third limitation of the government's argument for a lower threshold is that it ignores the capacity of new technologies and new public-private relationships to draw public inferences of private activities such that the location of the search becomes irrelevant in factoring the severity of the intrusion. This point is more nuanced and will be expounded upon in a later section.

Fourth, the assertion that a search of a third party data custodian would be "less invasive" of the data subject's privacy than one of the subject him or herself, also ignores the question of the availability of remedial measures intrinsic to any determination of invasiveness. That is, if a third party stands in place of the subject as the object of unreasonable surveillance, do they have equal standing in law to advance such a claim against the government?

ii. Third-party Intermediaries

Third party intermediaries would not have standing under s. 24 of the Charter for infringements of subscribers' privacy. Section 24(1) reads: "*Anyone whose rights or freedoms*, as guaranteed by this Charter, *have been infringed or denied* may apply to a court of competent jurisdiction to obtain such remedy as the court considers appropriate and just in the circumstances."[52]

The contours of a Charter remedy do much to govern the shape of the protected right. "The question of breach must, therefore, be assessed in terms of the interests protected by the section and such remedy as the court can provide to secure them."[53]

An individual would have no knowledge of a search of personal information held by a third party and therefore no ability to challenge the reasonableness of a search. Current search and seizure law requires notification of the subject of a search or interception after the fact,[54] it

[50] [1995] 4 S.C.R. 411, ¶ 131.
[51] *Bach*, *supra* note 44, at 1065.
[52] Emphasis added.
[53] R. *v.* Rahey, [1987] 1 S.C.R. 588, ¶ 111.
[54] Criminal Code, R.S.C. 1985, ch. C-46, § 189 (5) (notice of intention to produce evidence), § 196 (notification required after interception), § 487.01(5.1) (notice required after covert entry).

would seem at least a partial solution to require that any production order standard incorporate the same requirement.

In claiming that a third party search would be "less invasive," the government would wrongly foist responsibility for seeking remedies for § 8 breaches on third parties with no standing under § 24(1) to enforce them. In *R. v. Thompson*,[55] Sopinka J. was careful to point out that the invasion of third-party privacy rights is not determinative of the reasonableness of the search. That is to say, an abrogation of third party privacy rights in the execution of a warrant would rarely factor into a § 8 challenge. A plain reading of § 24(1) would not grant standing to third parties in such cases.

Wilson J. in *Rahey* interpreted § 24(1) as providing application for remedy only to a person whose rights under the Charter have been infringed.[56] This would necessarily exclude third party standing, even were telecommunications and Internet service providers so inclined to act as guardians of their subscribers' privacy rights.[57]

Section 24(1) is not an exclusive remedy for breach of the Charter.[58] Nor is it necessary for an applicant to argue anything more than a breach of his or her § 8 rights to invoke a remedy under § 24(1) or § 52(1). Any court seized of the dispute has the power and the duty to determine the validity of the statute.[59] However, it seems clear that a § 52(1) remedy is narrower than the range granted under § 24(1). Thus, severance of the § 24(1) remedy or range of remedies for lack of standing is significant, particularly in the context of proposed routinized surveillance of subscribers by intermediaries acting as 'agents of the state'.[60]

---

[55] [1990] 2 S.C.R. 1111, 1143-1144.

[56] [1987] 1 S.C.R. 588, ¶ 61.

[57] Canadian Internet service providers have taken some steps to protect the privacy of their subscribers, but it is not unequivocal. *See* CANADIAN ASSOCIATION OF INTERNET PROVIDERS, CODE OF CONDUCT (2000), *available at* http://www.caip.ca/issues/selfreg/code-of-conduct/code.htm (Article 4 stating "Private information will be disclosed to law enforcement authorities only as required by law.") (last visited 3 Jan. 2005); CANADIAN ASSOCIATION OF INTERNET PROVIDERS, PRIVACY CODE (2000), *available at* http://www.caip.ca/issues/selfreg/privacy-code/privacy.htm (Article 5 stating that member ISPs "will use or disclose personal information only for the purposes it was collected, unless a user gives consent or as required by law.") (last visited 3 Jan. 2005). However, the explanatory note somewhat ambiguously expands on the point with the statement that members "may disclose personal information without consent when required to do so by law, *e.g.*,, subpoenas, search warrants, other court and government orders, or demands from other parties who have a legal right to personal information, or to protect the security and integrity of its network or system." *See also* Jay Thompson, *Liability for On-Line Activity: The Buck Stops Where?* (unpublished paper presented to the IT-CAN Conference, 3 Oct. 2002) (President of the Canadian Association of Internet Providers explaining that in the event of a third-party complaint about content, a member would "then typically advise the complainant to contact the police to pursue the complaint.").

[58] R. *v.* Big M Drug Mart, [1985] 1 S.C.R. 295, ¶ 37.

[59] PETER HOGG, CONSTITUTIONAL LAW OF CANADA 791 (4th ed. 1999).

[60] *Id.* at 773; s*ee, e.g.*,, *Rahey*, *supra* note 53 (comparing the interpretations of Wilson and La Forest JJ. on the theory that the contours of a remedy give shape to the right).

Telecommunications and Internet service providers will be the first line of defence against unreasonable electronic surveillance, particularly under any scheme of diluted judicial oversight. Providers are by default the guardians of informational privacy on the Internet. By offering online services, providers gain access to personal and private information of their many users. Individuals are therefore dependent on those who provide them with online services to keep their private communications secure and confidential.[61]

Presented with narrow constitutional redress, intermediaries will be less inclined to resist unreasonable investigatory demands by law enforcement, even in circumstances when they feel that such demands are unreasonable.

iii. Traffic Data

The *Lawful Access* document suggested that production orders for income tax information and tracking devices for dial number recorders, already extant in the Criminal Code, are analogous precedents for the adoption of production orders for Internet traffic data. This tended to be a common refrain in the law enforcement community. In its submission to the Department of Justice in response to the *Lawful Access* document, the Canadian Association of Chiefs of Police remarked:

> [T]he privacy interests that arise respecting traffic data are relatively low in comparison to those things that require a search warrant to seize. Traffic data can be likened to [Dial Number Recorder] information with respect to the level of confidentiality that it attracts. Therefore, a specific production order for the acquisition of traffic data ought to be established which is equivalent to the process used for obtaining DNR information.[62]

On its face, it is not difficult to distinguish income tax or DNR information from most Internet traffic data protocols: tax information is collected for a necessary regulatory purpose, while the DNR reveals much less about what Sopinka J. in *Plant* termed the 'biographical core'.

> It is fitting that § 8 of the Charter should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state." This "would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.[63]

The phrase 'biographical core' is evocative, but it is perhaps an unfortunate choice of phrase. 'Core' implies a centrality, permanence and fundamental quality which belies the ease with which information can be associated or disassociated with individuals. It also suggests a finite space in which we can locate types of personal information and exclude other types. Neither would be wholly accurate interpretations of the doctrine.

It is true that there are categories of information which, perhaps by statutory embrace, have been labeled personal and confidential in nature *e.g.,* financial and criminal records. These categories of information, for public policy reasons, may always reside within the legal

---

[61] Ian R. Kerr, *The Legal Relationship Between Online Service Providers and Users*, 35 CAN. BUS. L.J. 419, 443 (2001).
[62] CACP, *supra* note 7, at 18.
[63] *Plant*, *supra* note 49, at 293.

protection of the biographical core.[64] However, it would ordinarily be incorrect to interpret the biographical core as an enumeration of categories of information in which individuals would have a reasonable expectation of privacy. Predetermined labels put the cart before the horse and will rarely be determinative in deciding whether constitutional protection extends. Instead, one must look at the total context of the particular information in question.[65] For example, an individual's name in a phone book will attract a lower expectation of privacy than if it was found on a list of debtors or alleged terrorists, even though both may be called a "name".[66] Similarly, that same name in the phone book may attract a higher expectation of privacy if it belongs to a public figure, a victim of stalking or spousal abuse.

Digital traffic data in the hands of the average person may not be personally identifiable, but could take on a very different significance in the possession of someone able to link a pseudonym – either an IP address or some other unique identifier – with a particular individual, either by technical or legal means. Under such circumstances, otherwise non-personally-identifiable data could easily reveal intimate details of an individual's personal lifestyle or private decisions and therefore would be deserving of § 8 protection. This point relates both to the values represented by the data and the relationship of the subject of the data to the third party who is in possession or control of it: both aspects will be explored in more detail later in the paper.

iv. Inconsistent Standards For Criminal Investigations

The *Lawful Access* document suggested that because "production orders already exist in some federal laws, such as the Competition Act" a precedent has been set to create new order powers in the Criminal Code. This comparison failed to distinguish the inquisitorial and compulsive nature of criminal investigations from the regulatory investigations of the *Competition Act* and other statutes.

In *British Columbia Securities Commission v. Branch*, [67] Sopinka and Iacobucci JJ. favourably considered the analysis of the judge at trial in finding that the purpose of the Securities Act was "regulatory and administrative, not criminal or quasi-criminal".[68] The Court

[64] With the notable exception of the Swedish prototype Data Act of 1973, most general data protection statutes promulgated by OECD members in the seventies and eighties included an enumeration of categories of personal information, files or records which deserved explicit protection. *See, e.g.*, Privacy Act of 1974, 5 U.S.C. § 552A(a)(4) "record"; Privacy Act, R.S.C. 1985, ch. P-21, § 3 "personal information".

[65] R. *v.* Wholesale Travel Group Inc., [1991] 3 S.C.R. 154, 209 ("what is ultimately important are not labels (though these are undoubtedly useful), but the values at stake in the particular context").

[66] Englander *v.* Telus, [2004] F.C.J. No. 1935 at para. 65 (C.A.) (finding that a telecommunications provider could not imply a subscriber's consent for the publication of name, address and number in an online directory, nor could the provider deem consent for publication of the same information in a phone book in the case of first-time customers).

[67] [1995] 2 S.C.R. 3.

[68] *Id.* at ¶ 25.

was also careful to make a distinction between personal and business records: "documents produced in the course of a business which is regulated have a lesser privacy right attaching to them than do documents that are, strictly speaking, personal"[69]. Writing for the majority, Lamer C.J. cited La Forest J.'s analysis in *Thomson*:

> While [business] records are not devoid of any privacy interest, it is fair to say that they raise much weaker privacy concerns than personal papers. . . . These records and documents do not normally contain information about one's lifestyle, intimate relations or political or religious opinions. They do not, in short, deal with those aspects of individual identity which the right of privacy is intended to protect from the overbearing influence of the state.[70]

In *R. v. Fitzpatrick* the Court adopted a lower privacy threshold for records "that are statutorily compelled as a condition of participation in the regulatory area. Little expectation of privacy can attach to these documents, since they are produced precisely to be read and relied upon by state officials."[71]

> [I]t cannot be said that using the information contained [in these records is] an affront to individual dignity – a fundamental value that underlies so many Charter rights. For these records divulge nothing about the personality of the individual who has created them. The information recorded is of a purely objective kind, and…. [t]he information divulges nothing of the state of mind, thoughts, or opinions of the individual who has submitted the records.[72]

However, the Court distinguished these records and records in the criminal context: "searches and seizures of documents relating to activity known to be regulated by the state are not subject to *the same high standard as searches and seizures in the criminal context*."[73] and that "the requirement to keep records under the Fisheries Act does not impose any psychological or emotional pressures on the individual, and in this way the state intrusion at issue here *contrasts sharply with inquisitorial and police interrogatories and testimonial compulsion*."[74]

Thus, while production of records in the criminal context should always attract a higher judicial standard, a label as to whether a statutory scheme is "regulatory" or "criminal" should not be determinative in deciding whether an unreasonable search or seizure is authorized. Records produced for and under regulatory requirements may attract § 8 protection if they are subsequently used in the criminal context.[75] Moreover, although business records generally attract a lower expectation of privacy than personal records, this is again not because of any label, but rather because a contextual analysis of what these records typically contain and the purpose for which they were generated suggests that the content will likely not implicate privacy

[69] *Branch*, *supra* note 67, ¶ 62.
[70] *Thomson*, *supra* note 41, at 517-18.
[71] [1995] 4 S.C.R. 154, ¶ 49.
[72] *Id.* at ¶ 51.
[73] *Id.* (emphasis added).
[74] *Id.* (emphasis added).
[75] Baron *v.* Canada, [1993] 1 S.C.R. 416, 444.

interests. This is consistent with the holding of the Court in *Dagg v. Canada (Minister of Finance)*,[76] which dealt with sign-in logs at a workplace:

> In determining whether an individual has a reasonable expectation of privacy in a particular piece of information, it is important to have regard to the purpose for which the information was divulged [by the subject]. Generally speaking, when individuals disclose information about themselves they do so for specific reasons [and] they do not expect that the information will be . . . released to third parties without their consent.[77]

In *Plant*, the Court found that there was no confidential obligation on the part of a utility to one of its customers because the records in question – billing records – "could not reasonably be said to reveal intimate details of the appellant's life since electricity consumption reveals very little about the personal lifestyle or private decisions of the occupant of the residence."[78] In *R. v. Johnston*,[79] counsel for the accused relied on *Plant* in arguing that a digital recording ammeter (DRA) was a much more invasive investigative tool than computerized consumption pattern records and that the information collected was of an intimate and private nature. The Court engaged a contextual analysis of the ability of the DRA to collect information and the nature of the information collected in finding that it was not an unreasonable invasion of privacy:

> [T]he police . . . witnesses for the Crown, along with the defence's witness . . . all confirm that one really cannot tell anything about what appliance a person may be using, if they are home at all, and if so, what they are doing. As Crown counsel indicated, a next-door neighbour or person on the street would likely have more information on what was going on in a house than the information obtained from the DRA. All it does is give a general graph of electrical use, and nothing more. In my view, this does not at all infringe on the privacy rights of an individual as contemplated by the Charter and as set out in *R. v. Plant*.[80]

Defence counsel and the court in *Johnston* relied on *Plant* as authority for the proposition that the interpretation of 'biographical core' must be on the basis that it is permeable and infinite. Information can be outside the biographical core in one context and within it in another. The analysis of that in which an individual has a reasonable expectation of privacy must be a contextual one.

IV. NORMATIVE SUGGESTIONS

A. Traffic data should attract a reasonable expectation of privacy

The *Lawful Access* document argued that traffic data attracts a lower expectation of privacy than other kinds of data, such as the content of a communication. However, in the digital environment, labels like "traffic" and "content" are both outmoded and unhelpful. What is important is an understanding of what values are represented by traffic data. This section reviews

[76] [1997] 2 S.C.R. 403
[77] *Id.* at ¶ 75.
[78] [1993] 3 S.C.R. 281, 293.
[79] [2002] A.J. No. 843.
[80] *Id.* at ¶ 6.

several statutory and international instruments to illustrate the broad scope of traffic data; discusses why digital traffic data might be different than traffic data in an analog environment; suggests a number of reasons why digital traffic data might reveal intimate details of the lifestyle and personal choices; and, concludes with a review of how the courts have approached information of this nature.

1. 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. As will be seen, however, the lack a precise definition hardly frustrates the argument against the rationale for a lower expectation of privacy in traffic data in Canada.

The *Lawful Access* document used "telecommunications associated data" to mean "any data, including data pertaining to the telecommunications functions of dialing, routing, addressing or signaling that identifies, or purports to identify, the origin, the direction, the time, the duration or size as appropriate, the destination or termination of a telecommunication transmission generated or received by means of the telecommunications facility owned or operated by a service provider."

A number of international statutory instruments also define traffic data, including the Convention,[81] and the work of the Group of Eight on cybercrime, in which Canada was a participant and principal drafter.[82] In addition, the European Union, the U.K. and the U.S. have promulgated legislation which includes related definitions.

Under the Convention, "traffic data" means "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."[83]

By comparison, the U.K.'s Regulation of Investigatory Powers Act[84] (RIPA) contains a tortured, but relatively narrower definition of "traffic data" that includes subscriber and routing information and 'post-cut-through' data, or digits dialed after a call has been connected (*i.e.* your

[81] Convention on Cybercrime, *supra* note 22, Art. 1.

[82] In May 2001, the G8 held a high-level public-private workshop on cybercrime, which acknowledged the difficulty of defining "traffic data" and, while providing examples of the categories of data which could fall under the rubric, ultimately settled on the thoroughly unhelpful definition of "not content" data. *See* G8, REPORT ON THE POTENTIAL CONSEQUENCES FOR DATA RETENTION OF VARIOUS BUSINESS MODELS CHARACTERIZING INTERNET SERVICE PROVIDERS (2001), *available at* http://www.mofa.go.jp/policy/i_crime/high_tec/conf0105-4.html (last visited 15 Oct. 2002).

[83] Convention on Cybercrime, *supra* note 22, at c. I, art. 1(d). For a plain illustration of the qualitative and quantitative differences in "traffic data," see A. Pascual, *Access to "Traffic" Data: When Reality is Far More Complicated Than a Legal Definition* (unpublished, 11 Oct. 2002), *available at* http://www.it.kth.se/~aep/private/cnglobal2002-escuderoa.ppt (last visited 19 Oct. 2002).

[84] Regulation of Investigatory Powers Act 2000 (U.K.), 2000, c. 23, *available at* http://www.hmso.gov.uk/acts/acts2000/20000023.htm (last visited 3 Jan. 2005).

bank password if you use telephone banking services).[85] It also includes the data which is found at the beginning of each packet in a packet-mode network, indicating which communications data attaches to which communication. According to the explanatory notes to the RIPA, "the tailpiece to the definition puts beyond doubt that in relation to internet communications, traffic data stops at the apparatus within which files or programs are stored, so the traffic data may identify a server but not a website or page."[86]

The European Union Directive on Privacy and Electronic Communications[87] incorporates a broader, enumerated definition which includes latitude, longitude and altitude of the sender's or recipient's terminal, direction of travel, identification of the network cell in which the terminal equipment is located at a certain point in time, any naming, numbering or addressing information, volume of a communication, network on which the communication originates or terminates, and the beginning, end or duration of a connection.

The U.S. Communications Assistance for Law Enforcement Act,[88] uses a narrower phrase "call-identifying information",[89] which means "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." The definition of "telecommunications carrier" excludes entities engaged in providing information services (*i.e.*, ISPs).[90] However, the newly-enacted USA PATRIOT Act[91] allows ISPs to voluntarily disclose "non-content" information to non-government entities for any purpose and to law enforcement in more limited circumstances.[92] The act also expands the information that law enforcement can seek from a service provider with only an administrative subpoena – and without notice to the subscriber[93] – to include records of session times and durations, temporarily assigned network addresses; and, means and source of payments, including credit card or bank account numbers.[94]

---

[85] *Id.* at § 2(9).

[86] Explanatory Notes to Regulation of Investigatory Powers Act 2000, *available at* http://www.hmso.gov.uk/acts/en2000/2000en23.htm (last visited 15 Oct. 2002).

[87] Council Directive 2002/58/EC of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) ¶ 15.

[88] 47 U.S.C. §§ 1001-1010 (1994).

[89] 47 U.S.C. § 1001(2).

[90] 47 U.S.C. § 1001(8) "telecommunications carrier" ((A) means a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire; . . . but (C) does not include (i) persons or entities insofar as they are engaged in providing information service§ . . .)). 47 U.S.C. § 1002(b)(2) exempts information service providers from assistance capability requirements.

[91] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001). The act is not a stand-alone statute, but rather an omnibus amendment to 15 other acts. *Available at* http://www.shorl.com/gipukufudrotu (last visited 15 Oct. 2002).

[92] *Id.* § 212, (amended at 18 U.S.C.§ § 2702 (2003)).

[93] *But see Doe v. Ashcroft*, No. 04 Civ. 2641, slip op. at 113 (S.D.N.Y. Sept. 28, 2004) (

[94] *Id.* §§ 210-11, (amended at 18 U.S.C.§ 2703(c)(2) (2003)).

2. Digital traffic data should attract § 8 protection because it can reveal intimate details of lifestyle and personal choices, is often collected, used and disclosed without an individual's knowledge or consent and is vulnerable to abuse.

The *Lawful Access* document sought to justify a lower expectation of privacy in traffic data by 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 expectation of privacy in these types of data."[95] 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.

Our activities in cyberspace are qualitatively different than many of their offline counterparts in three respects. First, wherever we go online and whatever we do, we leave behind a trail of data. This data are recorded, often aggregated and linked to create profiles of us as visitors, consumers or members of virtual communities. Information and communication technology is evolving so quickly that sometimes it is difficult to predict its impact, but one trend is clear: as our activities expand in cyberspace, the volume of data recorded about people will continue to grow dramatically. The persistence, pervasiveness, and permanence of information about our activities in cyberspace changes the nature of the information itself, independent of whether the content of the information reveals intimate details of lifestyle and personal choice. If we do not reflect this in policy, privacy will no longer have any meaning in cyberspace.

Second, some of the structural characteristics of the Internet lend themselves to the belief that we enjoy more privacy than we really do. 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. For example, in *United States v. Maxwell*, the U.S. Air Force Court of Criminal Appeals found that a subscriber had an expectation of privacy in his email because only he could access his password-protected account and there was little risk that any messages he sent would be retrieved or read by anyone other than the intended recipients for the same reason:

> In our view, the appellant clearly had an objective expectation of privacy in those messages stored in computers which he alone could retrieve through the use of his own assigned password. Similarly, he had an objective expectation of privacy with regard to messages he transmitted electronically to other subscribers of the service who also had individually assigned passwords. Unlike transmissions by cordless telephones, or calls made to a telephone with six extensions, or telephone calls which may be answered by anyone at the other end of the line, there was virtually no risk that the appellant's computer transmissions would be received by anyone other than the intended recipients.[96]

Further, 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."[97]

[95] LAWFUL ACCESS, *supra* note 1, at 12.
[96] [1995] 42 M.J. 568, 576.
[97] P. Steiner, THE NEW YORKER, 5 July 1993, at 61.

Trust is a difficult thing to judge online and we frequently do it blindly.[98] We assume that the interface protects us from prying eyes and that we enjoy more privacy in visiting Playboy.com from a laptop in the physical solitude of our living rooms than if we were to pick up the magazine in the local corner store, but is this actually true?[99]

Opinion polls consistently show that Canadians and Americans are concerned about their privacy in cyberspace,[100] but because most possess a poor appreciation of what actually takes place 'behind the screen',[101] these concerns remain ill-defined and actions unmitigated.[102] We knowingly exchange personal information only with organizations with whom we have relationships and we do so with the expectation that information will be kept confidential and not used for purposes inconsistent with the collection. However, many people are simply unaware that by visiting a web site, they are exchanging information with not only the operator of that site, but potentially many others as well. For example, while most people have heard of 'cookies', few actually understand how third party advertising networks or market metric companies can and do use cookies to compile profiles from visits to unrelated web sites.[103] In the

[98] *See, e.g.*,, Sirkka Jarvenpaa and Stefano Grazioli, *Surfing among sharks: How to Gain Trust in Cyberspace*, NATIONAL POST, 7 Aug. 2001, at 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).

[99] 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*]. In this case, 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. *Available at* http://shorl.com/hinudryfrestoma (last updated Feb. 2001).

[100] SUSANNAH FOX, ET AL., PEW INTERNET & AMERICAN LIFE PROJECT, TRUST AND PRIVACY ONLINE: WHY AMERICANS WANT TO REWRITE THE RULES (2000), *available at* http://www.pewinternet.org/pdfs/PIP_Trust_Privacy_Report.pdf (last visited 29 Mar. 2003). *See also* ELECTRONIC PRIVACY INFORMATION CENTER, PUBLIC OPINION ON PRIVACY, *available at* http://www.epic.org/privacy/survey/default.html (last visited 29 Mar. 2003).

[101] *See* SHERRY TURKLE, LIFE ON THE SCREEN: IDENTITY IN THE AGE OF THE INTERNET (1995).

[102] SEE EUROPEAN COMMISSION LEGAL ADVISORY BOARD, LEGAL ASPECTS OF COMPUTER-RELATED CRIME IN THE INFORMATION SOCIETY 25 (1998), *available at* http://europa.eu.int/ISPO/legal/en/comcrime/sieber.html (last visited 12 May 2003) [hereinafter 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.").

[103] In re Doubleclick, Inc. Privacy Litigation, 154 F. Supp. 2d 497, 502-05 (S.D.N.Y. 2001) (explaining the mechanics of a third party ad network). IAN GOLDBERG, A PSEUDONYMOUS COMMUNICATIONS INFRASTRUCTURE FOR THE INTERNET 64 (2000). *See also* Joel M. Schwarz, *A*

Pharmatrak case, Pharmatrak, Inc., under contract with client pharmaceutical companies, tracked individual users through a network of sensitive pharmaceutical product Web sites without visitors' knowledge:

> NETcompare was designed to record the webpages a user viewed at clients' websites; how long the user spent on each webpage; the visitor's path through the site (including her points of entry and exit); the visitor's IP address; and, for later versions, the webpage the user viewed immediately before arriving at the client's site (*i.e.*, the "referrer URL"). *This information-gathering was not visible to users of the pharmaceutical clients' websites*. [Footnotes omitted, emphasis added][104]

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. As one former Privacy Commissioner put it, the "new panopticon's [sic] strength is that we participate voluntarily, seeing only the obvious advantages – convenience, speed and personal safety – not the less tangible and more complex disadvantages."[105] This begs the question: if people don't understand how the technology works, how will they modify their behaviour to account for it? Is it fair to measure an individuals' expectations of privacy based on their misperceptions of the collection, use and disclosure of their personal information?

Finally, as the aforementioned definitions illustrate, "traffic data" is an arbitrarily defined label largely designed to classify information as separate from and different than the content of a message. By relying on obsolete analogies, this distinction is often used to justify different treatment for traffic data in law, *e.g.*, traffic data is like the address information on the outside of an envelope.[106] While the traffic/content distinction is accurate in the analog environment, it is highly problematic in the digital environment. The following example illustrates traffic data in an analog context.

> ***Figure 1: Traffic data on a plain old telephone system (POTS)***
>
> **20021021**070824178 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.)

Case of Identity: A Gaping Hole in the Chain of Evidence of Cyber-crime, 9 B.U. J. SCI. & TECH. L. 92, n.4 (2003) ("While a recent spate of alleged privacy violations by various companies has helped to alert the public that Internet sessions are not as anonymous as initially believed, most people fail to appreciate exactly how personal information on the Internet is captured and used.").

[104] *Pharmatrak*, *supra* note 99, at 4.

[105] B. PHILLIPS, PRIVACY COMMISSIONER OF CANADA, ANNUAL REPORT 1998-99, 1-2 (1999).

[106] Robert Hubbard, P. DeFreitas and Susan Magotiaux, *The Internet – Expectations of Privacy in a New Context*, 45 CRIM. L.Q. 170, 192 (2002) ("It is difficult to say that there can be any reasonable expectation of privacy in traffic data. While the sender of a sealed letter may expect the content of the letter to be private, no similar expectation can be held in relation to the outside of the envelope.").

However, as the two following examples[107] illustrate, traffic data in the context of digital networks can easily reveal information "about one's lifestyle, intimate relations or political or religious opinions." Elements of our identity as individuals which were recognized in common law as fundamental to privacy over two hundred years before the advent of the Internet.[108]

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).)

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**&2 p=&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.)

[107] Adapted from Pascual, *supra* note 83.
[108] Millar *v.* Taylor (1769), 4 Burr. 2303, 2379 98 E.R. 201 at 2379 and 242 .

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 of the aforementioned definitions of "traffic data", despite the fact that they are contextually very different. As was previously discussed, the *Plant* doctrine requires an analysis of what the data in a given category actually represents. 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; a point the Explanatory Report acknowledged, in part:

> [T]he privacy interest is generally considered to be less with respect to the collection of traffic data than interception of content data. Traffic data about time, duration and size of communication reveals little personal information about a person or his or her thoughts. However, a stronger privacy issue may exist in regard to data about the source or destination of a communication (*e.g.,* the visited websites). The collection of this data may, in some situations, permit the compilation of a profile of a person's interests, associates and social context. Accordingly, Parties should bear such considerations in mind.[109]

So too did the Canadian Association of Chiefs of Police:

> Search warrants [and not production orders under a lower standard] should be required in relation to information that tends to reveal intimate details of the lifestyle and personal choices of any individual affected by the order (see *R. v. Plant* [1993] 3 S.C.R. 281).[110]

In *Doubleclick*,[111] the court discussed how traffic and content information could be one and the same thing. In *Pharmatrak*, the U.S. 1st Circuit Court of Appeals unequivocally found

[109] EXPLANATORY REPORT, *supra* note 20, ¶ 227.
[110] CACP, *supra* note 7, at 17.
[111] *In re Doubleclick*, *supra* note 102, at 514 ("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 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.").

that data of the kind captured by the "GET" method in *Figure 3* was content[112] under the definition of the federal wiretap statute.[113]

3. A lower threshold for authorization of electronic surveillance fails to recognize new capacities to draw public inferences about private activities.

The *Lawful Access* initiative, like the Convention, was predicated on the challenges posed by "the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks".[114] The stated public policy objective of the initiative was to "maintain lawful access capabilities for law enforcement and national security agencies… and to preserve and protect the privacy and other rights and freedoms".[115] From the Canadian government's perspective, the purpose of ratifying the Convention then, is to maintain the *status quo* of government surveillance capability, not to increase it.

In 2000, in his last report to Parliament, of a tenure which spanned the widespread adoption of the Internet, Bruce Phillips, former Privacy Commissioner of Canada, warned that legal privacy protections had not maintained pace with the propensity of technology for surveillance:

> It's now a cliché that the last ten years have brought forth an information management revolution, thanks to ever more mind-boggling advances in computer and communications technology. It's even more true that the law still lags far behind in its duty to ensure this technology is harnessed to the cause of human liberation and not to its subjugation.[116]

Both these positions invoke technology as the circumstance from which to launch claims for legal change. While seemingly antagonistic, they are, in fact, aimed at the same problem, namely that of harnessing technology in the public interest; it is in the definition of 'public interest' that the two communities differ. The weakness in the government's perspective, as Marc Rotenberg deftly illustrated, is that to view this as a balancing problem between privacy and security, between liberty and public safety fundamentally misunderstands both the nature of democratic society and the nature of technology, because it ignores the lack of oversight and accountability in technological solutions.

---

[112] *Pharmatrak, supra* note 99, 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").

[113] 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.").

[114] Convention on Cybercrime, *supra* note 22, preamble; LAWFUL ACCESS, *supra* note 1, at 3.

[115] LAWFUL ACCESS, *supra* note 1, at 6.

[116] B. PHILLIPS, PRIVACY COMMISSIONER OF CANADA, ANNUAL REPORT 1999-2000 (2000).

> When we allocate to government any type of authority in a democratic society, we create mechanisms of public oversight and accountability: we do this through the legislative process, we do this through open records laws, we do this to ensure that the people and their elected representatives are fully informed about the nature of decision making by the government. You cannot transfer authority from the people to the government without changing the nature of that society…. In the world of technology there is no similar swing in the pendulum. There are pathways and there are tangents and these arcs in technological development create infrastructures of control, determine opportunity, choice and the degree of freedom.[117]

Thus, the laws that permit electronic surveillance typically incorporate the authority to intercept and the means of oversight, but rarely does surveillance technology contain more than the first aspect.[118] The result is that there is no guarantee that the authority will be used in a lawful manner. Further, as has already been argued in this paper, a misunderstanding of technological nuances can translate lawful uses of surveillance technology into immoral if not unconstitutional ones. Brandeis J., in his famous dissent in *Olmstead* warned against such apprehensions in 1928:

> Time works changes, bring[ing] into existence new conditions and purposes. Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.[119]

In *R. v. Wong*, the Supreme Court cautioned that it would be wrong to limit the requirement for prior judicial authorization for electronic surveillance to any particular technology.

> Rather it must be held to embrace all existing means by which the agencies of the state can electronically intrude on the privacy of the individual, and any means which technology places at the disposal of law enforcement authorities in the future.[120]

In *Kyllo v. United States*, involving a search of the outside of a house using infrared monitoring equipment, the U.S. Supreme Court ruled that where the government uses a device that is not in general public use, to explore the details of a private home that would previously have been unknowable without physical intrusion, the surveillance is a "search" and is presumptively unreasonable without a warrant.[121] The Ontario Court of Appeal adopted *Kyllo* in

---

[117] Marc Rotenberg, A New Calculus of Freedom: Balancing Personal Liberties and Public Safety in an Age of Technologically Sophisticated Terrorism (Forced to be Free: Technology, Freedom and Control in a Digital Age, Faculty of Law, Harvard University, 20 Apr. 2002), *available at* http://jolt.law.harvard.edu (last visited 27 May 2002).

[118] *See* McCullagh *supra* note 19.

[119] Olmstead *v.* United States, 277 U.S. 438, 473 (1928).

[120] R. *v.* Wong, [1990] 3 S.C.R. 36, 43 (warrantless video surveillance of hotel room constitutes unreasonable search and seizure).

[121] (2001), 121 S. Ct. 2038 at ¶ 25 (where the "government uses a device that is not in general public use, to explore the details of a private home that would previously have been unknowable without physical intrusion, the surveillance is a Fourth Amendment 'search' and is presumptively unreasonable without a warrant").

R. v. Tessling, concluding that the state should be required to obtain a warrant before using technology that has the capacity for generating public inferences about private activities:

> The [surveillance] . . . reveals what cannot otherwise be seen and detects activities inside the home that would be undetectable without the aid of sophisticated technology . . . . [B]efore the state is permitted to use technology that has the capacity for generating information which permits public inferences to be drawn about private activities . . . it should be required to obtain judicial authorization to ensure that the intrusion is warranted.[122]

The Supreme Court disagreed with the lower court that infrared monitoring technology in question had the capacity to generate public inferences about private activities. In finding that "technology must be evaluated according to its current capability, and its evolution in future dealt with step by step" the Court left intact the principle that if the technology had been either intrusive or capable of generating public inferences about private activities, it could – and would likely – be considered a 'search' subject to § 8 of the Charter.[123]

Also consider that because of the nature of packet-mode communications (discussed in more detail below), network traffic data intercepted at some random 'hop' between the sender and the intended recipient may not attract any greater expectation of privacy than that now accorded to telephone traffic data or to the information on the outside of an envelope, but if the point of interception revealed patterns of information and communication, this would invariably attract greater legal protection to the extent it revealed intimate details of the lifestyle and the personal choices of the subject. Electronic surveillance by law enforcement or intelligence agencies would very likely fall within this latter category.

Both the Explanatory Report to the Convention and the *Lawful Access* document suggested 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.[124] However, this ignores 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 1980'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.[125] By the early 1980s, the private sector overtook the state as the primary threat to privacy, replacing Orwell's dystopic vision of one Big Brother with a new one filled with many little ones.[126]

The courts have found in *Del Zotto v. Canada (Minister of National Revenue)*[127] that a reasonable expectation of privacy is not founded on the location of the information in which the expectation is held. In that case, records that "could reveal incredibly intimate and personal

[122] [2003] O.J. No. 186 (C.A.) at ¶¶ 68-69.
[123] *Tessling*, *supra* note 36.
[124] EXPLANATORY REPORT, *supra* note 20, at ¶ 171; LAWFUL ACCESS, *supra*, note 1, at 11.
[125] Christopher Berzins, *Protecting Personal Information in Canada's Private Sector: The Price of Consensus Building*, 27 QUEEN'S L.J. 609, 616 (2002).
[126] DANIEL J. SOLOVE, THE DIGITAL PERSON 27-47 (2004) (suggesting Kafka as a better metaphor than Orwell).
[127] (1997) 147 D.L.R. (4th) 457 (SCC).

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. Characterizing it as "a window into most of a person's private life", the documents contemplated by the Court included reading materials, relationships with churches, charities or political parties, personal tastes, relationships with other people and documents relating to the appellant's financial affairs. Information of this nature could clearly be the target of any production order for a telecommunication or an Internet service provider's subscriber's records. For example, the traffic data from *Figure 2*, above, reveals that the two callers went from the Montréal airport to the Hilton Hotel at 1 o'clock in the morning. From this, we can easily infer information wholly unrelated to the routing of the message. The traffic data in *Figure 3*, above, is even more revealing of the kind of information contemplated in *Del Zotto* and yet caught by most definitions of "traffic data" found in the aforementioned international cybercrime instruments, including the proposal in the *Lawful Access* document.

B. Disclosure of personal information to third parties should not circumscribe general expectations of privacy

Even the least participation in society requires that we engage in frequent information transactions with third parties. Usually, we exchange personal information for some benefit, such as access to medical care, warranty coverage or membership to a website. This is not personal information as a pure commodity – although increasingly there are those types of transactions too – but an exchange of personal information as a way of authenticating an individual's eligibility to receive something. In such cases, simply because we have disclosed our personal information should not mean that we give up all expectations of privacy we may have in it. We have voluntarily disclosed it to a known party, for a specified purpose, or alternately we have disclosed personal information unknowingly or have been compelled to do so, but in any case the personal information remains part of our identity and belongs to us. The Supreme Court first adopted this principle of 'information self-determination' in *R. v. Dyment*:

> This notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit. In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected. Governments at all levels have in recent years recognized this and have devised rules and regulations to restrict the uses of information collected by them to those for which it was obtained; see, for example, the *Privacy Act*, S.C. 1980-81-82-83, c. 111.[128]

The principle of information self-determination is properly deconstructed as a set of so-called 'fair information principles' which govern the manner in which personal information should be collected, used, stored and disclosed, and the rights that affected individuals should have to view, contest and correct such information; they form the basis for most privacy and data

[128] *Dyment*, *supra* note 49, at 429-430 (citations omitted).

protection statutes worthy of the name, including the recently enacted federal Personal Information Protection and Electronic Documents Act.[129]

To approach the argument from another direction, if our reasonable expectations of privacy were circumscribed by the limits of only what we could keep inside our heads, we might as well take up residence in a prison or a fishbowl. In 1963, Justice Brenner of the U.S. Supreme Court in *Lopez v. United States* remarked:

> The assumption, manifestly untenable, is that the Fourth Amendment is only designed to protect secrecy. If a person commits his secret thoughts to paper, that is no license for the police to seize the paper; if a person communicates his secret thoughts verbally to another, that is no license for the police to record the words…. The right of privacy would mean little if it were limited to a person's solitary thoughts and so fostered secretiveness.[130]

1. Individual subscribers have a reasonable expectation of privacy in traffic data by virtue of the subscriber-provider relationship.

To some degree, Canadian and American jurisprudence diverges on this point. 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.[131] In *United States v. Hambrick*,[132] the court found that in knowingly disclosing non-content information to a third party, Hambrick 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.[133] 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.[134]

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

[129] 2002, S.C. 2002, ch. 5, Sch. 1 (referencing the ten fair information principles found in the Canadian Standards Association's MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION).
[130] Lopez *v.* United States, 373 U.S. 427, 449-450 (1963).
[131] *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").
[132] 2000 U.S. App. LEXIS 18665 (4th Cir., 2000).
[133] *Id*. at 11-12 (citing interpretation in *Smith*, *supra* note 131, 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).
[134] 255 F.3d 325, 335-336 (6th Cir., 2001).

freedom and dignity of the individual."[135] Thus, the court in *Plant* arrived at the same result as did the courts in *Hambrick* and *Guest.*

> The nature of the relationship between the appellant and the Commission cannot be characterized as a relationship of confidence. The Commission prepared the [billing] records as part of an ongoing commercial relationship and there is no evidence that it was contractually bound to keep them confidential.[136]

However, the *Plant* court arrived there by a very different road.

> This is not to suggest that records prepared in a commercial context can never be subject to the privacy protection afforded by § 8 of the Charter. If commercial records contain material which meets the "personal and confidential" standard set out above, the commercial nature of the relationship between the parties will not necessarily foreclose a § 8 claim.[137]

Of the two components of this approach, the second question as to whether the commercial records contain material which meets the "personal and confidential" standard has already been discussed. The conclusion we cannot fail to reach is that digital traffic data can, in many cases, meet this test.

Next, we turn to the first question, as to the nature of the relationship between the parties. In *Plant* the Court of Appeal found that the records were "created in the context of a commercial transaction… for the purposes of billing rather than for customer use".[138] This was affirmed on appeal to the Supreme Court which, moreover, concluded that not only were the records routinely released to the police, but that they were also available to the public-at-large. In other words, there was no contractual obligation to keep the impugned records confidential nor was there a reasonable expectation that they would be.

Contrast this situation with the one in which most subscribers find themselves *vis à vis* their service providers, as described by University of Ottawa law professor Ian Kerr in his article *The Legal Relationship Between Online Service Providers and Users*. Professor Kerr finds that although the relationships we may establish with service providers can span the spectrum from the strange and whimsical to the gateway to paid services, they are almost always contractual.

> Whether in exchange for remuneration, information, graft or graffiti, the vast majority of online service providers do not merely create a public thoroughfare for virtual voyeurs. Rather, they attempt to establish some sort of relationship with those who show interest in their services. Reduced to their most basic form, almost all of these subscriber-provider relationships can be understood as contractual in nature. Something of value is offered by one person to another in exchange for an online service.[139]

Further, Kerr surveyed more than 40 provider terms of service agreements to conclude that "[m]any… promise that the service provider will take steps to ensure the confidentiality of a user's communications and will only release personal information in circumstances where the

---

[135] Schreiber *v.* Canada (Attorney General), [1998] 1 S.C.R. 841, 854.
[136] *Plant*, *supra* note 46, at 294.
[137] *Id.*
[138] *Id.* at 294, *aff'g* 116 A.R. 1 at 6-7 (C.A.).
[139] Kerr, *supra* note 62, at 429-430.

provider is legally compelled to disclose."[140] Unlike the situation in *Plant* and distinguished from facts in *Hambrick* and *Guest*, the information disclosed to or through the service provider is neither public nor void of a reasonable expectation of privacy.

Kerr's article concludes that, in some cases, providers are not only guardians of their subscribers' information privacy on the Internet, but may owe fiduciary responsibility to the subscriber, as in relationships where the subscriber is peculiarly vulnerable to discretion exercised by the provider.[141]

2. The behaviour of individuals online suggests they hold an expectation of privacy which while perhaps misplaced could nonetheless be reasonable.

As stated previously, opinion polls consistently show that North Americans are concerned about their privacy in cyberspace, but because most possess a poor appreciation of what actually takes place behind the screen, these concerns remain ill-defined and their actions unmitigated. Put another way, even though individuals may have generalized privacy concerns in cyberspace, they do not act to sufficiently protect ourselves because they have made false assumptions about the capabilities and the extent of surveillance they may be exposed to when engaging in online transactions. Alternatively, individuals cannot fail to be aware that some entities, most obviously their access provider, stand in a unique position to observe their online activities, but they rely on the contractual or else fiduciary relationship to protect such disclosures.

> [Access providers] are in a unique position to gather and store information pertaining to individual users. [They] are the gatekeepers, standing between individual users and the [Internet]. Access providers send and receive information to and from users and route it through to [the larger Internet]. Billing and other necessary information needed to carry on the service provider-user relationship can obtain and record accurate information detailing the exact location of particular users at a particular time, and can compile lists of all their points of destination while online. In some cases, this allows access providers to learn the habits and preferences of their users. By linking the real life identity of the user to her online activities, the access provider can build a highly personal profile of the user.[142]

Thus it would seem that as much as our own ignorance about what actually takes place behind the screen encourages us to make false assumptions about our online privacy, so too does the trust we place in our service providers. Every day, across cyberspace, people engage in very private behaviour on the public Internet. They engage in virtual sex, submit income tax returns, research health ailments, pay bills, collaborate with co-workers, make purchases, plan vacations,

---

[140] *Id* at 434.

[141] *Id* at 443, 451; *see also* Frame *v.* Smith, [1987] 2 S.C.R. 99, ¶ 60; Office of the Privacy Commissioner of Canada, Commissioner's Findings, Internet Service Provider Accused of Withholding E-Mails Sent to Suspended Account (28 Aug. 2002), *available at* http://www.privcom.gc.ca/cf-dc/cf-dc_020828_e.asp (last visited 27 Feb. 2003) (appeal as of right to the F.C.T.D. – applicant arguing that ISP breached fiduciary duty to not withhold email in absence of contractual terms to the contrary).

[142] Kerr, *supra* note 62, at 423.

enter contests and so forth. Much of this activity is done in the clear and all of this information is submitted, one way or the other, through providers. Does the mere fact that individuals engage in these kinds of activities mean that they no longer hold reasonable expectations of privacy in the information disclosed to third parties? Does it imply some kind of trust relationship between subscriber and the recipient of the information? Does it suggest a certain level of ignorance on the part of the subscriber as to exactly what happens when they click "Send"? The only other explanation is that individuals just do not care that they are exposing intimate details of lifestyle and personal choice. This conclusion is not supported historically, either by polls or by established expectations of privacy in those same activities offline.

The Supreme Court has addressed the question of behaviour as a factor in the contextual determination of a reasonable expectation of privacy. In *R. v. Shearing* the Court found the contents of a diary of secondary importance as to whether the owner had a reasonable expectation of privacy in the contents:

> It was a diary. Diaries are supposed to be private. [T]he fact that [the owner] specifically chose to record her thoughts and recollection of daily events in a private, locked diary, rather than, for instance, on a calendar on her bulletin board, post-it notes on the refrigerator, or even her school notebook, suggests to me that she had a high expectation of privacy in what she wrote, *regardless of its content*…. The fact that the diary contained "mundane" sorts of information is not, in my view, fatal to her wish to keep private the entries she did choose to record in her private diary."[143]

Similarly, in *R. v. Law*,[144] the Supreme Court did not examine the contents of the private documents to evaluate the owner's privacy interest. In that case, thieves stole a safe containing commercial documents from two restaurant owners. The police recovered the safe, but before it was returned to the owners, an officer who suspected the owners of tax violations photocopied some of the documents inside and forwarded them to Revenue Canada. Bastarache J., writing for the Court, concluded that the owners' reasonable expectation of privacy in their documents derived not from their contents, but from the fact that they chose to keep the documents confidential by locking them in a safe. In its reasoning, the Court adopted the principle in *Dyment* that information privacy derives from the assumption that all information about a person is in a fundamental way his or her own, for him or her to communicate or retain as he or she sees fit.[145]

The obvious rule in these two cases is that if an individual takes steps – perhaps by registering under a pseudonym or by using some form of encryption[146] or anonymization software – to protect their information that passes to or through a service provider, this could

[143] R. *v.* Shearing, [2002] S.C.C. 58 at ¶¶ 112 and 167 (emphasis added).
[144] 2002 S.C.C. 10.
[145] *Id.* ¶ 6.
[146] *But see Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication*, 110 HARV. L. REV. 1591, 1604-07 (1997) (arguing that encryption is insufficient to establish a reasonable expectation of privacy because contrary to the use of a password, encryption merely obscures the meaning of a message and does not prevent someone from viewing it).

trigger § 8 protection.[147] Could the same rule apply in cases where an individual maintains an expectation of privacy in information, but takes no action to mitigate exposure to a third party because they are ignorant of the potential for surveillance? This would be inequitable to say the least. Although ignorance of the *law* is not a defence in law, ignorance of technology might be.

What if the individual is aware of the disclosure, but instead of relying on a technological or administrative-type mitigation, relies instead upon legal ones such as contractual terms in the service agreement, principles of equity or on public policy articulated in self-regulatory instruments or legislation?

C. Interception of a packet-switched communication is liable to massively infringe third-party Charter rights

1. Digital networks work differently than analog networks.

In traditional or analog telecommunications, a telephone switch establishes a "circuit" between the caller and recipient, and that channel remains open during a call to carry information back and forth. By contrast, in digital or "packet switched" communication, information – voice or data – is broken down into small pieces of data called "packets." Each packet is like an envelope, containing both message content and a header that indicates the point from which the packet originates and the point to which it is being sent. The header of a packet is analogous to a dialed number on a traditional telephone system; the message content is identical to the content of a telephone conversation. Each packet, containing a portion of the message, is transmitted individually and when all the packets reach their destination, they are reassembled into the complete message.[148]

Packet-mode communication is the transmission technology of the Internet. It is also increasingly important for the transmission of voice and data in telecommunications.

2. Investigatory tools for packet-mode communications cannot precisely separate traffic and content data, necessitating a reasonable expectation of privacy for both.

[147] American jurisprudence recognizes a similar principle. In *Robbins v. California*, 453 U.S. 420, 426-427 (1981) the Supreme Court found that by placing information within "a closed, opaque container," an individual manifests an objectively reasonable expectation of privacy in that information. However, the court also found that there can be no Fourth Amendment protection if the container is not closed, if it is transparent, or if its contents can be inferred from its outward appearance.

[148] *Communications Assistance for Law Enforcement Act* (Third Report and Order) (1999), CC Docket No. 97-213, FCC 99-230 (F.C.C.) at ¶ 55. The above analogy is quite different from those which draw comparisons between traffic data and the information contained on the outside of an envelope *viz. supra* note 106. The header of an individual packet consists only of routing data and prior to reassembly, the individual packets reveal almost nothing of the content of the message *in toto*.

Packet-mode investigative tools suffer from overbroad application. Indeed, this is true of any automated classification system, including web search engines and filtering software.[149] As has already been discussed, divorcing traffic data from the content of the message is very difficult to do in the legal context. It is also difficult to do from a technical perspective.

Automated classification systems are predicated on the ability to 'see' the target content and treat it according to pre-determined technical parameters. However, the underlying architecture of most digital networks precludes effective operation of this model. As Tim Berners-Lee, the inventor of the World-Wide Web, explains:

> There's a freedom about the Internet: as long as we accept the rules of sending packets around, we can send packets containing anything to anywhere…" The architecture of the network is designed to be "neutral with respect to applications and content. By placing intelligence in the ends, the network has no intelligence to tell which functions or content are permitted or not."[150]

By requiring that the network itself remain neutral and open, with intelligence built into applications using the network, the underlying architecture has enabled extraordinary innovation, but has also made it extremely difficult to regulate content or even find and isolate it.[151] The U.S. Ninth Circuit Court of Appeals recently described this architecture as "end-to-end."[152] End-to-end disables central control over how the network develops and, as Industry Canada recently concluded, effectively precludes content-based determinations.[153]

A recently disclosed internal FBI memo on the operation of Carnivore, a packet-mode, automated interception system, indicated that filter inaccuracy is not a hypothetical problem.

> The FBI software not only picked up the E-mails under the surveillance of the FBI's target… but also picked up E-mails on non-covered targets. The FBI technical person was apparently so upset that he destroyed all the E-mail take, including the take [on the target].[154]

---

[149] *See, e.g.*,, American Library Ass'n, Inc. et al. *v.* United States, et al., 201 F. Supp. 2d 401, 448 (E.D. Pa. 2002) ("automated review processes, even those based on 'artificial intelligence,' are unable with any consistency to accurately distinguish material that falls within a category definition from material that does not").

[150] LESSIG, *supra* note 12, at 40 (emphasis added) (citations omitted).

[151] GERRY MILLER ET AL., INDUSTRY CANADA, REGULATION OF THE INTERNET: A TECHNOLOGICAL PERSPECTIVE 3 (1999) *available at* http://strategis.ic.gc.ca/epic/internet/insmt-gst.nsf/vwapj/005082_e.pdf/$FILE/005082_e.pdf (last visited 3 Jan. 2005); *see also* YOUNG, *supra* note 13.

[152] AT&T *v.* City of Portland, 216 F.3d 871, 879 (9th Cir. 2000) ("The Internet's protocols themselves manifest a related principle called "end-to-end": control lies at the ends of the network where the users are, leaving a simple network that is neutral with respect to the data it transmits, like any common carrier."). The phrase comes from the work of network architects J. Saltzer, et al., *End to End Arguments in System Design*, 2 ACM TRANSACTIONS IN COMPUTER SYSTEMS 277-288 (4 Nov. 1984).

[153] MILLER, *supra* note 151, at 3.

[154] FBI memo on errors in Foreign Intelligence Service Act intercepts using the FBI Internet monitoring system, Carnivore, at http://www.epic.org/privacy/carnivore/fisa.html.

The author of the memo states that "[t]he software was turned on and did not work correctly." In fact, it *was* working correctly, but packet-mode automated classification systems suffer from poor precision[155] and are liable to massive invasions of privacy of innocent third party subscribers, not because of the nature of the tool or technique so much as the environment in which they will be employed.[156] Notwithstanding technological development of new investigatory tools, surveillance by these means will always be liable to inaccuracy in targeting and collecting only that information which may be relevant to a given person. This can best be explained by way of illustration.

An Illustration of the (In)Accuracy of a Packet-Mode Filter

Let us assume that one person out of a 100,000 is a terrorist and communicating evidence of such over the network. Law enforcement installs a filter at a service provider that is designed to trap all packets that may be of interest to an anti-terrorism investigation. The filter or "packet-sniffer", as it is commonly-known, traps only packets described by specific, target parameters and is 99.999% accurate in its task – if a packet contains evidence of terrorism, the filter has a 99.999% chance of identifying it and an 0.001% chance of erring and identifying the packet as innocent. Similarly, if a packet is innocent, the filter has a 99.999% chance of saying so, and an 0.001% chance of incorrectly flagging it as evidence of terrorism. For the sake of simplicity, we will also assume that each subscriber only sends or receives one packet per day (in reality, the average Internet subscriber probably sends or receives approximately one million packets per day, but this would make the calculations unwieldy for our purposes).

If one packet in 100,000 actually does contain evidence of terrorism, what happens? The filter will almost certainly catch that one packet. It will also tag 0.001% of innocent packets – which also works out to almost exactly one per 100,000. Of the packets tagged by the filter, half are innocent. Since packets equal people in our illustration, the filter will finger one innocent person for every terrorist. An accuracy rate of 50%.

To be precise with the numbers:

Figure 4: Filter with 99.999% Precision

1 in 100,000 guilty packet/person = 0.00001 per 1 input
99,999 innocent packet/people = 0.99999 per 1 input
Flag 99.999% of guilty packets/people » catch (correctly) 0.000099999 per 1 input
Flag 0.001% of innocent packets/people » false positives 0.000099999 per 1 input
They are equal, so it is trivial that the result is 50/50.

For a slightly less accurate (but more realistic) filter:

Figure 5: Filter with 99.99% Precision

1 in 100,000 is a guilty packet/person = 0.00001 per 1 input

[155] To simplify the explanation, I will use "precision" to refer to both precision and recall inaccuracies, *see American Library Association*, *supra* note 149.

[156] VATIS, *supra* note 10, at 33 (31% of investigators identified the inability to selectively monitor traffic as a problem they encountered at least often, compared to only 22% who said they had never encountered this problem).

99,999 are innocent packets/people = 0.99999 per 1 input
Flag 99.99% of » catch (correctly) 0.00009999 per 1 input
Flag 0.01% of innocent » false positives 0.00099999 per 1 input
Total flagged » 0.00009999+0.00099999 = 0.00109998 per 1 input

How much of flagged traffic is innocent?

0.00099999 ÷ 0.00109998 = 0.9090983472 = ~ 91%

How would we feel about a system in which almost all guilty persons were charged, but where between 50-91% of those charged were innocent? In 2001, Bell Canada had in excess of 1.5 million Internet subscribers and 4.4 million wireless subscribers.[157] Using *Figure 5* above, 150 innocent Bell Canada Internet subscribers and 440 wireless subscribers would have been incorrectly labeled as terrorists in 2001.

3. Infringement of third party privacy is contrary to the spirit of § 8; massive infringements can be determinative of constitutionality.

An automated classification system's lack of precision has legal implications. In *R. v. Thompson*, the Supreme Court considered whether the extent of an invasion of a third party's rights could be determinative of constitutionality for the second stage of a § 8 analysis, namely the unreasonableness of the search.

> "[A] potentially massive invasion of . . . privacy" of members of the general public who were not involved in the suspected criminal activity . . . cannot be ignored simply because it is not brought to the attention of the court by one of those persons. Since those persons are unlikely to know of the invasion of their privacy, such invasions would escape scrutiny, and § 8 would not fulfill its purpose.[158]

While massive invasions of third-party privacy rights may sometimes be "justified in appropriate circumstances" as Sopinka J. observed in *Thompson*, it would seem that if a technology was liable to massively infringe these rights that its use by law enforcement would attract the very highest *ex ante* scrutiny and not the reverse, as proposed by the *Lawful Access* document. Section 8 would have very little value as a guarantee to the right to privacy if it operated only to exclude, *ex post facto*, information obtained in an unreasonable manner; by that time, the individual's privacy would have already been violated and the personal information would be in the hands of the authorities.[159] This prophylactic interpretation of § 8 has found effective expression in the judicial preauthorization requirement developed by Dickson J. in *Hunter*:

> [The] purpose [of § 8 is] to protect individuals from unjustified state intrusions upon their privacy. That purpose requires a means of *preventing* unjustified searches before they happen, not simply of determining, after the fact, whether they ought to have occurred in

[157] BELL CANADA FINANCIAL INFORMATION 2004, ANNUAL REPORT (April 16, 2002) at 8 ("Customer Connections").
[158] *Thomson*, *supra* note 41, at 1143.
[159] *Schreiber*, *supra* note 135, at 866.

> the first place. This, in my view, can only be accomplished by a system of *prior authorization*, not one of subsequent validation.[160]

More recently, La Forest J., for the majority in *Duarte*, opined on the importance of *ex ante* scrutiny:

> [I]f the surreptitious recording of private communications is a search and seizure within the meaning of § 8 of the Charter, it is because the law recognizes that a person's privacy is intruded on in an unreasonable manner whenever the state, without a prior showing of reasonable cause before a neutral judicial officer, arrogates to itself the right surreptitiously to record communications that the originator expects will not be intercepted by anyone other than the person intended by its originator to receive them….[161]

D. The complexity of technological systems increases the risk of unintended consequences

It is tempting to think of technology as merely a tool which can be applied to or removed from a given process to produce an intended result. Technology *is* a tool, but it is an unpredictable one, infused with characteristics that we cannot fully understand without the benefit of hindsight. Therefore, technology is not merely a tool, but also a value construct. It is an abstract collection of values and propensities towards particular values – called valences – which have both internal and external origins.

The nature of the value construct is often not obvious in the way that the physical properties of a tool itself might be. It is obvious that a television is designed to be watched, but it is not obvious that the television is not conducive to social interaction and is, in fact, valenced towards isolation: this is a facet of the value construct we have come to understand through our use of the technology.[162]

1. Complexity increases the risk of opacity

Our ability to penetrate, describe and comprehend the nature of a value construct diminishes with its complexity. Complexity is more than a function of being complicated, as even relatively simple systems can represent complex value structures. Instead of describing mere sophistication, complexity specifically refers to the unintended consequences associated with our ignorance of those values or valences which attach to systems of law and of technology. It is our inability to describe the value construct which requires cognizance of the relationship between law and technology and caution in our adoption of new technologies to solve social or legal problems.

---

[160] *Hunter*, *supra* note 37, at 160; for a discussion of the exclusionary rule under the 4th Amendment, *see* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002).

[161] *Duarte*, *supra* note 35, ¶ 28 (emphasis added).

[162] HOWARD RHEINGOLD, SMART MOBS: THE NEXT SOCIAL REVOLUTION 58 (2002).

In complex systems inputs do not sum to give predictable outputs.[163] This confuses our attempts to understand how systemic variables might evolve in response to changes we make to any other given internal variable, or how they might interact with external norms or laws. Instead, minor adaptations can create exponential complexities over time and even intuitive solutions to discrete problems will lead would-be tinkerers into uncharted territories.[164] For example, antibiotics kill bacteria, more antibiotics kill more bacteria, but at some point the use of antibiotics leads to resistant and much more dangerous bacteria.[165] This is not an intuitive result, but is indicative of a common complex problem.

Like technology, law can also be a complex system. Tax amnesties encourage people who otherwise would not pay taxes to do so. However, amnesties also signal that the government may be periodically willing to overlook malfeasance. Ergo, amnesties will encourage short-term compliance of a small segment of the population at the expense of long term compliance of a potentially larger subset.[166] Moreover, amnesties weaken the signaling effect of compliance among groups for which that may be important. Thus, even if amnesties encourage those who typically don't comply to do so in the short-term, it will also encourage those segments who typically comply *not* to do so in the short *and* long term. The sum result of amnesties can be a net reduction in tax compliance in both the short and long term. Again, this is not an intuitive result.

Legal or social systems founded upon a substrate of fluid technology will exhibit an even greater degree of complexity than those that are not. In such instances, changes made to any of the technological, normative or legal environments will cascade through interdependent relationships in unpredictable ways.

2. The myth of 'technoneutrality' promotes the adoption of undesirable value constructs

---

[163] *See, e.g.*,, John Holland, *What Is To Come And How To Predict It*, in JOHN BROCKMAN, ED., THE NEXT FIFTY YEARS: SCIENCE IN THE FIRST HALF OF THE TWENTY-FIRST CENTURY (2002); Jennifer Light, *New Technologies and Regulation: Why the Future Needs Historians*, 2001 L. REV. M.S.U.-D.C.L. 241, 242.

[164] *See, e.g.*,, Rajen Akalu & Deepa Kundur, *DRM and the Courts: Lessons Learned from the Failure of CSS*, IEEE SIGNAL PROCESSING MAGAZINE SPECIAL ISSUE ON DIGITAL RIGHTS: MANAGEMENT, PROTECTION, STANDARDIZATION 21:2 (March 2004) 119, discussing the unintended consequences of ineffective copyright protection schemes combined with ill-considered legislation; *see also* Ken Roach, *Globe and Mail* (11 Sept. 2003) (arguing that "memorial" legislation, such as the anti-terrorism statute rammed through Parliament in the months after 9/11, fails to intelligently address the problems for which it was promulgated and, in fact, may exacerbate the threat by lulling us into a false sense of security).

[165] Bill Joy, *Why the future doesn't need us*, WIRED.COM 8.04 (April 2000) *available at* http://www.wired.com/wired/archive/8.04/joy_pr.html.

[166] *See* Eric Posner, *Law and Social Norms: The Case of Tax Compliance*, 86 VA. L. REV. 1781, 1793 (2001).

Technological neutrality is a concept which has gained some currency in legal circles.[167] The phrase describes a state in which technology has no embedded value, no bias and a minor role to play in our understanding of how to regulate it: technology is just a tool.[168] Fundamentally, technoneutrality denies the symbiotic relationship between technology, law and social norms.[169]

Technoneutrality posits that we can discern value from technology only from the ways in which people *use* it and the ways in which they *understand* how it should be used, and not independently from the tools themselves.[170] Most conceptions of technoneutrality do not claim that technological artifacts are without value, but instead that they reflect only contextual values, that is, only the values represented in the surrounding environment. This is an attractive thought, because it leads us down that path of thinking that we can predict and manage the consequences of present and future technologies if we are careful and clever enough. It is particularly attractive to policymakers who hope to counter the effects, through law, of disruptive technologies.

Social norms are natively transparent. We are inculcated with norms from birth. Most of us know that it is wrong to steal because that is how we were raised. A pedophile knows that pedophilia is abnormal, even though they are personally predisposed to it, because they live in a society in which the value of pedophilia is discounted. Social norms are the language we speak with one another. It would be difficult to navigate around our world without an understanding of them. How would we know to pay for bubblegum we found in a store and not eat the bubblegum we find on the street? How would we know it is rude to stick our tongues out at strangers or to gossip about the misfortunes of others? Law too is transparent, for the most part, because it is written in the language of social norms. The transparency of the values expressed in social norms or in law often delude us into thinking that because we understand them, we can manipulate them with abandon. Technoneutrality is an extension of this hubris.

In order for technological values to be manipulable, we would need to be able to predict them within a finite range: we would need to be able to define the value construct. There are four reasons why this is practically impossible without historical perspective. First, unlike social norms or law, most of us are not native 'speakers' of the values inherent in technology. Even designers of new technologies rarely know how their inventions will be ultimately used or perceived in all contexts. Second, even if we could know the values of present technologies, we could never predict future developmental directions. Third, to the extent that values fit within a constellation of other values – either internal to the system itself or contextually – the sums of these value propositions would be non-additive. Predictions would be flawed for simplicity, even monolithicity. Finally, even if we could know all the values, for all the reasons just stated it would be impossible to manipulate them with precision.

---

[167] *See, e.g.,*, SUNNY HANDA, COPYRIGHT LAW IN CANADA 440-41 (2002).

[168] *See* PRISCILLA REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 10-15 (1995) (contrasting determinism and neutrality with realism, in which law and science have a dynamic relationship, each one shaping the direction of the other); *see also* DAN BURK, CYBERLAW AND THE NORMS OF SCIENCE (unpublished).

[169] NEIL POSTMAN, TECHNOPOLY: THE SURRENDER OF CULTURE TO TECHNOLOGY 142 (1993).

[170] I use the terms 'artifact', 'system' and 'tool', 'architecture' and 'technostrata' interchangeably to refer to technological structures or technology, broadly speaking.

There is another approach to understanding technology which should be mentioned here. It is interpretively quite different from the notion of technoneutrality and yet it has a functionally similar effect when considered in the context of policymaking. This approach is known as 'technological determinism' and it posits, first and foremost, that the relationship between technology, law and society is one way, but in the *opposite* direction in which we understand the relationship in the technoneutrality context. Determinism posits that technology is, by degrees, autonomous, independent, self-controlling, self-determining, self-generating, self-propelling, and self-perpetuating.[171]

The critiques of determinism are interesting for how they help us understand the limitations of the neutrality argument. Accordingly, human choice drives technology development, not the other way around. Technology is shaped by society and is subject to human control.[172] Artifacts usually reflect the plans, purposes and ambitions of some individual, some institution, or some class. Not surprisingly, it will embody the values implicit in those purposes. Of course, plan, purposes and ambitions can and do change and intentions are rarely ever perfectly realized.[173]

While neutrality and determinism differ interpretively, both adopt the idea that technology is divorced from or subordinate to other regulatory factors, such as law or the market. They both share an ignorance of the intentions, values and social understanding of those who design, develop, market and control technology and of the conscious or subconscious understanding of users, consumers, beneficiaries, victims, and others. Consequently, both neutrality and determinism – though scribed by different labels – adopt one-dimensional views of the relationship between technology, law and social norms. These views encourage policymakers to incorrectly abstract technology from the context of use and perception, by focusing on outcomes instead of means.[174]

Few would dispute that bias may arise from use, and so the first, easiest argument to make to those who are reluctant to ascribe values to artifacts, is to argue that some technologies are valenced towards *particular* uses. Guns are valenced towards violence; the presence of a gun in a given situation raises the potentiality of violence by its presence alone.

Valenced uses express the conscious or subconscious values of those who design, develop, market and control technology, else the understanding of those who use, consume, profit, lose, or are otherwise affected, or both. Insofar as they do, they become embedded in the artifact itself, destroying certain values, making others virtually impossible to fulfill, creating certain (dis)values and increasing the likelihood that others will be realized.[175]

Thus, the idea that a technological artifact can be neutral seems plausible only if we abstract it from the contexts of use and perception.[176] Letters on an otherwise blank sheet of paper are merely a series of abstractions until you rearrange them into, for example, a list of names of poor credit risks; a nuclear bomb would be meaningless junk to a Roman Centurion,

---

[171] *See, e.g.*, JACQUES ELLUL, THE TECHNOLOGICAL SOCIETY 14 (J. Wilkinson trans. 1967).
[172] NEIL POSTMAN, TEACHING AS A CONSERVING ACTIVITY 91 (1979).
[173] RHEINGOLD, *supra* note 162, at 58.
[174] Michael Geist, *Is There A There There?*, 16 BERK. TECH. L. J. 1359, 1401 (2001).
[175] *Id.*
[176] *See* Daniel Chandler, *Engagement with Media: Shaping and Being Shaped*, COMPUTER-MEDIATED COMMUNICATIONS 14:2 (1 Feb. 1996).

but represent very different values to a 21st Century third-grader, even though the latter would have no more knowledge of how to operate such a device than the Centurion. Once we envision a use, technology loses its neutrality and comes to embody any number of symbolic, moral, aesthetic, technical and political meanings.

All tools and media – from language to the computer – embody basic biases towards one kind of use or mode of experience. Any real world application of deterministic or neutral approaches fails to recognize inherent values, but rather treats technology as if it is divorced from regulation or that the relationship is top-down, from regulation to technology, but not vice-versa. Any regulatory approach which fails to recognize that values inhere in artifacts, any approach that fails to recognize that technology influences the market, law and policy, will blindly import those values into the regulation itself. Unfortunately, this is precisely what the *Lawful Access* document does when it suggests lower thresholds for the operation of production orders.

It has become increasingly accepted that establishing effective and enduring guidelines or standards for the [new information and communications technologies] requires the adoption of a 'technology neutral' approach. Technology neutral approaches have been a hallmark of many Internet law policy initiatives, including the development of e-commerce legislation in Canada and the adoption of electronic evidence statutes.[177]

Marshall McLuhan admonished that the unconsciousness effect of any force is a disaster, especially a force that we have made ourselves.[178] The problem with technoneutrality – with treating technology as merely a tool – is not that it imports values, but that it encourages unconscious importation of values and precludes intelligent and principled discussions about whether it would even be desirable to import them. This is the 'technoneutrality trap.' To avoid the trap, we need to understand the value propositions we are adopting in technology. There are a number of approaches we can take to minimize our ignorance of the value propositions inherent in a particular technology: they are discussed elsewhere.[179] It is perhaps enough to note here that, as has been illustrated in earlier sections, the Canadian government has failed to take even the preliminary step to consider how the value construct of traffic data changes the intended meaning of a production order. We will now turn to considering an area of law in which a failure to consider the unintended consequences of diluted judicial standards continues to have grievous effects.

E. Diluted judicial standards grant too much subjective discretion to individual law enforcement officers

[177] Geist, *supra* note 174, at 1373-74.

[178] MARSHALL MCLUHAN, THE GUTENBERG GALAXY: THE MAKING OF TYPOGRAPHIC MAN 248 (1962).

[179] *See, e.g.,*, JASON YOUNG, ROUGH JUSTICE: AN ANALYSIS OF THE CANADIAN PRIVATE COPYING REGIME (unpublished) *available at* http://www.lexinformatica.org/dox/privatecopying.pdf (last visited 20 Nov. 2004).

The requirement that law enforcement first seek independent judicial authorization for warrants serves as a check against the unfettered discretion of individual law enforcement officers and creates a record of accountability subject to audit of abuse and defects in the law.

Under the Highway Traffic Act in Ontario, and similar statutes in other provinces, the standards for search and seizure have been diluted in ways similar to that now proposed in the *Lawful Access* document. A discussion of the policy, jurisprudence and social commentary relating to investigatory detentions can help stakeholders chart future directions in the *Lawful Access* debate.

In 1977, the Etobicoke Police Service implemented an anti-drinking and driving campaign called "Reduce Impaired Driving in Etobicoke" ("R.I.D.E."). The program required police to establish strategic, stationary checkpoints to screen passing motorists for alcohol consumption. Officers screened randomly or on the belief that a motorist might be impaired. Any person refusing a screening test could be detained and subject to criminal sanctions.

The dilution of probable cause under the R.I.D.E. program was mitigated, to an extent, by its high-visibility and by its more or less equal application to all motorists transiting stationary checkpoints. Even if the ultimate decision to screen one motorist and not another was made by a single officer exercising his or her own personal biases, that officer's conduct "can be observed by other officers. Since he [or she] has limited time to observe a vehicle, his [or her] decision will be either truly random or based on some objective basis. The result is that this method of enforcement is somewhat more carefully designed to serve enforcement, less intrusive, and not as open to abuse as [a roving random stop]."[180] Today, the R.I.D.E. program has been expanded across Ontario and into other Canadian jurisdictions.[181] Importantly, it no longer operates under the same organized procedures.

Section 48 of Ontario's Highway Traffic Act,[182] authorizes law enforcement to stop any motorist at any time to determine "whether or not there is evidence to justify making a demand [for a breathalyzer analysis]". A police officer need not satisfy any other grounds – or any objective criteria at all – in order to stop a motorist and subject him or her to a screening test. Similarly, on its face § 216(1) of the *Act* grants police officers authority to stop motor vehicles for any lawful reason related to the enforcement of laws relating to motor vehicle use.

Under § 48 and § 216(1) of the *Act* in Ontario and similar provisions in other provincial statutes throughout Canada, 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. In *Ladouceur*, Sopinka J. observed the flaw in this formula: "If… no reason need be given or is necessary, how will we ever know [if a stop violates

[180] Sopinka J. concurring in result, R. *v.* Ladouceur, [1990] 1 S.C.R. 1257, ¶ 10. U.S. courts have adopted a similar approach in *Michigan Dep't of State Police v. Sitz*, 496 U.S. 444 (1990) (ruling that checkpoint searches do not require "particularized suspicion").

[181] In British Columbia, the equivalent program, established in 1984, is known as "Drinking Driving Counterattack".

[182] R.S.O. 1990, ch. H.8, § 48(1).

the Charter]? The officer need only say, "I stopped the vehicle because I have the right to stop it for no reason. I am seeking unlicensed drivers."[183]

In *R. v. Hufsky*,[184] Le Dain J., writing for a unanimous Supreme Court, held that random stops conducted under an organized "spot check" program and authorized by the Highway Traffic Act did not violate the Charter. The Court concluded that, although the random stop constituted arbitrary detention in violation of § 9 of the Charter, it was justified under § 1 in view of the importance of highway safety. The Court also held that the random stop did not constitute an unreasonable search and seizure in violation of § 8 of the Charter.[185]

1. Subjective assessment can mask discriminatory conduct

In *R. v. Ladouceur*,[186] the Supreme Court expanded the *Hufsky* doctrine in finding that a routine but otherwise "purely random" check under the Highway Traffic Act was an arbitrary detention in violation of § 9 of the Charter, but was reasonably and demonstrably justified in a free and democratic society under § 1. The officers had no basis of suspicion and no other reason to stop the appellant, but the Court held that the power should be justified because the *Act* dealt with a pressing and substantial concern (*i.e.*, highway safety), the random check was the only effective deterrent, and it impaired the § 9 right as little as possible. Although all nine judges of the Court concurred in the result, the minority of four recognized that unlimited police discretion to stop was problematic and for those reasons would have sided with the Ontario Court of Appeal in deciding that the *Act* should be interpreted as being limited "to an organized

[183] *Ladouceur*, *supra* note 180, ¶ 11. Sopinka J. concurred in the result, but not the reasons for judgment. *See also* Alan Young, *All Along the Watchtower: Arbitrary Detention and the Police Function*, 29 OSGOODE HALL L. J. 329, text accompanying n.49 (1991) (describing the operation of General Order 304.10 by the D.C. Metro Police which required the documentation of "contacts" and "stops" in an effort to make police more accountable for their interaction with members of the public, particularly visible-minorities).

[184] [1988] 1 S.C.R. 621, 633.

[185] In the United States, vehicle and "stop-and-frisk" or "Terry" stops are scrutinized under the search and seizure provisions of the Fourth Amendment. Canada deals with investigative detentions under § 9 of the *Charter*, which provides that, "[e]veryone has the right not to be arbitrarily detained or imprisoned." The lawfulness of this type of detention has been recognized and limited in Canada by the Ontario Court of Appeal in *R.* v. *Simpson*, *infra* note 188 and subsequently in the Courts of Appeal of Alberta, Saskatchewan, Newfoundland, Manitoba, Nova Scotia and Québec: *R.* v. *Dupuis* (1994), 162 A.R. 197 (C.A.); *R. v. Lake* (1996), 113 C.C.C. (3d) 208 (Sask. C.A.); *R. v. Burke* (1997), 118 C.C.C. (3d) 59 (Nfld. C.A.); *R. v. G. (C.M.)* (1996), 113 Man. R. (2d) 76 (C.A.); *R. v. McAuley* March 26, 1998, AR97-30-03243, AR97-30-03328 [reported (1998), 124 C.C.C. (3d) 117 (Man. C.A.)]; *R. v. Chabot* (1993), 86 C.C.C. (3d) 309 (N.§ C.A.); *R. c. Pigeon* (1993), 59 Q.A.C. 103.

[186] [1990] 1 S.C.R. 1257.

programme of stopping, like the R.I.D.E. programme, or road-blocks where all vehicles are required to halt, or [stop] for some articulable cause."[187]

Three years later, the Ontario Court of Appeal, in *R. v. Simpson*,[188] narrowed the effective application of *Ladouceur* in finding that an officer's purpose for stopping a vehicle for "purely investigative purposes" unrelated to the enforcement of laws relating to the operation of motor vehicles was not lawful and was not justified on the facts because the detaining officers lacked "articulable cause" for the detention. In justifying the "articulable cause" standard in *Simpson*, Doherty J.A. wrote:

> These cases require a constellation of objectively discernible facts which give the detaining officer reasonable cause to suspect that the detainee is criminally implicated in the activity under investigation. . . . A "hunch" based entirely on intuition gained by experience cannot suffice, no matter how accurate that "hunch" might prove to be. Such subjectively based assessments can too easily mask discriminatory conduct based on such irrelevant factors as the detainee's sex, colour, age, ethnic origin or sexual orientation.[189]

In *Brown v. Durham Regional Police Force*[190] the court considered that a stop may be lawful under § 216 of the Highway Traffic Act even if it is made for purposes other than those related to highway safety matters provided that these other purposes are not themselves improper. Doherty J.A. directly addressed the concern raised in this case:

> While I can find no sound reason for invalidating an otherwise proper stop because the police used the opportunity afforded by that stop to further some other legitimate interest, I do see strong policy reasons for invalidating a stop where the police have an additional improper purpose…. Officers who stop persons intending to conduct unauthorized searches, or who select persons to be stopped based on their sex or colour, or who stop someone to vent their personal animosity toward that person, all act for an improper purpose.[191]

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 visible or be used as a pretext for investigation of unrelated criminal activity. These assumptions are strongly supported by social science research, literature and media reports.[192]

In 1979, in *Delaware v. Prouse*,[193] a motorist challenged the constitutionality of a "random spot check" procedure under which state patrol officers could stop a motorist without probable cause to check the validity of the vehicle's registration or the driver's license.

In ruling in the motorist's favor and striking down the practice, the U.S. Supreme Court considered social science data suggesting that unbridled discretion would lead law enforcement officers to stop individuals on the basis of "salient cues" such as race. The data demonstrated the

---

[187] *Id.* ¶ 13.
[188] (1993), 12 O.R. (3d) 182 (C.A.).
[189] *Id.* ¶ 61.
[190] (1998), 138 C.C.C. (3d) 1 (Ont. C.A.).
[191] *Id.* at 17.
[192] Anthony Thompson, *Stopping the Usual Suspects: Race and the Fourth Amendment*, 74 N.Y.U. L. REV. 956, 974 (1999).
[193] 440 U.S. 648 (1979).

tendency of officers to use their discretionary power to conduct stops, interrogations, and searches of people who are "different" from the racial majority and, more importantly, different from the police officers themselves. Echoing this sentiment in Canada, the Supreme Court in *R. v. Landry* noted that "abuses of police power will rarely affect respectable members of the middle classes," but will instead "focus upon the poor and on the marginal, minority groups."[194]

In the more recent case of *Whren v. United States*,[195] the petitioner cited anecdotal evidence that police officers disproportionately target people of color for traffic stops and requests for consent to search. While acknowledging the difficulties of substantiating the claim of racial motivation given that police departments often fail to document their stops, the petitioner pointed to patterns of police conduct in Florida, Pennsylvania, and Colorado that demonstrated the disproportionate frequency with which officers stop motorists of colour.[196]

In *Indianapolis v. Edmonds*, the court reaffirmed the importance of particularized suspicion over a general interest in crime control:

> We have never approved a checkpoint program whose primary purpose was to detect evidence of ordinary criminal wrongdoing. Rather, our checkpoint cases have recognized only limited exceptions to the general rule that a seizure must be accompanied by some measure of individualized suspicion. We suggested in *Prouse* that we would not credit the "general interest in crime control" as justification for a regime of suspicionless stops. Consistent with this suggestion, each of the checkpoint programs that we have approved was designed primarily to serve purposes closely related to the problems of policing the border or the necessity of ensuring roadway safety. Because the primary purpose of the Indianapolis narcotics checkpoint program is to uncover evidence of ordinary criminal wrongdoing, the program contravenes the Fourth Amendment.[197]

In Toronto, a police board of inquiry, in dismissing a complaint brought against an officer, found that two black men on their way home from work appeared suspicious when they stared "intently" at a marked police car.[198] This suspicious behaviour was enough to justify a stop of the vehicle and a high-risk takedown of its occupants neither of whom were ultimately arrested. The complaint and appeal were dismissed,[199] as was a conduct hearing, which nonetheless observed that while the Board of Inquiry was aware of the "perception held by some members of the public that black motorists are randomly and arbitrarily stopped by police officers for no reason other than the colour of their skin," it was satisfied that the officers' conduct was warranted in light of the "suspicious activity" of the complainant's vehicle.[200]

The Board's ethereal 'public perception' materialized into hard numbers recently in an analysis of Toronto arrest statistics by *The Toronto Star*. Information from the Criminal Information Processing System, a database of all arrests made by Metro Toronto police, proves

---

[194] R. *v.* Landry, [1986] 25 C.C.C. (3d) 1 at 30 (S.C.C.).
[195] 517 U.S. 806 (1996).
[196] *Whren v. United States*, 517 U.S. 806 (1996) (No. 95-5841) (Brief for Petitioners at 18-19).
[197] 531 U.S. 32, 41-42 (2000).
[198] Ontario *v.* Hannah, [1997] 145 D.L.R. (4th) 443, 445 (Ont. Gen. Div. (Div. Ct.)).
[199] David Tanovich, *Using the Charter to Stop Racial Profiling: The Development of an Equality-Based Conception of Arbitrary Detention*, 40 OSGOODE HALL L.J. 145, 155-57 (2002).
[200] Philip Mascoll, *Police Cleared In 'Take Down'*, THE TORONTO STAR, 27 Sept. 1995, at A1.

that police ticket a disproportionate number of blacks for violations that routinely surface only after a stop has been made. In the absence of any other charge, it isn't clear why drivers involved in these offences were stopped in the first place.[201] In the recent case of *R. v. Brown*, the Ontario Court of Appeal made specific note of this problem in affirming the existence of racial profiling.[202] Even more disturbing than the bare facts of these cases, is the observation by former Osgoode Hall law professor, Alan Young, who argued that "we have yet to recognize that vast discretionary powers are exercised by the police that do not ever crystallize into a formal arrest or the laying of a charge."[203] Thus, while it would be easy to dismiss these cases as rare and anecdotal, it would be incorrect to view them as the anything but the tip of the iceberg.

2. Profiling is a function of stereotyping, not racism

It is now beyond debate that police discretion is often exercised on a racial and class basis.[204] The police exercise their discretion in a manner that targets those who appear out of place or simply different from the police themselves; these determinations are often premised upon race or socio-economic factors, but the salient cues could take any form.

"Racial profiling provides its own motivation – a belief by a police officer that a person's colour, combined with other circumstances, makes him or her more likely to be involved in criminal activity."[205] It is said that "officers look for and employ status cues to determine what action they should take; in this sense, 'police activity is as much directed to who a person is as to what he does.'"[206]

In a study of video surveillance use by police in the United Kingdom, Dr. Clive Norris and Gary Armstrong of the Centre for Criminology and Criminal Justice at Hull University found that

---

[201] *Brown*, *infra* note 202, ¶ 94; *see also Police Target Black Drivers*, THE TORONTO STAR, 20 Oct. 2002; *The Story Behind the Numbers*, THE TORONTO STAR, 19 Oct. 2002; *Treatment Differs By Division*, THE TORONTO STAR, 19 Oct. 2002.

[202] *R. v. Brown* [16 April 2003], Toronto C37818 (Ont. C.A.) (the court differentiated the act of stereotyping from racism).

[203] Young, *supra* note 183, at 341.

[204] R. Harper, *Has the Replacement of Probable Cause with Reasonable Suspicion Resulted in the Creation of the Best of All Possible Worlds*, 22 AKRON L. REV. 13, 38 (1988). ("Research suggests that while the police do tend to detain and arrest blacks at a higher rate than they do whites with whom they come in to [sic] contact, it is probable that race, in itself, is not the explanatory factor. It is more likely that poverty and low socio-economic status, with which race tends to be associated, figure more importantly into the police detention and arrest decision. It is thus in poorer neighbourhoods, where the police presence is likely to be greater, where the citizens' demeanour toward the police may be interpreted as offensive, and where the people with whom the police interact generally lack resources and other indicia of social power, that the police are less likely to refrain from stopping citizens for investigation.") *See also* Sheri Johnson, *Race and the Decision to Detain a Suspect*, 93 YALE L.J. 214 (1983).

[205] *Brown*, *supra* note 202, ¶ 86..

[206] Young, *supra* note 183.

> the gaze of the cameras do not fall equally on all users of the street but on those who are stereotypically predefined as potentially deviant, or through appearance and demeanor are singled out by operators as unrespectable. In this way youth, particularly those already socially and economically marginal, may be subject to even greater levels of authoritative intervention and official stigmatization, and rather than contributing to social justice through the reduction of victimization, [surveillance] will merely become a tool of injustice through the amplification of differential and discriminatory policing.[207]

According to former Harvard Business School professor, Renato Tagiuri, we cluster information into categories which leads inevitably to prejudgment based upon our perceptions of those groupings. Stereotypes have been defined as the "general inclination to place a person in categories according to some easily and quickly identifiable characteristic such as age, sex, ethnic membership, nationality, or occupation, and then to attribute to him qualities believed to be typical of members of that category."[208] Of course, stereotypes about groups tend not to be any more accurate than any other type of generalization because they represent oversimplification of complexities.[209] But we tend to rely on them and, at times, to be prejudiced by them in making complex discretionary decisions.

State intrusion in the name of law enforcement has a tendency to expand into social control of groups perceived to be deviant or marginalized. The history of "street powers… demonstrates that the traditional practices of law enforcement on the streets have had very little connection with crime *per se* and a great deal to do with social control of the urban populace."[210]

3. A lower threshold for engaging in electronic surveillance could lead to profiling by law enforcement and the de facto *offence of,* inter alia*, 'surfing while Muslim'*

The Supreme Court has justified reduced judicial scrutiny of investigative detentions under the Ontario Highway Traffic Act, and equivalent statutes in other provinces, on the grounds that highway safety poses a reasonable and justifiable limit on § 9 and § 8 rights under the Charter. However, time and increased public attention have raised important considerations

---

[207] CLIVE NORRIS & AND GARY ARMSTRONG, THE UNFORGIVING EYE: CCTV SURVEILLANCE IN PUBLIC SPACES 8 (1998) (the study also determined that camera operators focused most frequently on attractive females and males who wore caps, were visible minorities or who looked at the cameras).

[208] Renato Tagiuri, *Person Perception, in* G. LINZEY & E. ARONSON, EDS., HANDBOOK OF SOCIAL PSYCHOLOGY (2nd ed. 1985).

[209] *See* Russell Spears, *From Personal Pictures in the Head to Collective Tools in the World, in* C. MCGARTY ET AL., EDS, STEREOTYPES AS EXPLANATIONS: THE FORMATION OF MEANINGFUL BELIEFS ABOUT SOCIAL GROUPS (2002) (shared stereotypes allow groups to represent and change social reality); Bernd Wittenbrink, et al., *Structural Properties of Stereotypic Knowledge and Their Influences on the Construal of Social Situations*, 72 J. OF PERSONALITY & SOCIAL PSYCH. 526-543 (1997) (stereotypic assumptions about cause-effect relations provide important constraints for the causal structure underlying the perceiver's subjective representation of social information).

[210] M. Brogden, *Stopping the People – Crime Control Versus Social Control, in* J. BAXTER & L. KOFFMAN, EDS., POLICE: THE CONSTITUTION AND THE COMMUNITY 106 (1985).

regarding the lack of objective criteria for investigative detentions. First, 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. Second, a lower threshold precludes effective judicial and public oversight of inevitable Charter 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.[211]

The *Lawful Access* document proposed broadening investigatory powers under the Criminal Code and other statutes and, in so doing, ignored the lessons learned in the investigative detention context in North America and in video surveillance of public spaces by law enforcement in the United Kingdom.[212] Why should we expect that reduced judicial scrutiny – as applied to digital communications – will be any less discriminatory simply because we are traveling on a digital and not an asphalt highway? Indeed, we should expect that reduced scrutiny of cybercrime investigations could easily be more discriminatory than we have already seen in the highway safety context, for the reasons already discussed elsewhere, namely that: 'traffic data' and 'content data' are difficult to divorce from each other such that the act of 'stopping' a packet is the same as searching it; when you 'stop' one target packet, there is a high-probability that you will stop unintended packets along with it; and, the richness of available data increases the potential if not the propensity for abuse.

Reduced judicial oversight and the natural predilection of even the most fair-minded person to prejudge their perceptions has, in the context of investigative detentions of drivers, led down a slippery slope of subjectivity that many Black North Americans euphemistically call "DWB", the offence of "Driving While Black".[213] The reality is that while discretion is the hallmark of individualized justice, it can easily contain the seeds of inequity. Without procedural safeguards, discretion will often be exercised in a manner not consonant with the goals and spirit of valid legislative objectives.[214]

In the present political atmosphere and in the context of the *Lawful Access* 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 Canada, of "Surfing While Muslim". Salient interests could include a Muslim-sounding name, an IP address from an Arab country or organization, an online purchase of the most recent book by

---

[211] *See, e.g.,, Brown, supra* note 202.

[212] LAWFUL ACCESS, *supra* note 1, 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).

[213] *See* D. HARRIS, AMERICAN CIVIL LIBERTIES UNION, DRIVING WHILE BLACK: RACIAL PROFILING ON OUR NATION'S HIGHWAYS (1999) *available at* http://www.aclu.org/profiling/report (last visited 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 (2000); G. Webb, *DWB*, ESQUIRE 131:4 (Apr. 1999) 118.

[214] *See, e.g.,,* K. Lunman, *Muslims 'Threatened' by New Law, Group Says*, THE GLOBE & MAIL, 15 May 2003, at A7 (Muslim group argues discretionary powers under the Anti-terrorism Act, S.C., 2001, ch. C-41 used to profile Muslims citizens).

author 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.

Some might be inclined to suggest that we could engineer technology to filter for bias in the same way that we could engineer it to discriminate. Accordingly, we would create a filter which could take undesirable operator valences into account. For the sake of argument, let us assume that the earlier discussion of congenital engineering flaws in packet-based systems does not apply and consider the bias question in isolation.

The first flaw in this argument is that it assumes that the technological medium is without inherent bias, and that additionally we can perfectly audit and engineer the biases of those who design and operate these filters, neither of which are true.

Technology is not neutral[215], moreover it is biased in particular ways,[216] which are frequently unknown to us.[217] In fact, the easiest argument to make to those who are reluctant to ascribe values to technological artifacts is to argue that some technologies are valenced towards *particular* uses.

Indeed, the idea that a technological artifact can be neutral seems plausible only if we abstract it from the contexts of use and understanding.[218] Once we envision a use, technology loses its neutrality and comes to embody any number of symbolic, moral, aesthetic, technical and political meanings.[219]

The second flaw in the 'engineering out' argument is that when placed in the larger context of regulation, it fails to answer the question of why we need to adopt a lower standard for investigatory procedures. If we could engineer a perfect filter, then adopting a lower standard would be superfluous. On the other hand, if we cannot achieve perfection, then we must consider how regulation will unconsciously import unwanted and unintended values into law.

This is not to say that we could not or should not try to factor the valence of technology: this is the thesis statement for this paper. A regulatory approach which fails to recognize that values embed in artifacts; an approach that fails to recognize the imprint of the designer or user on an artifact; an approach that fails to recognize that ultimately technology influences the market, law and policy, will blindly import those values into the regulation itself. Unfortunately, these approaches have become the default, if not the norm in many areas outside the one under consideration here, but here also. In the Canadian cybercrime context, factoring for undesirable technological value does not lead us towards the kind of regulation discussed herein, but away from it.

---

[215] *See generally* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).
[216] *See generally* RHEINGOLD, *supra* note 160.
[217] *See, e.g.,,* Holland, *supra* note 161; Light, *supra* note 161.
[218] *See* Chandler, *supra* note 176.
[219] *See, e.g.,,* JASON YOUNG, GHOST IN THE SHELL: THE MYTH OF TECHNONEUTRALITY AND POLICYMAKING FOR PRIVACY (unpublished) *available at* http://www.lexinformatica.org/dox/ghostintheshell.pdf (last visited 20 Nov. 2004).

V. CONCLUSION

Applying traditional rules of electronic surveillance to the persistent, pervasive and permanent information realm of cyberspace is not simply maintenance of the *status quo*, but rather introduces new and unique implications for privacy and freedom of expression. The Canadian government's lawful access initiatives have failed to provide any meaningful justification for the proposed expansion of powers, save to suggest that Canada has an international obligation to adopt the Council of Europe Convention on Cyber-crime, that many of the most problematic amendments are merely cosmetic, and that the purpose of the initiative is simply to maintain the *status quo*.

The reality is that the proposed amendments in the *Lawful Access* document would have the effect of moving criminal investigations away from carefully constructed standards of reasonable and probable cause – that an investigator has sufficient grounds to believe that a *specific* person has committed or is likely to commit an offence – towards the general proposition that everyone is potentially of interest simply for "driving on the information highway."

There is little doubt that new information and communications technologies are impeding traditional investigations of crime, including online crime. Moreover, it is uncontested that at some point in the near future, we may see new kinds of *sui generis* cybercrime – identity theft is the first portent of this – which may require the articulation of different legal standards. At present, cybercrime is little more than conventional crime by less conventional means. Without more information, it would be heavy-handed to promulgate sweeping new changes in law. Unlike highway safety legislation which permits reduced judicial oversight for investigations related to highway safety, the argument that new legal standards are required to effectively combat cybercrime is not rationally connected to promoting safety or ameliorating a well-defined and serious social problem.

Stanford law professor, Lawrence Lessig, has observed that more than law alone enables legal values, and law alone cannot guarantee them.[220] In cyberspace, and in cybercrime investigations, frequently code and technical standards are as important as law. The *Lawful Access* document 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. Empirical analysis supports the conclusion that improved *technological* and *administrative* solutions would substantially address the public policy objectives of lawful access. The author suggests that a holistic approach aimed at reducing the impediments of cybercrime investigation and prosecution will be more effective than a narrowly legal approach. Most importantly, such an approach would very likely have less of an impact on Canadians' constitutional rights and freedoms.

The government recognizes the importance of code-as-law to the degree that it seeks to compel telecommunications and Internet service providers to provide the technical capability for *Lawful Access*, but fails to factor technological values into the consideration of the standard for access to traffic data. In many instances, traffic data will reveal as much if not more about one's lifestyle, intimate relations or political or religious opinions as content data. Canadian courts

[220] Lawrence Lessig, *The Law of the Horse: What Cyberspace Might Teach*, 113 HARV. L. REV. 501 (1999).

have determined that such information attracts a reasonable expectation of privacy, particularly in the criminal investigation context. Further, the line between traffic and content will only become more blurred as Canadians expand their daily activities in cyberspace, providing increased opportunities for linkages between formerly discrete aspects and transitory bits of our personal lives.

Similarly, the federal government has singularly failed to consider the implications that increased individual discretion under a lower authorization threshold will have on Charter rights in cyberspace. Investigation is a legitimate and necessary police power, but efforts must be made to ensure it does not blossom into a form of panoptic surveillance.

We cannot afford to wait to vindicate privacy only after it has been violated, this is inherent in the notion of being secure against unreasonable searches and seizures. Invasions of privacy must be prevented, and where privacy is outweighed by other societal claims, there must be clear rules setting forth the conditions under which it can be violated. The factual foundation of 'reasonable and probable' grounds that an offence has been or will be committed is not only a safeguard against unfettered individual discretion, but it creates a record of accountability subject to audit of abuse of authority and inevitable defects in the law.

Cybercrime initiatives have grave implications for privacy and freedom of expression in Canada and elsewhere. The conclusion we cannot fail to reach is that applying traditional rules of electronic surveillance to the realm of cyberspace is, in fact, not simply maintaining the *status quo*.