Facebook, Streetview, and What's Next: Navigating Your Way Through New Issues in Privacy Law

Alex Cameron

Fasken Martineau DuMoulin LLP

Paper presented to *15th Biennial National Conference: New Developments in Communications Law and Policy*

April 23-24, 2010

National Arts Centre, Ottawa

Facebook, Streetview, and What's Next:

Navigating Your Way Through New Issues in Privacy Law

Alex Cameron
Fasken Martineau DuMoulin LLP

Facebook, Streetview, and What's Next:
Navigating Your Way Through New Issues in Privacy Law

Alex Cameron[1]

Fasken Martineau DuMoulin LLP

INTRODUCTION

Privacy issues are present at the heart of many new developments in communications law, policy and practice. Privacy questions are central, for example, in cloud computing, in individuals' and organizations' use of social media, and in behavioural advertising, traffic management/network neutrality, anti-spam legislation, and lawful access legislation, among other areas. New and emerging technologies frequently pose challenges for privacy laws and regulatory authorities and raise fundamental questions regarding social norms about privacy. In January 2010, the following statement by Facebook's co-founder, President and CEO, Mark Zuckerberg, became a focal point of debate about the current state of privacy:[2]

> People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time. We view it as our role in the system to constantly be innovating and be updating what our system is to reflect what the current social norms are.

---

[1] Alex Cameron is an associate in the Litigation Group and the Privacy and Information Protection Group at Fasken Martineau DuMoulin LLP in Toronto. Called to the bar in British Columbia and Ontario, his practice focuses on commercial litigation and legislative compliance matters, including privacy, access to information, and technology and intellectual property. Published in 2008, the Office Privacy Commissioner of Canada commissioned Alex to write a landmark privacy report for businesses, titled *Leading by Example: Key Developments in the First Seven Years of PIPEDA*. Alex is also a doctoral candidate in law at the University of Ottawa. He can be reached at acameron@fasken.com. Alex wishes to thank Laurie Turner and Susan Newell for their outstanding contributions to this paper and Sarah Turney for her significant contribution to an earlier draft of a portion of this paper. Laurie, Susan and Sarah are articled students at Fasken Martineau DuMoulin LLP. Alex Cameron also wishes to thank the organizers of the *15th Biennial National Conference: New Developments in Communications Law and Policy*, and in particular Robert J. Buchan and Laurence J.E. Dunbar, for the invitation to participate in that leading conference. The views expressed herein are the author's alone.

[2] See *e.g.* Ann Cavoukian, "Privacy is still a social norm" *The Globe and Mail* (15 March 2010), online: <http://www.theglobeandmail.com/news/opinions/privacy-is-still-a-social-norm/article1499215/>.

> A lot of companies would be trapped by the conventions and their legacies of what they've built, doing a privacy change - doing a privacy change for 350 million users is not the kind of thing that a lot of companies would do. But we viewed that as a really important thing, to always keep a beginner's mind and think what would we do if we were starting the company now and **we decided that these would be the social norms now and we just went for it**.[3]

In the passage above, Zuckerberg was alluding to Facebook's decision to make changes to its privacy controls in late 2009.[4] That decision was made following an in-depth investigation of Facebook by the Office of the Privacy Commissioner of Canada ("OPC") earlier in 2009.[5] Yet, notwithstanding the OPC's investigation and Zuckerberg's claim that social norms have changed, some of the changes that Facebook announced in late 2009 were criticized for removing privacy controls over certain information[6] and for making, by default, certain information on Facebook more public than it had been in the past.[7] Facebook's changes sparked a new complaint to the OPC; an investigation is underway.[8] In the meantime, on March 26, 2010, Facebook announced that it was planning to make yet more controversial changes to its privacy practices.[9]

---

3 Interview of Mark Zuckerberg by Michael Arrington (8 January 2010) in "Facebook Founder on Privacy: Public is the New Social Norm" *Mashable The Social Media Guide*, online: <http://mashable.com/2010/01/10/facebook-founder-on-privacy/>. [emphasis added]

4 Letter from Mark Zuckerberg (1 December 2009), online: <http://blog.facebook.com/blog.php?post=190423927130> [Zuckerberg].

5 Office of the Privacy Commissioner of Canada, News Release, "Facebook agrees to address Privacy Commissioner's concerns" (27 August 2009), online: OPC <http://www.priv.gc.ca/media/nr-c/2009/nr-c_090827_e.cfm>.

6 Kevin Bankston, "Facebook's New Privacy Changes: The Good, The Bad, and The Ugly" Electronic *Frontier Foundation* (9 December 2009), online: Electronic Frontier Foundation <http://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly> [Bankston]; Ryan Tate, "The Facebook Privacy Settings You've Lost Forever" *Gawker* (undated), online: Gawker <http://gawker.com/5428155/the-facebook-privacy-settings-youve-lost-forever>.

7 Bankston, *ibid*; Zuckerberg's own photographs and other personal information became public as a result of the changes, see: Ryan Tate, "Facebook CEO's Private Photos Exposed by the New 'Open' Facebook" *Gawker* (16 December 2009), online: Gawker <http://gawker.com/5423914/the-intimate-facebook-ceo-pics-exposed-by-facebooks-privacy-rollback/>.

8 Office of the Privacy Commissioner of Canada, News Release, "Privacy Commissioner Launches New Facebook Probe" (27 January 2010), online: OPC < http://www.priv.gc.ca/media/nr-c/2010/nr-c_100127_e.cfm>.

9 Letter from Michael Richter (26 March 2010), online: <http://blog.facebook.com/blog.php?post=376904492130> [Richter].

Providing an interesting and timely contrast to Zuckerberg's statement above, on March 17, 2010 it was announced that a California court had approved a $9.5 million settlement in a class-action lawsuit against Facebook regarding its now infamous Beacon advertising program launched in 2007.[10] That program was cancelled in late 2009. Some of the criticisms that had been levelled against Beacon were similar to the ones that followed Facebook's privacy changes in late 2009 and its further proposed changes announced in March, 2010.[11] In fact, one commentator characterized Facebook's latest proposed changes as sounding like "Beacon in reverse": "Where that now-shuttered program had Facebook publishing details of users' activities on other sites to their Facebook profiles, here Facebook would push some of their profile data out to other sites."[12]

Following a public groundswell of opposition to Beacon, in December 2007 Zuckerberg apologized for the way that Beacon had shared individuals' information by default, without requiring them to opt-in to the program:

> When we first thought of Beacon, our goal was to build a simple product to let people share information across sites with their friends. It had to be lightweight so it wouldn't get in people's way as they browsed the web, but also clear enough so people would be able to easily control what they shared. We were excited about Beacon because we believe a lot of information people want to share isn't on Facebook, and if we found the right balance, Beacon would give people an easy and controlled way to share more of that information with their friends.
>
> But we missed the right balance. At first we tried to make it very lightweight so people wouldn't have to touch it for it to work. The problem with our initial approach of making it an opt-out system instead of opt-in was that if someone forgot to decline to share

---

[10] *Sean Lane, et. al. v. Facebook Inc, et al.,* (N.D. Cal. 2010 –No. C 08-3845 RS), online: Wired <http://www.wired.com/images_blogs/threatlevel/2010/03/beaconbeacon.pdf>.

[11] Richter, *supra* note 9; Kelly Fiveash, "Facebook prepares for another privacy row with its users" *The Register* (29 March 2010), online: The Register <http://www.theregister.co.uk/2010/03/29/facebook_privacy_tweaks/>.

[12] Rob Pegoraro, "Facebook privacy changes would share user data with other sites" *The Washington Post* (29 March 2010), online: The Washington Post <http://voices.washingtonpost.com/fasterforward/2010/03/facebook_privacy_changes_would.html>; Another commentator characterized the move as "Facebook Beacon done right (for Facebook)", see: Larry Dignan, "Facebook's privacy changes: When will it go too far (and will you even notice?)" *ZDNet* (29 March 2010), online: *ZDNet* <http://blogs.zdnet.com/BTL/?p=32427>.

> something, Beacon still went ahead and shared it with their friends.[13]

Thus, notwithstanding that new technologies can and do pose challenges for privacy, privacy appears to be alive and well in the eyes of the law (as evidenced by the OPC investigations into Facebook and the Beacon settlement, among other developments) and as a social norm (as evidenced by the public and media responses to the Beacon program and to Facebook's 2009 and potential 2010 privacy changes).[14] It is also remarkable that the very platform – Facebook – that has been a cause of privacy consternation for many of its users has also proved to be a powerful and effective tool for mobilizing opposition to some of the privacy changes that have caused the most concern for many Facebook users. Consider that as of April 8, 2010, the Facebook group "MILLIONS AGAINST FACEBOOK's PRIVACY POLICIES AND LAYOUT REDESIGN" had nearly 2.3 million Facebook users as members.[15]

This paper endeavours to briefly review and stimulate discussion about some of the key privacy issues present in contemporary communications practice, law and policy. Part I of this paper describes three landmark developments at the intersection between privacy and emerging technologies: XCP digital rights management, Facebook, and street-level imaging, with a focus on the example of Google Street View. Although those three developments are not uniquely Canadian, each involved leading action by the OPC. The Facebook example in particular is representative of the leading role that Canada has played on matters of global privacy. Part II of the paper looks ahead to a number of privacy issues on the near horizon, including social media, cloud computing, online tracking and advertising, and a handful of potential legislative developments in Canada (*e.g.* reform of the *Personal Information Protection and Electronic Documents Act* (PIPEDA)[16] and potential re-introduction of the *Electronic Commerce Protection*

---

[13] Letter from Mark Zuckerberg (5 December 2010), online: <http://blog.facebook.com/blog.php?post=7584397130> [Zuckerberg, "Beacon"].

[14] See, for example, Caroline McCarthy, "Rough seas nearly sink Facebook's Beacon" *CNET News* (30 November 2007) online: CNET <http://news.cnet.com/8301-13577_3-9826664-36.html>; Moveon.org, a civic action organization, formed an online petition and pro-privacy Facebook group in response to Beacon. The Facebook group grew to over 80,000 members. See: "Recent Success Stories" *Moveon.org* (undated), online: Moveon.org <http://www.moveon.org/success_stories.html>; See the comments of Facebook users in response to Mark Zuckerberg's letter, "Thoughts on Beacon", at Zuckerberg, "Beacon" *supra* note 13.

[15] See <http://www.facebook.com/group.php?gid=27233634858>. See also, *ibid.*

[16] S.C., 2000, c. 5.

Act[17]). Finally, Part III reflects on several key questions and themes raised by the examples discussed herein and concludes with a look to future work and challenges in the area.

I. PRIVACY AND EMERGING TECHNOLOGIES

Technology often raises privacy questions.[18] Indeed, PIPEDA was enacted in part as a response to the privacy issues raised by technology: "[t]he purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information…"[19] Focusing on matters relating to communications practice, law and policy, this Part reviews three high-profile examples of the nexus between privacy and technology.

(A) XCP digital rights management

Digital rights management technology ("DRM") is a term commonly used to refer to technological systems used by copyright holders and others to automatically regulate access to and manage rights in relation to information, including copyright works.[20] DRM functions to control copyright works, principally to collect payments for uses of works and to prevent works from being accessed or used (*e.g.* copied) in unauthorized ways.[21] In fulfilling its protective and rights management roles, DRM typically contains monitoring and reporting functionality.[22]

---

[17] Canada, Bill C-27, *Electronic Commerce Protection Act*, 2nd Session, 40th Parl., 2009 [ECPA]. This bill did not become law before the 2nd Session of the 40th Parliament ended on December 30, 2009.

[18] For a discussion of the privacy questions posed by GPS and biometrics technologies, for example, see: Canada, Office of the Privacy Commissioner of Canada, *Leading by Example Key Developments in the First Seven Years of the Personal Information Protection and Electronics Documents Act (PIPEDA)* (Ottawa: Minister of Public Works and Government Services Canada, 2008), online: OPC <http://www.priv.gc.ca/information/pub/lbe_080523_e.cfm#ftnref44>. The author was commissioned by the OPC to draft that report. See also *Wansink v. TELUS Communications Inc.* 2007 FCA 21 (CanLII) (finding the use of voiceprint biometrics reasonable under PIPEDA).

[19] PIPEDA, *supra* note 16 at section 3.

[20] See Mark Stamp, "Risks of digital rights management" (2002) 45 Communications of the ACM 120 (discussing DRM as a form of "remote control" over works after the works have been delivered to users).

[21] See generally, Niels Rump, "Digital Rights Management: Technological Aspects–Definition, Aspects, and Overview" in Eberhard Becker et al., eds., *Digital Rights Management-Technological, Economic, Legal and Political Aspects* (Berlin: Springer-Verlag, 2003) [Rump, "DRM"].

[22] See generally U.S., *Information Infrastructure Task Force, Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights*, (September 1995) at 187, online: US Patent and Trademark Office <http://www.uspto.gov/web/offices/com/doc/ipnii/ipnii.pdf> ("These systems will serve the functions of tracking and monitoring uses of copyrighted works as well as licensing of rights and indicating attribution, creation and ownership interests" at 191); Niels Rump, "Digital Rights Management: Technological Aspects–Definition, Aspects, and Overview" in Eberhard Becker et al., eds., *Digital*

These functions permit copyright holders to track accesses and uses of their works and, through the DRM, to automatically grant or refuse permissions and to collect payments.[23] Identification and authentication of individuals or devices endeavoring to access or use works is a key part of many DRM systems. In other words, DRM needs to know whether the person requesting access or use of a work is a person who has authorization to do so.[24]

In October 2005, Sony-BMG was the subject of a high-profile privacy controversy regarding its Extended Copy Protection (XCP) DRM technology.[25] When an individual inserted a music CD containing XCP DRM into their Windows computer, a program was installed on their computer. The program was designed *inter alia* to prevent copying of the CD. Mark Russinovich, an expert in operating system architecture and design, was the first to report concerns about the XCP DRM program on his blog: "Sony put software on my system that uses techniques commonly used by malware to mask its presence [and] the software is poorly written and provides no means for uninstall. Worse, most users […] will cripple their computer if they attempt the obvious step of deleting the cloaked files."[26] Russinovich also reported that the XCP DRM caused security vulnerabilities in the computers and networks that it was installed on.[27]

Rights Management-Technological, Economic, Legal and Political Aspects (Berlin: Springer-Verlag, 2003) at 4; Ian Kerr and Jane Bailey, "The Implications of Digital Rights Management for Privacy and Freedom of Expression" (2004) 2 *Info, Comm & Ethics in Society* 87 at 89-91.

[23] See Rump, *ibid*; Jeffrey P. Cunard, "Technological Protection of Copyrighted Works and Copyrighted Management Systems: A Brief Survey of the Landscape," ALAI Congress (2001) at 2, online: ALAI <www.alai-usa.org/2001_conference/pres_cunard.doc>; Lawrence Lessig, *Code version 2.0* (New York: Basic Books, 2006) at 191.

[24] See generally Chris J. Hoofnagle, "Digital Rights Management: Many Technical Controls on Digital Content Distribution Can Create a Surveillance Society" (2004) 5 Colum. Sci. & Tech. L. Rev. 1 at 3; Deirdre K. Mulligan, John Han & Aaron J. Burstein, "How DRM-based content delivery systems disrupt expectations of 'personal use'" in *Proceedings of the 2003 ACM workshop on Digital rights management* (New York: ACM Press, 2003) at 82-83; Julie Cohen, "A Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace" (1996) 28 Conn. L. Rev. 981; Lessig, *Code version 2.0*, *ibid*. (noting that trusted systems are dependent on information about how products are used and thus need to track and monitor).

[25] See *e.g.* Mark Russinovich, "Sony, Rootkits and Digital Rights Management Gone Too Far", Mark's Blog (31 October 2005), online: Mark Russinovich <http://blogs.technet.com/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx>; Bruce Schneier, "Real Story of the Rogue Rootkit", Wired.com (17 November 2005), online: Wired <http://www.wired.com/politics/security/commentary/securitymatters/2005/11/69601>; Jeremy DeBeer, "How Restrictive Terms and Technologies Backfired on Sony BMG" (2006) 6 *Internet & E-Commerce Law in Canada* 93 [deBeer, "Backfired"].

[26] *Ibid*.

[27] *Ibid*.

In the wake of the above reports, the US Computer Emergency Readiness Team, an arm of the National Cyber Security Division at the Department of Homeland Security, issued a recommendation that individuals not install software from audio CDs.[28] Microsoft categorized the XCP DRM as 'spyware'.[29]

The XCP DRM raised privacy questions because when an XCP-enabled CD was played on a computer with an Internet connection, the program reportedly opened the individuals' computer to potential attack by hackers and viruses. The program could also reportedly "phone home"[30] to send information to Sony-BMG, including the computer's internet protocol (IP) address, information about when a CD was played and information about whether the individual had attempted to copy the CD.[31]

The OPC provided the following account of its privacy-related concerns in connection with technology protection measures components of DRM, "especially those [such as XCP DRM] that are based on rootkit technology":

> Failing to give adequate notice that these technologies are being used and failing to obtain informed consent from users;
>
> Automatically installing files even when users choose not to run the application. Although users may be presented with terms and conditions that refer to software installation before launching the CD, it appears safe to assume that few, if any, realize that doing so could result in a security and potential privacy risk;

---

[28] U.S., United States Computer Emergency Readiness Team, *First 4 Internet XCP (Sony DRM) Vulnerabilities* (18 November 2005), online: US CERT <http://www.us-cert.gov/current/archive/2005/11/21/archive.html#xcpdrm>.

[29] "Microsoft to remove Sony CD code" *BBC News* (14 November 2005), online: BBC News <http://news.bbc.co.uk/1/hi/technology/4434852.stm>.

[30] Graham Greenleaf, "IP, Phone Home: Privacy as Part of Copyright's Digital Commons in Hong Kong and Australian Law" in Lawrence Lessig, ed., Hochelaga Lectures 2002: The Innovation Commons (Hong Kong: Sweet & Maxwell Asia, 2003).

[31] See *e.g.* Dan Kaminsky, "Welcome To Planet Sony", DoxPara Research (15 November 2005), online: Doxpara <http://www.doxpara.com/?q=sony>; Interview of Ari Schwartz, *et al*. by Neda Ulaby, (2005) in "Sony Music CDs Under Fire from Privacy Advocates", National Public Radio (4 November 2005), online: <http://www.npr.org/templates/story/story.php?storyId=4989260>; deBeer, "Backfired" *supra* note 25 (describing how the DRM technologies at issue "surreptitiously monitor and report information about consumers' computer systems and listening activities" at 98); Office of the Privacy Commissioner of Canada, "Fact Sheet: Digital Rights Management and Technical Protection Measures" (November 2006), online: OPC <http://www.privcom.gc.ca/fs-fi/02_05_d_32_e.asp> [OPC, "DRM Fact Sheet"].

> Requiring users to reveal their identity and rights to access protected content, thus preventing the anonymous consumption of content;
>
> Facilitating the profiling of users' preferences or limiting access to certain content. This is done by assigning an identifier to content or to the content player, and attaching personal information to the identifier. If based on online verification, DRMs may invade people's privacy by tracking personal data and transmitting them to DRM managers;
>
> Establishing a connection with the vendor's site and sending the site an ID associated with the media or content. Vendors may not be doing anything with the data, but with this type of connection their servers could record each time a copy-protected CD is played and the IP address of the computer playing it; and
>
> Failure of the uninstaller programs to completely remove the software.[32]

Class action lawsuits regarding XCP DRM were launched and ultimately settled in several Canadian provinces.[33] In the settlement agreement, Sony BMG maintained that some of the privacy concerns about the XCP DRM were without merit. Nevertheless, Sony BMG agreed *inter alia* to take steps to destroy information collected through the XCP DRM within 10 days after collecting it.[34] As part of the settlement, Sony BMG also agreed to and subsequently did retain an independent third-party to verify the above representations.[35]

---

[32] OPC, "DRM Fact Sheet", *ibid*.

[33] Sony-BMG established a website to provide information regarding the settlements: "Information Website", *Sony BMG* (28 June 2007), online: BMG <http://cdtechsettlement.sonybmg.ca/en/>; See also Jeremy deBeer, "Sony BMG Settles Canadian Class Actions", *Jeremy deBeer* (19 November 2006), online: Jeremy deBeer <http://www.jeremydebeer.ca/index.php?option=com_content&task=view&id=87>.

[34] The settlement that was reached was published by Sony BMG on its website. See, <http://cdtechsettlement.sonybmg.ca/en/pdfs/SettlementAgreement-English.pdf> ("No Collection of Personal Data. SONY BMG asserts that it has not used the MediaMax or XCP Software […] to collect, aggregate or retain Personal Data about persons who listened to XCP CDs or MediaMax CDs on computers, without such persons' express consent. SONY BMG further asserts that it has only collected information necessary to provide enhanced CD functionality. SONY BMG believes and, on that basis, asserts that such functionality requires that the album title, artist, IP address, and certain non-personally identifiable information be collected. […] SONY BMG will take commercially reasonable steps to destroy the information it collects to provide enhanced CD functionality, including logs of IP addresses, within ten (10) days after the collection of such data […] SONY BMG shall, however, be permitted to compile aggregate, non-personally identifiable data about hits to its servers from enhanced CDs").

[35] "Privacy Assessment" *Sony BMG* (2006), online: Sony BMG< http://www.sonymusic.com/xcp-mediamax/Privacy_Assessment_final.pdf>.

The XCP DRM incident came at a time of intense debate regarding DRM technologies in Canada. Several months before the XCP DRM story broke, the Canadian government had introduced *Bill C-60*[36] to amend the *Copyright Act*.[37] Among other things, that law would have provided legal protection to the technology protection measures, components of DRM. As such, looking back on the incident today one might not find it surprising that the XCP DRM incident, including its potential privacy ramifications, attracted the attention of individuals, regulators, the mainstream press and others at that time.[38]

Nonetheless, with action by the Department of Homeland Security[39], with class actions launched in Canada[40], New York[41], and California[42], with the Texas Attorney General commencing an action alleging, among other things, that the XCP DRM system violated the state's spyware and deceptive trade practices laws[43], among other responses, the XCP DRM incident unquestionably put the technology-privacy nexus on the map in a way that no previous incident had done. In retrospect, the incident also demonstrates that online privacy issues existed before Facebook – which was made available to the public only as of September 2006 – difficult as it may be for some younger readers to believe that *anything* existed "pre-Facebook".[44]

---

[36] *An Act to Amend the Copyright Act,* 1st session, 38th Parl., 2005.

[37] R.S., 1985, c. C-42 [Copyright Act].

[38] See *e.g.* Tom Zeller, "Sony BMG Sued over CD's with Anti-Piracy Software" *New York Times* (22 November 2005), online: NY Times <http://www.nytimes.com/2005/11/22/technology/22sony.html> [Zeller]; "Sony sued over copy-protected CDs" *BBC News* (10 November 2005), online: BBC News <http://news.bbc.co.uk/2/hi/technology/4424254.stm>[BBC, "Copy-protected"]; Elizabeth Bowles and Eran Kahana, "The 'agreement' that sparked a storm" (2007) 16 Business Law Today, online: American Bar Association <http://www.abanet.org/buslaw/blt/2007-01-02/kahana.shtml>; Richard Menta, "Bush Administration to Sony: It's your intellectual property – it's not your computer" *MP3 Newswire* (11 December 2005), online: MP3 Newswire <http://www.mp3newswire.net/stories/5002/admonish.html> [Menta]; Joshua Merchant, "Sony Class Action Settlement Info" *Merchant Law Group LLP* (21 April 2009), online: Merchant Law Group LLP <http://www.merchantlaw.com/classactions/sony.php> [Merchant].

[39] *Supra* note 28.

[40] Merchant, *supra* note 38.

[41] Zeller, *supra* note 38.

[42] *Ibid*.

[43] Texas Attorney General, Press Release, "Attorney General Abbott Brings First Enforcement Action In Nation Against Sony BMG For Spyware Violations" (21 November 2005), online: OAG <http://www.oag.state.tx.us/oagnews/release.php?id=1266>.

[44] Letter from Carolyn Abram, (26 September 2006), online: <http://blog.facebook.com/blog.php?post=2210227130>. ("You've heard it before, and you'll hear it again; here at Facebook, we want to help people understand their world. We started at one school, and realized over and over again that this site was useful to everyone—not just to Harvard students, not just to college students, not just to

(B) Facebook

Facebook is the world's largest social networking site.[45] Facebook is intended to "giv[e] people the power to share and make the world more open and connected."[46] Facebook collects and stores a considerable amount of information about its users. A fully completed Facebook profile contains over 40 pieces of personal information, including a full name, birthday, political and religious views, contact information, gender, sexual preference, relationship status, education, employment history and at least one photo.[47]

In 2008, the Canadian Internet Policy and Public Interest Clinic ("CIPPIC") filed a complaint with the OPC under PIPEDA concerning Facebook's privacy practices and policies.[48] In July 2009, the OPC released its findings and recommendations following an in-depth investigation of Facebook.[49] In August 2009, Facebook and the OPC announced that Facebook had agreed to make changes to the way it collects, stores and disseminates personal information in order to comply with some of the OPC's recommendations.[50]

The CIPPIC complaint alleged that Facebook had violated PIPEDA in twenty-two ways. In its initial response to the OPC, Facebook addressed four of the deficiencies identified in the CIPPIC complaint: the collection of a user's date of birth, default privacy settings, advertising,

---

students, not just to former students. We've kept growing to accommodate this fact. This includes your friends who graduated pre-Facebook (yes, there was such a time), your friends who don't have school or work email addresses, and your friends whose schools don't give out email addresses. Now you can all connect.")

45 See James Grimmelmann, "Saving Facebook*"* (2009) Iowa Law Review 1143 [Grimmelmann].

46 Facebook, "Homepage", online: Faceboook <http://www.facebook.com/facebook?ref=pf>.

47 Grimmelmann, *supra* note 45.

48 Canadian Internet Policy and Public Interest Clinic (CIPPIC), "PIPEDA Complaint: Facebook" (30 May 2008), online: CIPPIC <http://www.cippic.ca/uploads/CIPPICFacebookComplaint_29May08.pdf> [CIPPIC, "Complaint"].

49 Elizabeth Denham, Assistant Privacy Commissioner of Canada, *Report of findings into the complaint filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. under the Personal Information Protection and Electronic Documents Act* (16 July 2009) [Report].

50 See also "Facebook Announces Privacy Improvements in Response to Recommendations by Canadian Privacy Commissioner" (27 August 2009), online: Facebook <http://www.facebook.com/press/releases.php?p=118816>. Office of the Privacy Commission of Canada, "Facebook agrees to address privacy concerns" *News Release* (27 August 2009), online: OPC <www.priv.gc.ca/media/nr-c/2009/nr-c_090827_e.cfm> [News Release]; Elizabeth Denham, Assistant Privacy Commissioner of Canada, "Remarks at a Press Conference on the Facebook Investigation" (27 August 2009), online: <http://www.priv.gc.ca/speech/2009/sp-d_20090827_ed_e.cfm> [Remarks].

and monitoring of anomalous activity.[51] The corrective measures taken by Facebook in respect of these issues included improving the default security settings on a user's profile, better informing users of the circumstances under which their date of birth could be shared, and increasing the transparency about advertising.[52] In light of the measures taken by Facebook, the OPC held that CIPPIC's complaint about the above four issues was "well founded and resolved".[53]

Included in the above "well-founded and resolved" issues is one significant point worthy of note. The CIPPIC complaint included allegations that Facebook was engaged in inappropriate targeted marketing and advertising. This allegation raised the question of the distinction between collecting personal information for a primary purpose as opposed to a secondary marketing purpose. Advertising would in most other contexts be considered a secondary use of personal information, requiring at least an ability for individuals to opt out of that purpose. However, the OPC noted that the Facebook's business model necessitated advertising:

> In the past, when discussing marketing, the Office always drew a distinction between primary and secondary purposes. A primary purpose is that which is essential to the service. A secondary purpose is additional to that for which the information was needed in the first place. In our earlier cases regarding advertising, it was often considered to be a secondary purpose – one that users can opt out of in certain circumstances.
>
> Facebook has a different business model from organizations we have looked at to date. The site is free to users but not to Facebook, which needs the revenues from advertising in order to provide the service. From that perspective, advertising is essential to the provision of the service, and persons who wish to use the service must be willing to receive a certain amount of advertising.
>
> This complaint concerns two types of advertising that involve the use of personal information – one which the user must consent to in order to use the site (Facebook Ads) and one which a user can opt out of (Social Ads). As far as Facebook Ads are concerned, I am satisfied that the information Facebook gives to advertisers is in aggregate form and therefore Facebook does not disclose users'

[51] Report, *supra* note 49.

[52] *Ibid*.

[53] *Ibid*.

> personal information to advertisers. Nevertheless, there is no doubt that accessing users' attributes from their profiles, rendering the data into aggregate form, and serving ads to users constitute uses of personal information under the Act.
>
> Of the two types of targeted advertising at issue, I view Social Ads to be the more problematic because of their inherently intrusive nature. A Social Ad uses the individual's actions, thumbnail photo and name to promote a certain product or service. The ad then becomes part of the News Feed and intertwines itself in the regular interactions of the user and his or her friends. In effect, the Social Ad takes on the appearance of an endorsement of the product by the user. For this reason, users would not reasonably expect their information to be used in such a manner and they should, as is the current situation, be able to opt out of such an active use of their personal information.
>
> In contrast, Facebook Ads are far less invasive. Only the user can see the ads delivered to him or her and the user is not being co-opted into endorsing a product. We acknowledge that Facebook needs to have a means of generating revenue and most Facebook users reasonably expect to receive advertisements. In the circumstances of Facebook's ostensibly "free" social networking service, I find it reasonable that users are required to consent to Facebook Ads as a condition of service Facebook has a different business model from organizations we have looked at to date. The site is free to users but not to Facebook, which needs the revenues from advertising in order to provide the service. From that perspective, advertising is essential to the provision of the service, and persons who wish to use the service must be willing to receive a certain amount of advertising.[54]

The above finding may have significant ramifications for the wide variety of "free" online services beyond the Facebook case.[55] Indeed, much of the content on the internet is "free".

The remaining concerns raised in the CIPPIC complaint can be divided into four categories: (a) the use of personal information by third-party application developers, (b) the deletion and deactivation of Facebook accounts, (c) the protection of information about deceased users, and (d) the protection of personal information about non-Facebook users. These four

---

[54] *Ibid*. at para. 130-134.

[55] See generally FTC Commissioner Pamela Jones Harbour's Statement, "Regarding Staff Report: Self-Regulatory Principles For Online Behavioral Advertising", (February 2009), online: <http://www.ftc.gov/os/2009/02/P085400behavadharbour.pdf>.

issues were the focus of the OPC's findings and recommendations and are discussed in turn below.

(a) Third-party applications

In May 2007, Facebook changed its programming platform to allow third-party developers to create applications that could run inside Facebook.[56] Once a Facebook user had chosen to add a particular application to their profile, the third-party developers were given access to that user's personal information. CIPPIC complained that Facebook did not explain the purpose for supplying personal information to third-party application developers and that it provided third-party application developers with access to an excessive amount of personal information. [57]

The OPC found that providing access to users' information was unacceptable for a variety of reasons. In particular, the OPC focused on the issues of limiting the collection of information, obtaining consent for disclosure and safeguarding information. The OPC recommended that third-party developers be granted access to a limited amount of information required to run the application, that they be prevented from accessing other users' information, and that consent should be obtained from the user prior to the application being installed.[58]

Facebook agreed to retrofit its application platform in order to prevent an application from accessing users' information until it obtains express consent for the specific categories of information that it wishes to access. The changes were intended to permit users to control the categories of information that an application would be permitted to access and use.[59] Users' friends would be provided the option of blocking some or all applications from accessing their personal information as well.

(b) Deactivation and deletion

Facebook users can either 'deactivate' or delete their Facebook account. 'Deactivation' separates the Facebook profile from the active profiles that can be searched by other users.

---

[56] CIPPIC, "Complaint", *supra* note 48 at 17.

[57] *Ibid*. at 19.

[58] Report, *supra* note 49.

[59] News Release, *supra* note 49.

However, 'deactivation' does not delete an individuals' information. Instead, the information is stored on Facebook servers indefinitely so that users can reactivate their account in the future, if they choose to do so.[60] Facebook claimed that 50% of users that deactivate their accounts return to Facebook within a month of deactivation.[61] CIPPIC alleged that it was not clear whether users knew that their 'deactivated' accounts still existed in digital storage.[62] In reply to the OPC, Facebook agreed to notify users of the option to delete their profile during the deactivation process.[63] In addition, Facebook agreed to better explain the distinction between 'deactivation' and deletion in its privacy statements, and during the deactivation process.[64] Notwithstanding the changes above, the OPC did not expressly require Facebook to implement a retention policy: "While we asked for a retention policy, we looked at the issue again and considered what Facebook was proposing. We determined the company's approach to providing clarity and alleviating the confusion is acceptable. We were willing to reconsider our position…".[65]

(c) Information about deceased users

When Facebook is notified that an individual has passed away, it keeps the user's profile in a memorialized status for a period of time. However, that practice was not explained in Facebook's privacy policy and nor were individuals given the opportunity to opt out. The OPC concluded that the failure to advise users of this potential use of their information contravened PIPEDA but that users need not be given an opt out.[66] Facebook agreed to add an explanation of the memorialisation process in its privacy statement.[67]

(d) Information about non-users

Non-users have unique privacy concerns with Facebook because people who are not on Facebook, perhaps by choice, have not consented to Facebook's privacy policies and practices.

---

60 CIPPIC, "Complaint", *supra* note 48 at 19.

61 Report, *supra* note 49 at para. 236.

62 *Ibid*. at 19.

63 Office of the Privacy Commissioner of Canada, "Letter from the OPC to CIPPIC outlining its resolution with Facebook" (25 August 2009), online: OPC <www.priv.gc.ca/media/nr-c/2009/let_090827_e.cfm> [OPC, "Letter"]; News Release, *supra* note 59.

64 *Ibid*.

65 Remarks, *supra* note 50.

66 Report, *supra* note 49.

67 OPC, "Letter", *supra* note 63.

Yet, non-users' information can be seen on Facebook under a variety of circumstances. For example, the platform allows users to name or "tag" non-users in photos and videos, and add captions that reveal information about non-users (*e.g.* their name) to those with access to the user's profile.[68] In cases where the security settings of that user's profile are low, the non-user's information could be widely viewed without their knowledge or consent.

To address privacy concerns for non-users, Facebook prompted the user tagging non-users to provide the non-user's email address, which was designed to allow Facebook to inform the non-user that they have been "tagged" and to invite them to join Facebook. However, that practice also gave Facebook the ability to advertise to non-users and provided to Facebook information about non-users that it would not otherwise have.[69] In response to the OPC's concerns, Facebook agreed to add "appropriate language to its Statement of Rights and Responsibilities, to inform users of their obligations to obtain the consent of non-users before providing their email address to Facebook" and to refrain from retaining non-users' email addresses for any purpose.[70]

While the OPC investigation of Facebook was initially hailed as a victory for privacy, those that felt the findings did not go far enough were soon after vindicated when Facebook announced changes to its privacy practices in late 2009. Those changes ignited public outcry on privacy ground as discussed in Part II A.(b) below.

(C) Street-level imaging

Street-level imaging involves taking photographs of public places which are then used to create maps or for other purposes. Google Street View, the focus of this section, is the most well-known example of a service that involves street-level imaging. However, in addition to Google Street View, the OPC and the privacy commissioners in British Columbia, Alberta and Quebec have identified Canpages Street Scene and other applications for "geomatics, surveying,

---

[68] CIPPIC, "Complaint", *supra* note 48.

[69] *Ibid*. at 28-29.

[70] OPC, "Letter", *supra* note 58.

mapping and urban planning" as raising privacy concerns in connection with street-level imaging.[71]

Where photographs are collected for the purpose of creating graphical (*i.e.* not photographic) maps for use in GPS services, however, privacy issues are arguably confined to collection, use and retention because the images themselves are not published. On the other hand, Google Street View and Canpages Street Scene publish the actual photos taken, subject to certain privacy-protective modifications and practices as described herein. As a result, such services have unsurprisingly been the primary focus of attention of privacy authorities, including the OPC. The OPC first began monitoring issues related to street-level imaging in 2007 with a view to "ensuring that that [this technology] protects the privacy of Canadians by meeting the requirements of PIPEDA, such as knowledge, consent, safeguards, and retention."[72]

On October 7, 2009, Google launched Street View in Canada, effectively enabling citizens worldwide to "take a virtual walk through many neighbourhoods in Canada."[73] The application was an instant success – more than 28 million images of locations were viewed within a day of the application being launched in Canada.[74] Google describes Street View as

---

[71] Office of the Privacy Commissioner, "Captured on Camera Street-level imaging technology, the Internet and you" (7 April 2009), online: OPC <http://www.priv.gc.ca/fs-fi/02_05_d_39_prov_e.cfm> [OPC "Captured on Camera"] ("A number of companies have begun collecting images of public places in Canada, which may then be made available over the Internet or through other means. Individuals may be captured in these images, perhaps incidentally. One of the most widely known is Google's Street View application, which allows computer users to make "virtual visits" to cities such as Paris, London, New York and, eventually, major Canadian centres. Canpages is another company that provides street images on the Internet. Other applications have also been developed for fields such as geomatics, surveying, mapping and urban planning.").

[72] Office of the Privacy Commissioner of Canada, "Statement: Appearance Before the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) on the Privacy Implications of Camera Surveillance" (October 2009), online: OPC <http://priv.gc.ca/parl/2009/parl_20091022_ed_e.cfm> [OPC, "Statement"]; See also OPC, Maps, *supra* note 73. See also Office of the Privacy Commissioner, "Letter to Google Inc. regarding the company's proposed retention plan for images collected for its Street View application"(21 August 2009), online: OPC <www.priv.gc.ca/media/nr-c/2009/let_090821_e.cfm> [OPC, "Letter to Google"].

[73] Office of the Privacy Commissioner of Canada, "Remarks at the PIPA Conference – Privacy and the Changing World of Maps" (October 2009), online: OPC <http://www.priv.gc.ca/Speech/2009/sp-d_20091015_ed_e.cfm> [OPC, "Maps"].

[74] Sarah Schmidt, "Privacy not protected on Google Street View, MPs told" *National Post* (22 October 2009), online: National Post <http://www.nationalpost.com/story-printer.htmll?id=2133506> [Schmidt].

allowing users to "explore the world through images [...] provid[ing] 360° horizontal and 290° vertical panoramic street level views."[75]

In a conference address in October 2009, Elizabeth Denham, the Assistant Privacy Commissioner of Canada, stated that many of the images caught by street-level imaging fall within the definition of "personal information" in PIPEDA and are thus subject to the legislation.[76] Objects that are contained in such imaging will be considered "personal information" where the object has the ability to be connected to a specific individual – such as a vanity license plate.[77] As a result, the OPC took the position that PIPEDA required Google to obtain consent from individuals prior to collecting and/or displaying their personal information within Street View.[78]

(a) Response to Street View in Canada

As a consequence of the differing legal obligations arising under American and Canadian law, Google used a modified form of the application, distinct from the original form launched in the United States, when launching Street View in Canada.[79] The modified form of Street View was first used in Canada by Google in May 2008; it utilizes a sophisticated computer algorithm to search Google's database of images for faces and license plates which it blurs.[80] That blurring technology is cited by Google Canada as one of the measures that helps ensure that Google protects privacy in its Street View application.[81] The following is the full list of privacy measures identified on the Google Maps website with respect to the Street View application:

---

[75] Google Maps Canada, "Behind the Scenes", online: Google <http://maps.google.ca/intl/en_ca/help/maps/Street View/behind-the-scenes.html> [Google, "Behind the Scenes"].

[76] OPC, "Maps", *supra* note 73.

[77] *Ibid*.

[78] *Ibid*.

[79] Face-blurring technology was not used when Street View was first introduced in the United States, but Google began using the technology in Manhattan in 2008 and has since implemented the technology more broadly in other jurisdictions, including Canada, where the blurring technology is used in all Street View images.

[80] Steven Shankland, "Google begins blurring faces in Street View" *CNET* (13 May 2008), online: CNET <http://news.cnet.com/8301-10784_3-9943140-7.html>.

[81] Google Maps Canada, "Privacy", online: <http://maps.google.ca/intl/en_ca/help/maps/Street View/privacy.html> [Google Maps, "Privacy"].

> "Public Access Only" – images contained in Street View are "no different" than those which are visible to individuals driving or walking down streets;
>
> "Street View Images are not real time" – the images presented on Street View represent only a moment-in-time. The images on Street View are not current but rather range from being a few months to a few years old;
>
> "Individuals and license plates are blurred"; and,
>
> "You can request removal of an image" – the website includes a tool which allow users to request that images which contain content that is inappropriate or features an individual, their family, car or home, be removed.[82]

Notwithstanding the above positions and measures, the OPC has raised three privacy-related concerns regarding Street View.

- Blurring technology and take down policy

The OPC has pointed out that Street View's facial-blurring technology remains "imperfect", noting that, "[t]here have been many cases where individuals are still identifiable, even after the blurring process has been applied."[83] A further example of how the technology is imperfect is represented by occurrences of "false positives"; for instance, in some images on Street View it has been noted that the faces of KFC's Colonel Sanders or individuals contained in billboard advertisements are blurred.[84] Google has responded to such concerns by assuring the OPC that it will continue to improve its already highly sophisticated facial-blurring technology and by emphasizing the company's "industry-leading take-down policy".[85] The policy includes a promise by Google Canada to remove any image within 24 hours of receiving a complaint.[86] Moreover, the OPC has noted that Google has, "made a commitment to contact community

---

[82] *Ibid*.

[83] OPC, "Statement", *supra* note 72.

[84] Schmidt, *supra* note 74.

[85] OPC, "Letter to Google", *supra* note 39; Schmidt, *supra* note 37.

[86] Schmidt, *supra* note 74.

organizations – for example, umbrella groups representing women's shelters – prior to launching Street View in Canada to let them know the process for having images removed."[87]

- Notification

An additional concern raised by the OPC relates the issue of notification. The OPC has expressed the view that commercial enterprises engaged in street-level imaging should ensure that individuals are notified and are made aware of when images are going to be collected in their neighbourhoods so "they may adjust their plans accordingly".[88] While it does not appear that the OPC is fully satisfied with the notification procedures being utilized by companies using street-level imaging, such as Google and Canpages, the OPC has indicated that both companies have become increasingly compliant with the notification methods that the OPC has suggested.[89] The OPC has suggested that companies engaged in street-level imaging implement the following notification methods: (i) the companies' vehicles bearing cameras should be visibly marked; (ii) the companies should issue press releases and use media outlets and the internet to notify the public that they are collecting images; and, (iii) companies provide clear information about where individuals can go for further information about the street-level imagery.[90]

- Retention of images

In its fact sheet entitled, *Captured on Camera – Street-level imaging technology, the Internet and you*,[91] the OPC sets out the privacy protections that are of particular relevance to the issue of street-level imaging. One of these protections relates to the retention by Google of unblurred Street View images. The OPC noted that Google initially failed to provide a concrete timeline for retention of images.[92]

Google has since provided the OPC with a retention plan; the plan entails Google retaining images for "a maximum period of one year after publication, after which time the

---

87 OPC, "Maps", *supra* note 73.

88 *Ibid*; OPC, "Statement", *supra* note 72.

89 *Ibid*.

90 OPC, "Maps", *supra* note 72.

91 OPC, "Captured on Camera", *supra* note 71.

92 OPC, "Letter to Google", *supra* note 72. See Schedule 1 to PIPEDA which sets out ten principles that govern the collection, use and dissemination of personal information in Canada of the code - in particular, see principle 5 which refers to, "limit[ing] use, disclosure and retention".

images will be permanently blurred."[93] While the OPC has deemed Google's current retention plan as "reasonable", it has also expressed an interest in Google working to further reduce the retention period.[94]

(b) Street View as Art? Implications for privacy

It has been suggested that Google could respond to a formal complaint to its Street View application by contending that the images contained in Street View fall under the artistic purpose exception under PIPEDA[95]—namely, as stated at section 7(1), "[...] an organization may collect personal information without the knowledge or consent of the individual only if [...] the collection is solely for journalistic, artistic or literary purposes."[96] Whether this exception would effectively enable Street View to operate without the consent of the individuals whose personal information is displayed remains undecided. While the Assistant Privacy Commissioner of Canada has remarked that it is unlikely the exception would apply because Street View does not appear to be an "artistic endeavour", a Google representative has suggested that "precedent has been set that maps are considered to be a form of artistic expression."[97] Similarly, photographs are considered a creative work and worthy of protection under the *Copyright Act*.

(c) International responses to Street View

In the United States, where the Street View application has been active since 2007, Google has faced challenges on a number of fronts – including from private citizens and government officials. While private citizens have been unsuccessful in invasion of privacy claims in an attempt to thwart Street View from using their images[98], different facets of the American government have been more successful, including banning Google from publishing

---

93 OPC, "Letter to Google", *supra* note 72.

94 *Ibid*.

95 Schmidt, *supra* note 74.

96 *Supra* note 16.

97 Schmidt, *supra* note 74.

98 For an example of where a U.S. court has denied a claim of invasion of privacy related to Google's Street View see: *Boring et al v. Google Inc.*, (Ct. Of Appeal, Third Circuit - D.C. No. 08-cv-00694), available online: <http://www.ca3.uscourts.gov/opinarch/092350np.pdf>.

Street View images of U.S. military bases,[99] and delaying the publication of images in security-sensitive areas.[100]

In contrast to the United States' relatively hands-off legal stance towards Street View, European nations have generally reacted more strongly to the introduction of Street View. For example, the European Union has demanded that Google warn residents *via* the internet and local or national press prior to sending out cars to collect images for Street View and that Google retain original (unblurred) images for only 6 months after their creation.[101] Google has threatened to pull Street View out of the European Union as a result of those demands.[102] In May 2009, Google was temporarily prohibited from gathering Street View images in Greece until "it [provided] further guarantees about privacy."[103] Street View has also faced resistance in the UK where, in April 2009, residents of a small town demonstrated their opposition to Street View by binding together to create a human shield to block a Google car from collecting photographs for use on Street View.[104] Finally, privacy concerns have been raised in Japan where, among other steps, Google agreed to lower the height of its cameras to avoid looking over fences. Japan's Communications Ministry later concluded that Street View complied with Japanese privacy law if it blurred images.[105]

In addition to the OPC's work in the area of street-level imagery, Natural Resources Canada commissioned a survey in 2009 to gain a deeper understanding on where Canadians

---

[99] "Pentagon bans Google from mapping military bases" *Canadian Broadcasting Corporation* (6 March 2008), online: CBC < http://www.cbc.ca/world/story/2008/03/06/google-maps.html>.

[100] Chris Parry, "Google Street View camera-cars invade West Vancouver and Surrey: Send us our pics" *Vancouver Sun* (30 April 2009), online: Vancouver Sun <http://www.vancouversun.com/Google+Street+View+camera+cars+invade+West+Vancouver+Send+your+pics/1550512/story.html?id=1550512>.

[101] Aoife White, "EU Orders Google to Remove Street View Photos After 6 Months" *Huffington Post* (26 February 2010), online: Huffington Post <http://www.huffingtonpost.com/2010/02/26/google-privacy-woes-eu-or_n_478551.html>.

[102] Claudia Rach, "Google May drop Street View in EU if photo storage time is cut" Business Week (3 March 2010).

[103] Google Street View blacked out in Greece" *CNN* (13 May 2009), online: CNN <http://edition.cnn.com/2009/WORLD/europe/05/13/greece.google.street.view.blocked/index.html>.

[104] "Google Camera blocked by residents" *Herald Scotland* (3 April 2009), online: Herald Scotland <http://www.heraldscotland.com/google-camera-car-blocked-by-residents-1.906641>.

[105] The Hindu News Service, "Japan says "Ok" to Google's Street View Service," (23 June 2009).

stood in respect of street-level imaging and related practices.[106] The following passages from the Executive Summary of that report provide telling examples:

> Respondents are not comfortable with images of themselves taken in public being posted to the Internet without their permission regardless of whether steps are taken to hide their identity. Even if their entire image is blurred out, less than half of respondents (43%) indicated that they would be comfortable with images of themselves taken in public places being posted to the Internet without their permission. Very few respondents (10%) were comfortable with such images being posted without their permission if no steps were taken to protect their identity.
>
> Canadians views on whether street-view images of private residences such as those on Google™ Street-View™ should be allowed in Canada are divided. Just over one-quarter (28%) agreed that it should be allowed, while 36% were neutral on the subject, and 36% felt that it should not be allowed. It should be noted, however, that the timing of the fieldwork for this study does not reflect the impact of Google's street-view service going live in Canada as the vast majority of the fieldwork was conducted just prior the service being launched in 12 Canadian cities.[107]

II. WHAT'S NEXT?

The examples of XCP DRM, Facebook and Street View discussed above demonstrate that new online technologies, even those with offline components (*e.g.* audio CD's and street-mapping cars), can often come into conflict with and be answerable to privacy law and social norms about privacy. The examples in Part I are informative of the importance of knowledge and consent, explaining purposes, default settings (*e.g.* opt-in *vs.* opt-out) in products and services, and retention requirements. At the same time that the technologies can raise privacy questions, however, they can also be a part of the solutions (*e.g.* Street View's blurring technology and the use of Facebook by its users to organize opposition to Facebook's privacy changes).

---

[106] Phase 5 Consulting Group, "Research Related to Privacy and the Use of Geospatial Information" Report for Natural Resources Canada, November 2009, online: <http://epe.lac-bac.gc.ca/100/200/301/pwgsc-tpsgc/por-ef/natural_resources/2009/091-08/report.pdf>

[107] *Ibid.*

In the sections that follow, this paper takes a look ahead to the next wave of privacy issues raised by the introduction of a variety of new technologies. Hardly a day goes by without myriad developments in this field; at the best of times it is difficult to keep pace with all of the latest and emerging developments. The following sections provide some 'quick hits' regarding (a) social media, including Google Buzz, Facebook and location-based services, (b) cloud computing, (c) online tracking and advertising and (d) potential legislative developments, including PIPEDA, lawful access, copyright and *ECPA*. Following a brief review of the highlights in these areas, Part III of this paper brings together several key themes and concludes with a look ahead to future work and challenges.

(A) Social media

(a) Google Buzz

In February 2010, Google launched "Buzz", an application which encompasses various social media tools within Gmail[108], such as photo and video sharing and status updates. Approximately 150 million people use Gmail on a monthly basis.[109] Buzz quickly earned a place in the privacy spotlight largely on account of one of its features which automatically searched an individuals' Gmail account email contacts and published the names of the user's most frequently emailed contacts as "followers" on the user's widely available online profile.[110]

In Canada, while there has yet to be a formal complaint launched against Google, the OPC issued a news release in February 2010, soon after Buzz was launched, stating, "[w]e have seen a storm of protest and outrage over alleged privacy violations and [the] Office also has questions about how Google Buzz has met the requirements of privacy law in Canada."[111] The Canadian Broadcasting Corporation reported that "One user blogged about how Buzz automatically added her abusive ex-boyfriend as a follower and exposed her communications

---

[108] Jessica Guyunn, "Google aims to take on Facebook with new social feature called 'Buzz'" *Los Angeles Times* (9 February 2010), online: LA Times <http://latimesblogs.latimes.com/technology/2010/02/google-facebook-social-networking.html>.

[109] Andy Beal, "Google Buzz Launches 150+ Million User Social Network" The Marketing Pilgrim (9 February 2010), online: The Marketing Pilgrim <http://www.marketingpilgrim.com/2010/02/google-buzz-launches-150-million-user-social-network.html>.

[110] Office of the Privacy Commissioner, "Commissioner challenges Google Buzz over privacy concerns" (17 February 2010), online: OPC <www.priv.gc.ca/media/nr-c/2010/nr-c_100217_e.cfm> [OPC, "Google Buzz"].

[111] OPC, "Google Buzz", *supra* note 110.

with a current partner to him".[112] In a higher profile example of the kind of breach that Google Buzz's original default settings could cause, Wired magazine reported that:

> …White House head of internet policy Andrew McLaughlin's use of the Google Buzz service with its initial default settings revealed several Google employees among his regular e-mail correspondents. McLaughlin is Google's former head of global public policy, so on one level, it makes sense that he would stay in touch with Google. However, a group called Consumer Watchdog, which opposed McLaughlin's appointment in the first place, filed a Freedom Of Information Request with the government asking for all communication between McLaughlin and Google, and says it hopes to find out whether the tech behemoth wields undue influence over U.S. policy.[113]

In the U.S., the Electronic Privacy Information Centre (EPIC) filed a complaint on February 16, 2010 about Google Buzz with the Federal Trade Commission. The complaint filed by EPIC claimed that, Google's attempt "to convert the private, personal information of Gmail subscribers into public information for the company's social network service Google Buzz [...] violated user privacy expectations, diminished user privacy, [and] contradicted Google's own privacy policy [...]."[114]

A class action law suit brought by a Harvard Law Student alleges that Google Buzz breaches, "several federal laws, including the *Federal Electronic Communications Privacy Act*, the *Federal Computer Fraud and Abuse Act*, and the *Federal Stored Communications Act*, as

---

[112] Peter Nowak, "Privacy commissioner reviewing Google Buzz" CBC (16 February 2010), online: <http://www.cbc.ca/technology/story/2010/02/16/google-buzz-privacy.html#ixzz0kFZ9F7LE>.

[113] Eliot Van Buskirk, "Google Reminds Buzz Users About Privacy Vulnerability" Wired (5 April 2010), online: <http://www.wired.com/epicenter/2010/04/google-reminds-buzz-users-about-privacy-vulnerability/>.

[114] Electronic Privacy Information Centre, "In the matter of Google Buzz, Complaint, Request for Investigation, Injunction, and Other Relief" *Federal Trade Commission* (16 February 2009), online: EPIC <http://epic.org/privacy/ftc/googlebuzz/GoogleBuzz_Complaint.pdf>. Note: the Federal Trade Commission (FTC) responded to the complaint made by EPIC, but would not confirm or deny that the FTC had launched an investigation; EPIC proceeded to file supplemental materials with the FTC requesting an injunction, an investigation and other relief. See: <http://epic.org/privacy/ftc/googlebuzz/> for further information.

well as California common and statutory law."[115] Nearly a dozen members of Congress have asked the FTC to investigate the privacy concerns raised by Google Buzz.[116]

Google responded quickly to the onslaught of criticism. It made numerous adjustments to the application, including changing the "auto-follow" default to "auto-suggest". As a result, Buzz now prompts users with suggestions of which other users they might want to follow, instead of automatically following others by default.[117] However, the list of users being followed by an individual is still public by default, requiring users to opt out of that practice.[118]

More recently, on April 5, 2010, Google announced that it would be asking Buzz users to reconfirm their privacy settings when they log into Buzz.[119] This move is designed to better ensure that Buzz users are not under any misapprehension about what their privacy choices and settings are and that have the ability to modify their settings if they so choose. It has also been noted that as a result of the secure HTTPS connection used in Google Buzz, users of that service may in fact enjoy a higher level of privacy protection in Buzz as compared to Facebook and Twitter.[120]

(b) Facebook

As mentioned in the Introduction, Facebook announced changes and potential changes to its privacy policies and practices in December 2009 and March 2010. Each of these announcements has caused a privacy stir.

---

[115] "Harvard Law student brings class action lawsuit over Google Buzz" *Harvard Law Record* (22 February 2010), online: <http://www.hlrecord.org/news/harvard-law-student-brings-class-action-lawsuit-over-google-buzz-1.1165204>.

[116] BBC News, "Google rolls out privacy reset for Buzz social network" BBC (5 April 2010), online: <http://news.bbc.co.uk/2/hi/technology/8603155.stm>.

[117] Christina Warren, "Google Buzz gets some serious privacy tweaks" *Mashable: The Social Media Guide* (February 2009), online: <http://mashable.com/2010/02/13/google-buzz-changes/>.

[118] Nicholas Carlson, "Google Buzz Still Has Major Privacy Flaw" *The Business Insider* (12 February 2010), online: The Business Insider <http://www.businessinsider.com/googles-nice-improvements-to-buzz-dont-correct-major-privacy-flaw-2010-2>.

[119] Todd Jackson, "Confirm your Buzz settings" Google Gmail blog (5 April 2010), online: <http://gmailblog.blogspot.com/2010/04/confirm-your-buzz-settings.html>. See generally Tom Krazit, "Google Buzz users: Double-check your settings" cnet News (5 April 2010), online: <http://news.cnet.com/8301-30684_3-20001748-265.html>.

[120] Ryan Singel, "Google Will Ask Buzz's Early Adopters to Confirm Privacy Choices" Wired (22 February 2010), online: <http://www.wired.com/epicenter/2010/02/google-buzz-confirm/>.

In December 2009, EPIC and nine other organizations filed a complaint with the Federal Trade Commission (FTC) regarding changes to Facebook's privacy policies and practices.[121] Some of these changes allegedly involved making information available to "everyone" as the default privacy setting and removing the option of opting-out of providing personal information to third parties."[122] The OPC received a similar complaint and is currently investigating.[123] Facebook announced further potential changes to its privacy policies and practices on March 26, 2010, which included potential changes to increase the use of location data and information shared with third parties.[124] Facebook described the draft policy as follows:

> *Pre-Approved Third-Party Websites and Applications*. In order to provide you with useful social experiences off of Facebook, we occasionally need to provide General Information about you to pre-approved third party websites and applications that use Platform at the time you visit them (if you are still logged in to Facebook). Similarly, when one of your friends visits a pre-approved website or application, it will receive General Information about you so you and your friend can be connected on that website as well (if you also have an account with that website). In these cases we require these websites and applications to go through an approval process, and to enter into separate agreements designed to protect your privacy.[125]

One commentator described the potential impact of the above change as follows:

> Imagine visiting a website and finding that it already knows who you are, where you live, how old you are and who your Facebook friends are, without your ever having given it permission to access that information. If you're logged in to Facebook and visit some as yet unnamed 'pre-approved' sites around the web, those sites may

---

[121] Electronic Privacy Information Centre, "In the Matter of Facebook, Inc. Complaint, Request for Investigation, Injunction, and Other Relief" *Federal Trade Commission* (17 December 2009), online: EPIC <http://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf>.

[122] *Ibid*.

[123] *Supra*, note 8.

[124] Richter, *supra* note 9.

[125] Facebook Site Governance: Privacy Policy - 4. Information You Share With Third Parties (26 March 2010), online: <http://www.facebook.com/note.php?note_id=10150162289930301>.

> soon have default access to data about your Facebook account and friends ….[126]

As of April 8, 2010, there were 2,225 comments on the announcement posted on Facebook's blog.[127] Many comments are detailed and express disapproval with the direction that individuals perceived Facebook to be taking with the potential new changes. For example, one individual wrote:

> I object to these changes. I want the ability to decide which information I provide (including my picture) and which information that includes me (such as being tagged in a photo) and which information you aggregate about me (such as my list of friends) is made available to various audiences (such as no one, friends, friends or friends, and ... See Moreeveryone). These new changes not only do not provide this, they yet again obfuscate and remove my ability to control access to this information. I should be able to specify the default value for all new privacy options. For example, if I could set that to "friends", then any future privacy options would default to making that item visible to "friends". Opt-out is unacceptable.[128]

German consumer protection minister, Ilse Aigner, is reported to have levelled harsh criticism against Facebook's proposed changes, demanding that Facebook "revise the privacy policy without delay" and that Facebook not "allow personal data to be passed on to third parties for commercial purposes without users' consent"[129]

In addition to the debate regarding Facebook's privacy changes, it is important to note that Facebook has been a source of other privacy concerns, namely data breaches. Given the magnitude of Facebook's operations – claiming more than 400 million users as of February 2010[130] – any breach by Facebook can impact a large number of people. On March 31, 2010,

---

[126] " Marshall Kirkpatrick, "Facebook May Share User Data With External Sites Automatically", Read Write Web (26 March 2010), online: <http://www.readwriteweb.com/archives/facebook_may_share_user_data_with_external_sites_a.php>.

[127] *Ibid*.

[128] *Ibid*.

[129] Associated Press, "German minister criticizes Facebook on privacy" Globe and Mail (5 April 2010), online: <http://www.theglobeandmail.com/news/technology/german-minister-criticizes-facebook-on-privacy/article1523426/>.

[130] Mark Zuckerberg, "Six Years of Making Connections" (4 February 2010), online: <http://blog.facebook.com/blog.php?post=287542162130>.

during an update to the site's code, Facebook publicly exposed its members' private email addresses for a period of approximately 30 minutes.[131] That report came a month after some Facebook members began receiving personal messages from other members that were not intended for them.[132]

Despite the critiques of Facebook's privacy changes by its users,[133] regulatory authorities,[134] public interest groups[135] and the media[136], Facebook's popularity does not appear to be suffering. According to the web analytics firm Hitwise, Facebook recently surpassed Google as the website most frequently visited in the United States for an entire week.[137]

(c) Location based services

Some of the most popular social media services are launching location based services. Such services are bound to be one of the most significant privacy issues of the near future. The microblogging service Twitter has a new feature called "Tweet with your location". It is available to customers in the United States and uses geolocation.[138] The default setting is that tweets will not reveal the users' location. Users must opt-in to tag locations to their tweets. The feature can be turned off for future tweets and may be removed for prior tweets. However, removing location tags from prior tweets will not guarantee that the information will be removed

---

[131] Jennifer Van Grove, "Facebook Bug Exposes Users' Hidden E-mail Addresses" Mashable (31 March 2010), online: <http://mashable.com/2010/03/31/facebook-bug/>.

[132] Jennifer Valentino-DeVries, "Facebook Glitch Sends Wrong Messages" The Wall Street Journal (25 February 2010), online: <http://blogs.wsj.com/digits/2010/02/25/facebook-glitch-sends-messages-to-the-wrong-people/tab/article/>.

[133] See. *e.g.* user comments posted to Richter*, supra*, note 9.

[134] See *e.g. supra*, notes 8, 48 and 120.

[135] See *e.g.* Bankston, *supra* note 6 and EPIC, *supra*, note 115.

[136] See *e.g.* Jared Newman, "Facebook Mulls Privacy Changes, Causes More Outrage" *PCWorld* (29 March 2010), online: PCWorld <http://www.pcworld.com/article/192816/facebook_mulls_privacy_changes_causes_more_outrage.html>; Rob Pagoraro, "Facebook privacy changes would share user data with other sites" *The Washington Post* (29 March 2010), online: The Washington Post <http://voices.washingtonpost.com/fasterforward/2010/03/facebook_privacy_changes_would.html>.

[137] Caitlin O'Connor, "Facebook beats Google as the most visited site in the U.S." *Daily News* (17 March 2010), online: Daily News <http://www.nydailynews.com/money/2010/03/17/2010-03-17_facebook_beats_google_as_the_most_visited_site_in_the_us.html>.

[138] Twitter, "About the Tweet With Your Location Feature" (12 November 2009), online: <http://help.twitter.com/forums/10711/entries/78525-geotagging-on-twitter>.

from copies of the data in third-party applications or in external search results.[139] Facebook will also be launching a location-based feature in late April 2010 and have stated they will use a similar opting-in policy.[140] Google Latitude is a feature on Google Maps that allows users to see where other users are located.[141] The feature is opt-in and requires the user's approval to share their geolocation data in response to requests from other users.[142]

Users may choose to reveal their exact location (latitude and longitude) or be less specific by revealing only their city; however, if a user chooses to reveal only their city, their exact location will be calculated first in order to determine that information. Twitter retains information about users' exact locations for a period of six months.[143]

Geolocation features raise privacy issues that may not be apparent to users because once location data and history is published, it may effectively be impossible to delete or rescind. Location-based services may also give rise to privacy considerations because if a user's location is published then it may expose that individual to certain risks. In making this point, the website PleaseRobMe.com, took users' published location data from their Twitter feeds and presented "opportunities" to visitors to Please Rob Me when it appeared that a user was not at home.[144] The site has since stopped presenting such "opportunities", having raised awareness about over-sharing location-based information on social media sites.[145]

(B) Cloud computing

Cloud computing is an evolving paradigm, making a concrete definition of the concept difficult. The OPC describes cloud computing as: "[t]he provision of web-based services using hardware and software managed by third parties. The services, including online file storage,

---

[139] Emily Pinkerton, "How to Tweet with your Location" (4 March), online: Twitter Support <http://help.twitter.com/entries/122236>.

[140] Nick Bilton, "Facebook will allow users to share location" *The New York Times* (Mar. 9, 2010), online: The New York Times <http://bits.blogs.nytimes.com/2010/03/09/facebook-will-allow-users-to-share-location>.

[141] For information about Google latitude, see <http://www.google.com/intl/en_us/latitude/intro.html>.

[142] Google, "Google Latitude" (2010), online: Google Mobile: <http://www.google.com/intl/en_us/mobile/latitude>.

[143] Eddie, "About the Tweet With Your Location Feature" (12 November 2009), online: Twitter Support <http://help.twitter.com/entries/78525>.

[144] Brian Caulfield, ""Please Rob Me" Confirms Your Worst Privacy Fears" Forbes.com (17 February 2010), online: <http://blogs.forbes.com/velocity/2010/02/17/please-rob-me-confirms-your-worst-privacy-fears/>.

[145] *Ibid.*

social networking sites, webmail and online business applications, are generally located on remote computers."[146]

Cloud computing can provide the benefit of free or inexpensive access to powerful computer resources, without requiring businesses or individuals to purchase and maintain such resources or acquire specific knowledge themselves. However, cloud computing services have raised important privacy questions; privacy and data security have been characterized as "[p]erhaps the greatest concerns that customers face when using a cloud computing solution"[147]. For example, control can conceivably be lost over personal information stored in a cloud, including where it may be stored, who has access to it, and how it may be used, retained or disclosed. Data may be stored on computers located in different countries, where it is subject to local laws.[148]

On February 11, 2010, OPC announced upcoming consultations on privacy issues related to cloud computing practices. The intent of the consultation is to canvass a broad range of views from business, government, academics, consumer associations and civil society to give the OPC a comprehensive understanding of the potential privacy issues raised by cloud computing. The results will help shape new public education, outreach materials and the OPC's input into the next parliamentary review of PIPEDA.[149]

In the United States, the FTC's Office of International Affairs held a conference on March 16 and 17, 2010, entitled "Securing Personal Data in a Global Economy",[150] as part of a roundtable discussion series on the privacy challenges associated with 21st century technology. The focus involved a similar discussion regarding the privacy issues raised by cloud computing

---

[146] Office of the Privacy Commissioner of Canada, "News Release: Privacy Commissioner launches public consultations on privacy implications of cloud computing" (11 February 2010), online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/media/nr-c/2010/nr-c_100211_e.cfm>.

[147] Stuart Levi & Kelly Riedel, "Cloud Computing: Understanding the Business and Legal Issues" (March 2010) 2 Practical Law 34 at 40.

[148] OPC, *supra* note 146.

[149] *Ibid*.

[150] "FTC Announces Speakers for Conference on Securing Personal Data in the Global Economy" (9 March 2009), online: Federal Trade Commission <http://www.ftc.gov/opa/2009/03/personaldata.shtm>.

and whether enhanced regulation would be beneficial.[151] The OPC and the FTC are not alone in their examination of the privacy questions raised by cloud computing. The Council of Europe is currently examining the question as well.[152]

Most recently, on March 29, 2010, the OPC published a comprehensive paper on the privacy issues associated with cloud computing: *Reaching for the Cloud(s): Privacy Issues Related to Cloud Computing*.[153] This paper will provide a valuable focal point for the OPC consultations on the issue of cloud computing. *Reaching for the Clouds* adopts the following expanded definition and explanation of cloud computing:

> […] cloud computing includes such common activities as storing photos online (on sites such as flickr); storing videos online (at sites like YouTube); using online applications such as Google's Office suite, Facebook or Twitter; using webmail like gmail or hotmail; paying to store computer files online or even backing up files online using services such as Jungle Disk. […] [C]loud computing isn't "the wave of the future" as much as it is an increasingly common use of today. […]
>
> However cloud computing is engaged, the effect may be said to replicate the mainframe/terminal days of early computing – that is, the personal computer becomes in essence a "dumb terminal", a machine that interacts with a cloud-mainframe in order to store, retrieve, or manipulate data.[154]

In *Reaching for the Clouds*, the OPC summarizes the potential privacy concerns of cloud computing under nine headings: Jurisdiction, Creation of new data, Security, Data intrusions. Lawful access, Processing, Misuse of data, Data permanence and Data ownership. It must be acknowledged that many of the privacy considerations raised in *Reaching for the Clouds* (and raised by other privacy authorities considering cloud computing as mentioned above), and indeed the privacy issues in cloud computing in general, are not novel or unique to cloud computing.

---

[151] Stephanie Condon, "FTC Questions Cloud-Computing Security" *Cnet News* (17 March 2009), online: Cnet News <http://news.cnet.com/8301-13578_3-10198577-38.html>.

[152] Mark Ballard, "Cloud security weaknesses prompt call for global data protection law" *Computer Weekly* (29 March 2010), online: Computer Weekly <http://www.computerweekly.com/Articles/2010/03/26/240731/cloud-security-weaknesses-prompt-call-for-global-data-protection.htm>.

[153] OPC, "Reaching for the Cloud(s): Privacy Issues related to Cloud Computing" (29 March 2010), online: <http://www.priv.gc.ca/information/pub/cc_201003_e.cfm>.

[154] *Ibid.*

Like any relationship where personal information is entrusted by individuals or an organization to a third-party, privacy risks can arise due to the distance and lack of control between individuals and their data. While the nature or degree of risks may differ in some cloud computing services, the risks (*e.g.* security risks) can often be found in a variety of other relationships involving the collection, use and disclosure of personal information.

It is notable that *Reaching for the Clouds* acknowledges that organizations' use of cloud computing services will in some cases be considered an outsourcing situation and that the usual requirements under PIPEDA will apply.[155] Presumably, where a cloud computing service involves the storage or processing of information outside of Canada, then organizations would be required to give notice to affected individuals in accordance with OPC findings and guidelines regarding transborder data flows.[156] However, although it might appear that some forms of cloud computing are no different than a third-party outsourcing arrangement where a third-party processes data on behalf of an organization, and where contractual and other measures are used to provide protection to personal information, consider that:

> [i]n a traditional outsourcing relationship, vendors will typically segregate or partition servers for a particular customer, and a customer may even be able to impose certain physical and logical security requirements. The multi-tenancy nature of cloud computing typically prohibits this level of customization. Therefore, once data is transferred to the cloud, customers are forced to rely on the physical and information security of the vendor to protect their valuable information.[157]

It also goes without saying that an organization ought to confirm the geographic location of where its data will be processed or stored as part of a cloud computing solution. That inquiry is an essential requirement under PIPEDA because organizations are required to provide a comparable level of protection while personal information is processed outside of Canada.

---

[155] *Ibid.* ("An organization contemplating moving towards storage or processing using the cloud computing infrastructure of a third-party should be considered to be "outsourcing for processing" and accordingly needs to consider issues of security of the information (both from intrusion and in terms of backup and recovery), binding the cloud provider to privacy controls equal to those imposed on the organization as data controller, and must ensure that access and correction procedures are possible, and that deletion procedures are adequate and appropriate.")

[156] OPC, "Guidelines for Processing Personal Data Across Borders" (January 2009), online: <http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.cfm>.

[157] *Ibid.*

Analysing risk will involve a consideration of the political and legal systems in place that are relevant to the protection of personal information in the relevant jurisdiction. The U.S. *Patriot Act* is often raised as a potential concern. Accordingly, cloud computing providers may increasingly find that their customers will come to the table with specific demands about where their data can and cannot be processed or stored.[158] These and other questions will unquestionably be worked out over time; it is hoped that initiatives such as the OPC consultation will contribute to a deeper understanding of the issues.

(C) Online tracking and advertising

Online behavioural advertising involves tracking and analyzing an individual's online activity in order to provide customized, targeted advertisements. The practice stormed onto the privacy radar several years ago when it was learned that British Telecom had reportedly run secret trials of a behavioural advertising system offered by Phorm.[159] That announcement led to a widespread backlash against behavioural advertising and in particular resulted in the European Commission opening an infringement proceeding against the United Kingdom.[160] That proceeding is unresolved. In addition, the Crown Prosecution Service in the United Kingdom recently revealed that it is considering possible criminal charges against British Telecom regarding its use of Phorm.[161] However, in better news for Phorm, it was also very recently announced that Phorm had landed contracts with five ISPs in Brazil.[162] After reportedly losing 90% of its share value after the British Telecom controversy, Phorm's shares rose as much as 15% on the announcement of the Brazil contracts.[163]

Online behavioural advertising can raise a variety of privacy concerns, principally issues of knowledge and consent. A recent study revealed that two thirds of Americans take issue with

---

[158] Denise J. Deveau, "When It Comes to Data, Location Matters", E-Commerce News (April 8, 2010), online: <http://www.ecommercetimes.com/story/When-It-Comes-to-Data-Location-Matters-69718.html>.

[159] Chris Williams, "BT confesses lies over secret Phorm experiments" The Register (17 March 2008), online: <http://www.theregister.co.uk/2008/03/17/bt_phorm_lies/>.

[160] European Commission, "Telecoms: Commission launches case against UK over privacy and personal data protection" IP/09/570.

[161] Chris Williams, "BT could face criminal case over Phorm trials" The Register (25 February 2010), online: <http://www.theregister.co.uk/2010/02/25/bt_cps/>.

[162] Maija Palmer, "Phorm wins ad-tracking deals in Brazil" Financial Times (26 March 2010), online: <http://www.ft.com/cms/s/0/985ff078-38d5-11df-9998-00144feabdc0.html>.

[163] *Ibid.*

their online information being collected by advertisers.[164] The study indicated that the majority of those polled did not understand privacy agreements or current laws with respect to privacy and the use of online tracking.[165]

Others argue that online tracking allows consumers access to information about products they are more likely to want, that tracking is essential to provide free online content and that the more individuals are aware of how their information is used, the fewer concerns exist regarding its collection.[166] Indeed, as discussed above in Part I.(B) of this paper, recall that the practice of collecting, using and disclosing personal information for advertising purposes in order to provide individuals with 'free' services was approved by the OPC in the Facebook case. In other words, it may be reasonable in many cases to condition access to a service on individuals' consent to the collection, use and disclosure of their personal information for advertising purposes. On the other hand, a recent settlement entered into between Sears and the FTC – arising after Sears had tracked users' activities without adequate disclosure, including the collection of data regarding personal finances, prescription medications and offline activity – suggests that inappropriate online tracking and advertising practices can give rise to potential sanctions.[167]

(a) FTC and OPC Activities

In Canada, the OPC has initiated a consumer consultation and call for submissions regarding online tracking, profiling and targeting.[168] The aim of the consultation is to promote debate about the privacy impacts of these practices, determine Canadians' expectations regarding privacy protections in the area, shed light on industry practices, and contribute to the next PIPEDA review process.[169] The OPC's call for submissions follows publication of a comprehensive set of materials on deep packet inspection (DPI), on which some behavioural

---

[164] Stephanie Clifford, "Two-Thirds of Americans Object to Online Tracking" *The New York Times* (29 September 2009), online: The New York Times <http://www.nytimes.com/2009/09/30/business/media/30adco.html>.

[165] *Ibid*.

[166] *Ibid*.

[167] "Sears settles FTC claims regarding its online tracking software" (10 June 2009), online: Health IT Law Blog <http://www.healthitlawblog.com/2009/06/articles/sears-settles-ftc-claims-regarding-its-online-tracking-software/>.

[168] Office of the Privacy Commissioner of Canada, "Notice of Consultation and Call for Submissions: Understanding Online Tracking, Profiling and Targeting", (20 January 2010), online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/resource/consultations/notice-avis_e.cfm>.

[169] *Ibid*.

advertising is premised.[170] The OPC identified the privacy concerns with DPI as including the use of such technology for targeted marketing purposes:

> DPI technology raises privacy concerns because it can involve the inspection of information sent from one end user to another. In other words, DPI technology has the capability to look into the content of messages sent over the Internet – enabling third parties to draw inferences about users' personal lives, interests, purchasing habits and other activities.
>
> The technology has the potential to give ISPs and other organizations widespread access to vast amounts of personal information sent over the Internet for:
>
> • Targeted advertising based on users' behaviour while browsing the Internet:
>
> • Scanning network traffic for undesirable or unlawful content, such as unlicensed distribution of copyright material or dissemination of hateful or obscene materials;
>
> • Capturing and recording packets as part of surveillance for national security and other crime investigation purposes; and
>
> • Monitoring traffic to measure network performance, and plan for future facilities investments.[171]

Meanwhile in the United States, on February 12, 2009, the FTC staff issued a report, "Self Regulatory Principles for Online Behavioural Advertising", providing guidance to the industry in the United States.[172] FTC Commissioner Jon Leibowitz commented: "this could be the last clear chance to show that self-regulation can – and will – effectively protect consumers' privacy in a dynamic online marketplace."[173] The FTC report states that privacy protections should cover any data that reasonably can be associated with a particular consumer or computer or other device. However, the report states that fewer privacy concerns are associated with websites that collect information but do not pass it along to third parties and with websites that

---

[170] OPC, "What is Deep Packet Inspection?", online: <http://dpi.priv.gc.ca/index.php/what-is-deep-packet-inspection/>.

[171] *Ibid.*

[172] Federal Trade Commission, "FTC Staff Revises Online Behavioral Advertising Principles" (12 February 2009), online: Federal Trade Commission <http://www.ftc.gov/opa/2009/02/behavad.shtm>.

[173] *Ibid.*

target advertisements based only on the page being viewed or search queries made.[174] Creative and effective disclosure mechanisms are encouraged to combat long confusing privacy policies or information collection outside the website context. Additional suggestions include retaining data only as long as is required for business purposes or law enforcement need and obtaining affirmative express consent for sensitive data such as financial, health, social security number information or information about children.[175]

More recently, on April 8, 2010, three privacy groups in the United States filed a complaint with the FTC against Microsoft, Google, Yahoo, and others regarding "Real-time Targeting and Auctioning, Data Profiling Optimization, and Economic Loss to Consumers and Privacy."[176] The complaint is revealing of aspects of the online profiling and behavioural advertising industry and is principally addressed at real-time advertising practices. AppNexus, a platform for advertisers to use Internet ad exchanges quoted in the complaint, explains the practice as follows: "Internet ad exchanges… basically markets for eyeballs on the Web. Advertisers bid against each other in real time for the ability to direct a message at a single Web surfer. The trades take 50 milliseconds to complete."[177] On March 11, 2010, the New York Times ran a story on AppNexus that described the real-time bidding practice as follows:

> Now, companies like Google, Yahoo and Microsoft let advertisers buy ads in the milliseconds between the time someone enters a site's Web address and the moment the page appears. The technology, called real-time bidding, allows advertisers to examine site visitors one by one and bid to serve them ads almost instantly.
>
> For example, say a man just searched for golf clubs on eBay (which has been testing a system from a company called AppNexus for more than a year). EBay can essentially follow that person's activities in real time, deciding when and where to show him near-personalized ads for golf clubs throughout the Web.

---

[174] *Ibid*.

[175] *Ibid*.

[176] Center for Digital Democracy, U.S. Public Interest Research Group, World Privacy Forum, Complaint, Request for Investigation, Injunction, and Other Relief, "Real-timeTargeting and Auctioning, Data Profiling Optimization, and Economic Loss to Consumers and Privacy" (April 8, 2010), online: <http://www.uspirg.org/uploads/eb/6c/eb6c038a1fb114be75ecabab05b4b90b/FTCfiling_Apr7_10.pdf>.

[177] *Ibid*.

> If eBay finds out that he bought a driver at another site, it can update the ad immediately to start showing him tees, golf balls or a package vacation to St. Andrew's, Scotland, often called the home of golf. If a woman was shopping, eBay could change the ad's color or presentation.[178]

Among other remedies, the complainants request that the FTC require behavioural advertising companies to require that individuals opt-in to such systems.

The experience in the United States, including the FTC report above, may inform the debate in Canada. In particular, the suggestion that organizations ought to consider creative disclosure mechanisms in place of complex privacy policies may be an area for further consideration in Canada. However, it must be acknowledged that Canada, unlike the United States, has a comprehensive data protection law in PIPEDA. As such, many practices in the area of online tracking and advertising would already come under the purview of PIPEDA and the OPC. It may be the case that the United States could learn more about privacy regulation from Canada than the reverse. Further, PIPEDA is not the only source of potential privacy protection in this area, as described in the next section.

(b) CRTC internet traffic management policy

On October 21, 2009, the Canadian Radiotelevision and Telecommunications Commission (CRTC) issued its 'net neutrality' policy, designed to govern the ability of ISPs to manage internet traffic. The policy imposes "a higher standard than that available under PIPEDA in order to provide a higher degree of privacy protection for customers of telecommunications services."[179]

CRTC Policy 2009-657 principally addresses the use of Internet Traffic Management Practices (ITMPs) by ISPs. The CRTC described its objective in the policy as one of balancing "the freedom of Canadians to use the Internet for various purposes with the legitimate interests

---

[178] Stephanie Clifford, "Instant Ads Set the Pace on the Web" *New York Times* (March 11, 2010), online: <http://www.nytimes.com/2010/03/12/business/media/12adco.html>.

[179] Canadian Radio and Telecommunications Commission (CRTC) *Review of the Internet Traffic Management Practices of Internet Service Providers*, Telecom Public Notice 2008-19, October 21, 2009 at para. 102.

of ISPs to manage the traffic thus generated on their networks, consistent with legislation, including privacy legislation."[180]

In response to the privacy concerns raised in a public consultation process, the CRTC directed "all primary ISPs, as a condition of providing retail Internet services, not to use for other purposes personal information collected for the purposes of traffic management and not to disclose such information."[181] Under the policy, primary ISPs are also required "to include, in their service contracts or other arrangements with secondary ISPs, the requirement that the latter not use for other purposes personal information collected for the purposes of traffic management and not disclose such information."[182]

Since the current stated practice of ISPs is to use aggregate (*i.e.* non-personal) information for ITMP, the privacy protection in the policy may not impact ISPs' current practices. Under the policy, ISPs may continue to use aggregate information to manage traffic on their networks.

The CRTC policy may close the door, at least for the time being, on behavioural advertising practices that rely upon the use and disclosure of personal information collected by ISPs for ITMP purposes. Nevertheless, it is arguable that the decision may leave open the use and disclosure of personal information for behavioural advertising purposes where personal information is not collected solely or primarily for the purpose of traffic management.

(D) Legislative developments

Given the plethora of new technologies, products and services that can raise potential privacy questions it is not surprising that governments have responded with legislation and regulatory activity in kind. A number of initiatives have already been mentioned herein and it was noted earlier that PIPEDA itself was enacted in response to the increasing tension between

---

[180] *Ibid.* at para. 7. It is also notable that the United States Federal Communications Commission's National Broadband Plan, designed to ensure that every American has access to broadband capability, includes comments on privacy concerns associated with widespread access to broadband. These concerns include issues such as the lack of transparency regarding how information is used once it is provided online and the lack of an established method of regaining control over data.

[181] *Ibid.* at para. 103.

[182] *Ibid.* at para. 104.

privacy and technology. The following section briefly sketches potential legislative developments under PIPEDA, lawful access, and copyright reform. That section is followed by a more detailed discussion of *ECPA*[183], which is widely expected to be re-introduced and passed into law in Canada in the form it was in before Parliament was prorogued in late 2009.

(a) PIPEDA, lawful access and copyright reform

There are a variety of current and potential legislative developments in Canada that may touch on many of the privacy issues discussed in this paper. For example, there is the obvious question of PIPEDA reform. Although PIPEDA review process produced a series of recommendations by the Standing Committee on Access to Information, Privacy and Ethics[184], responses by the government[185], and additional consultations and other activities[186], it has not yet resulted in legislative amendment to PIPEDA. Nor would any of the areas of potential amendment, perhaps with the exception of children's privacy issues, likely have any direct effect on the privacy issues discussed herein. Indeed, as mentioned above, one of the stated objectives of the OPC's recent consultations regarding cloud computing and online tracking and advertising is to inform the OPC's input into the *next* round of PIPEDA review.

There is also the question of lawful access legislation, which would arguably have one of the most significant impacts on online privacy of any other single legislative initiative. For example, the now defunct Bill C-47, the *Technical Assistance for Law Enforcement in the 21st Century Act* would have required telecommunications service providers to have the capability to intercept communications made using their networks and to grant law enforcement agencies access to certain subscriber information without a warrant or court order.[187]

---

[183] *ECPA, supra* note 17.

[184] Standing Committee on Access to Information, Privacy and Ethics, Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics, May 2007, online: http://cmte.parl.gc.ca/Content/HOC/committee/391/ethi/reports/rp2891060/ethirp04/ethirp04-e.pdf

[185] Government Response to the Fourth Report of the Standing Committee on Access to Information Privacy and Ethics, http://www.ic.gc.ca/eic/site/ic1.nsf/eng/h_02861.html

[186] *Ibid.* See also Canadian Bar Association, National Privacy and Access Law Section, "Personal Information Protection and Electronic Documents Act" (January 2008), online: <http://www.cba.org/CBA/submissions/pdf/08-06-eng.pdf>.

[187] Dominique Valiquet, Legal and Legislative Affairs Division, Bill C-47: Technical Assistance for Law Enforcement in the 21st Century Act, July 28, 2009, online: <http://www2.parl.gc.ca/Sites/LOP/LegislativeSummaries/Bills_ls.asp?lang=E&ls=c47&source=library_prb&Parl=40&Ses=2>.

It seems virtually certain that Bill C-47 and its companion, Bill C-46, the *Investigative Powers for the 21st Century Act* will be re-introduced in one form or another in Canada. However, if and when they are tabled again, they will be subject to intense scrutiny by privacy and civil liberties groups and by the OPC. On October 27, 2009, for example, the OPC wrote to the Standing Committee on Public Safety and National Security to offer preliminary views on the proposed legislation, which in the OPC's view raised "significant privacy concerns"[188]. The OPC concluded by urging Parliament to review the bills in light of the following questions:

> In specific terms, how is the current regime of judicial authorization not meeting the needs of law enforcement and national security authorities in relation to the Internet?
>
> What law enforcement or national security duty justifies access without a warrant by authorities to personal information or preservation of private communication?
>
> Why are some of these powers unrestricted, when the spirit of Canadian law clearly reflects the view that access or seizure without court authorization should be exceptional?
>
> And finally, are the mechanisms for accountability commensurate to the unprecedented powers envisaged?[189]

It remains to be seen how these and other fundamental questions may be addressed by Parliament and law enforcement proponents of the bills. Given the impact of the legislation on ISPs, it is also expected that they may have further input into the content of any future lawful access bill.

In addition to the examples above, there is also the possibility of a new copyright reform bill in Canada which will raise privacy considerations, as past bills have done.[190] As mentioned earlier in this paper, privacy questions arise in respect of any protections that our *Copyright*

---

[188] OPC, Letter regarding the Commissioner's initial analysis on the privacy implications of Bills C-46 and C-47, October 27, 2009, online: <http://www.priv.gc.ca/parl/2009/let_091027_e.cfm>.

[189] *Ibid*.

[190] Bill C-60, *An Act to amend the Copyright Act*, 1st Sess., 38th Parl., 2005l; Bill C-61, *An Act to amend the Copyright Act*, 2nd Sess., 39th Parl., 2008. As a result of intervening elections in Canada, neither Bill C60 nor Bill C-61 were passed into law. Canadians were divided in support for the proposed laws. See e.g. Angus Reid Strategies, Press Release, "Canadians Evenly Split on Proposed Amendments to Copyright Act" (June 19, 2008) (poll finding 45% of Canadians in favour of Bill C-61 and 45% against the bill); Peter Nowak, "Copyright law could result in police state: critics" CBC News (June 12, 2008), online: CBC <http://www.cbc.ca/technology/story/2008/06/12/tech-copyright.html>

Act[191] may provide for components of DRM technologies. It has been suggested, for example, that any amendments to the *Copyright Act* that would protect components of DRM should include privacy-protective provisions that permit individuals to circumvent DRM to protect their privacy.[192] Potential ISP liability provisions in the *Copyright Act* also raise privacy questions. ISP liability provisions typically spell out the responsibilities of ISPs to take action in respect of alleged copyright infringement and liabilities for failing to take action.[193]

Under a 'notice-and-notice' system, copyright holders can issue notices to be sent by ISPs to subscribers who are alleged to have committed copyright infringement.[194] ISPs may also be required to retain identifying information about individuals that are sent such notices, perhaps for a limited time period. If the copyright holder commences a lawsuit within the allotted time, then the ISP would have to retain the identity data for a longer period.

Under a notice-and-notice system, privacy issues can arise in respect of the nature of information retained by ISPs and the scope, duration, and purposes of retention and disclosure. For example, the OPC has expressed concern about the impact that ISP liability provisions can have on individuals' privacy interests, noting that a 'notice-and-notice' provision previously proposed in Canada raised important privacy concerns:

> Allowing a private sector organization to require an ISP to retain personal information is a precedent-setting provision that would seriously weaken privacy protections. When this provision was proposed in a previous proposal to amend the legislation it did not include any threshold that had to be met before the notice could be issued, nor did it provide any means for the ISP to contest the demand to retain the data. The extended retention periods create additional privacy concerns. PIPEDA requires that organizations

---

[191] R.S., 1985, c. C-42.

[192] Ian Kerr "If Left to their own Devices: How DRM and Anti-circumvention Laws Can Be Used to Hack Privacy", in Michael Geist, ed., *In the Public Interest: The Future of Canadian Copyright Law* (Toronto: Irwin Law, 2005).

[193] For a discussion of the liability of ISPs in the European Union, see van der Net "Civil Liability of Internet providers following the Directive on Electronic Commerce" in H. Snijders and S. Weatherill, *Ecommerce Law* (Hague: Kluwer, 2003) at 53. See also, EC, *Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society*, [2001] O.J. L. 167/10 at Article 5(1), online: Europa <http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_167/l_16720010622en00100019.pdf>.

[194] A 'notice and notice' system was proposed first in Bill C-60 and then again in Bill C-61. Each of the elements of a 'notice and notice' system described in this paragraph reflect elements of the proposal in Bill C-61.

> retain personal information for only as long as necessary to fulfill the purposes for which the information was originally collected. Limiting the extent of data collection and period of retention is a key strategy to minimize the risk of data breaches of personal information.[195]

Other forms of ISP liability provisions include 'notice-and-takedown' and 'notice-and-termination' provisions. Extra-judicial copyright enforcement regimes such as 'notice-and-takedown' and 'notice-and-termination', if adopted, could conflict with individuals' privacy interests in obvious ways, particularly if ISPs are required to retain data about their customers in respect of such notices.[196] Among other impacts, an effective notice and termination regime, for example, would presumably involve linking an individual's identity and subscriber information to a notice and termination history so that the same individual could not re-apply for ISP service with the same ISP. It is also conceivable that ISPs might be required to share such information with one another in order to avoid customers that had been terminated under the law by another ISP.

(b) *Electronic Commerce Protection Act*[197]

The history of *ECPA* can be traced to a process that began in 2004, with the creation of the Anti-Spam Action Plan for Canada, a private-sector task force chaired by Industry Canada to examine the issue of unsolicited commercial email. The task force issued a report that made a number of recommendations, including the creation of legislation that would address spam.

On April 24, 2009, the Honourable Tony Clement, Canada's Minister of Industry, introduced Bill C-27, the *Electronic Commerce Protection Act* ("*ECPA*"). *ECPA* addresses 'spam' and a number of related issues. *ECPA* identified its purpose as "promoting the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities."[198]

---

[195] Letter from Jennifer Stoddart, Privacy Commissioner of Canada, to Ministers Prentice and Verner (18 January 2008), online: OPC <http://www.privcom.gc.ca/parl/2008/let_080118_e.asp> [OPC, "January 2008 Letter"].

[196] See generally Electronic Frontier Foundation, "Unsafe Harbors: Abusive DMCA Subpoenas and Takedown Demands", (September 2003), online: EFF <http://www.eff.org/wp/unsafe-harbors-abusive-dmca-subpeonas-and-takedown-demands>; OPC, "January 2008 Letter", *ibid.*

[197] Bill C-27, *supra* note 17. This section is a revised and updated version of material derived from Alex Cameron & Sarah Turney, "Proposed regulation of commercial e-messages" (2009) 11 E-commerce Law & Policy 14.

[198] Bill C-27, *ibid.*

If re-introduced and passed into law, *ECPA* will amend four existing laws that deal with telecommunications, competition and privacy: the *Canadian Radio-television and Telecommunications Commission (CRTC) Act*[199], the *Competition Act*[200], PIPEDA, and the *Telecommunications Act*[201]. Included in the potential amendments are provisions that designate the *CRTC* as the primary authority responsible for administering and enforcing *ECPA* and that give new enforcement powers to both the OPC and Commissioner of Competition, within their respective mandates.

ECPA confers substantial investigation and production powers on the *CRTC*, along with the authority to levy considerable administrative penalties. *ECPA* also establishes a set of relatively broad definitions that appear to give the agencies identified by the legislation considerable scope for their authority. For example, the term "electronic address" has been defined to encompass email, instant messaging, text messages and messages on "any similar account," which could include those sent over Facebook, MySpace and Twitter.[202] The term "electronic message" is also quite broad, encompassing not just email, text messaging, and sounds, but also more traditional forms of communication including fax messages.

At the heart of the legislation is a consent requirement. *ECPA* requires that individuals must 'opt-in' to receive commercial electronic messages by expressly giving their consent and be allowed to 'opt-out' if they wish to withdraw that consent. Sending commercial electronic messages without consent is prohibited under *ECPA*. The consent provisions are intended to be used to prevent both spamming, and phishing (where the author of the message is disguised in an attempt to elicit information from the recipient), as well as other forms of unsolicited electronic contact. *ECPA* also outlines circumstances under which consent may be implied, including circumstances where there is an existing relationship between the sender and recipient, including a past business relationship. Finally, *ECPA* lays the groundwork to replace Canada's

[199] R.S.C. 1985, c. C-22.
[200] R.S.C. 1985, c. C-34.
[201] S.C. 1993, c. 38.
[202] *Ibid*.

controversial "do-not-call list" for telephone marketing with the 'opt-in' consent framework of *ECPA*.[203]

The main prohibitions of *ECPA* are laid out in clauses 6 – 9. Clause 6 makes spamming a violation. It also requires that any commercial electronic message that meets *ECPA*'s consent requirements be sent in a prescribed form that includes information about the author of the message, their reason for sending it and how to unsubscribe. Clause 7 addresses electronic security concerns, including certain types of "hacking" operations and prohibits any attempt to alter transmission data. Clause 8 prohibits the installation of computer programs without consent. Clause 9 prohibits the causing or procurement of any of the prohibited activities.

ECPA imposes significant monetary penalties for violations of clauses 6 – 9, and outlines a list of factors to be considered when determining the amount to be levied in any particular case. The factors include the nature and scope of the violation, any history of previous offences, ability to pay, any financial benefit obtained from the violation and any other relevant factors. The maximum penalty for an individual is $1,000,000, with the maximum for a corporation being $10,000,000. These fines are imposed per violation, and a violation is defined as being separate for each day that it continues. While violations of *ECPA* are not criminal offences, they do provide for direct and vicarious liability and allow for the possibility of holding directors and officers responsible for the actions of a corporation. In addition to the administrative remedies, *ECPA* creates a private right of action for individuals.

ECPA has generated significant discussion and controversy in Canada.[204] Critics of *ECPA* suggest that the proposed law casts its net too wide in targeting all commercial electronic messages. It has also been suggested that the exceptions defined in *ECPA* are either too narrow

---

[203] While clause 6(7) of the ECPA, dealing with "spamming", exempts the two-way voice communication usually used by telemarketers, clause 64 provides for the repeal of that exemption, indicating that while the do-not-call list may be exempt from the ECPA in the early stages of the act's implementation, the government may intend to eliminate that exception at a later date. See Michael Geist, "Government Quietly Lays Groundwork For Overhaul of Do-Not-Call-List" (27 April 2009) online: <http://www.michaelgeist.ca/index2.php?option=com_content&do_pdf= 1&id=3897&task=view>.

[204] See *e.g.* James Gannon, "Really Setting the Record Straight on the ECPA: A Reply to Professor Michael Geist's Article "The Copyright Lobby's Secret Pressure On the Anti-Spam Bill" (October 17, 2009), online: IP, Innovation and Culture <http://innovationandculture.wordpress.com/2009/10/17/really-setting-the-record-straight-on-the-ecpa-a-reply-to-professor-michael-geistSee also Canadian Bar Association, National Privacy and Access Law Section, Letter to House of Commons Committee on Industry, Science and Technology, (September 15, 2009), online: <www.cba.org/CBA/submissions/pdf/09-51-eng.pdf>.

or too vague, with the unintended consequence that legitimate business communication may be impaired. Rather than a blanket prohibition approach to electronic communications, critics would prefer to see *ECPA* only specifically target conduct that harms e-commerce, such as the use of email to spread malware, particularly in light of the significant monetary penalties that can be imposed under *ECPA*.

On the other hand, supporters of *ECPA* point out that many organizations that send electronic messages already obtain individuals' consent to do so under Canadian privacy law and that, in any event, the exceptions in *ECPA* are sufficiently broad that they will not impair legitimate e-commerce.[205] Similar tensions have arisen in respect of *ECPA* provisions that address the installation of computer programs.

III. PRIVACY IS DEAD. LONG LIVE PRIVACY.

> All predictions are wrong, that's one of the few certainties granted to mankind. But though predictions may be wrong, they are right about the people who voice them, not about their future but about their experience of the present moment.[206]

As suggested in the Introduction to this paper and as has hopefully been reflected in many of the examples discussed herein, individuals care very deeply about privacy notwithstanding that many may share more personal information with more people than they have ever done in the past. There are certainly more ways of sharing and publishing information about one-self today than at any other time in human history. While the law often plays catch-up when it comes to the privacy impacts of new and emerging technologies, much is being done through enforcement and potential 'upgrading' of existing laws, and through the introduction of new laws. Individuals themselves are also increasingly effective at using new technologies to inform organizations about their privacy expectations, particularly when those expectations are

---

[205] Michael Geist, Testimony before the Standing Committee on Industry, Science and Technology, June 11, 2009, online: Parliament of Canada <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=3987885&Language=E&Mode=1&Parl=40&Ses=2> ("Members of this committee have noted that this is broad legislation that extends beyond just spam. I'd like to submit that this is a feature, not a bug. With much talk of the need for a national digital strategy, I think Bill C-27 fits nicely within that framework, providing much-needed consumer protection for electronic commerce. It's fair to say that the spam task force members recognize the need to address the broader issues towards the end of our mandate and that the steps in this bill are consistent with our recommendations. […] While the legislation is broad, it's important to emphasize that the exceptions are broad as well.")

[206] Milan Kundera, *Ignorance*, trans. by Linda Asher (New York: Perennial, 2002) at 13.

not met.[207] This Part reflects on several key questions and themes raised by the examples discussed in the earlier sections and concludes with a look to future work and challenges in the area.

(A) Organizations' use of social media

As social media services increase in popularity, both individuals and organizations have more at stake in the way that such services address the collection, use and disclosure of personal information. For organizations, social media services have become increasingly attractive as vehicles to gather information about and to reach large numbers of individuals efficiently and at minimal cost.[208] However, the potential impact of the standard terms of service, privacy policy and other rules of the applicable service is often overlooked in organizations' use of social media services.

Such rules can both delineate the scope of an organization's permissible collection, use and disclosure of personal information and at the same time inform the consent that individuals may be said to have given for the collection, use or disclosure of their personal information by third-parties through the service. In addition to the usual legal rules that govern an organization's privacy practices, organizations must increasingly consider whether terms of service, privacy policies and other rules used by social media providers may also govern their activities. Such provisions can add a significant layer of complexity and potential risk for organizations.[209] Specifically, organizations may need to consider (i) whether user agreements and privacy policies written by the service provider comply with applicable privacy laws and (ii) whether the organizations' actions are in compliance with the provider's user agreements and privacy policies and with relevant privacy legislation.

---

[207] See *e.g. supra* note 15.

[208] Mark S. Melodia, Paul Bond and Amy S. Mushahwar, "Data Privacy & Security" in *Network Interference: A Legal Guide to the Commercial Risks and Rewards of the social media Phenomenon*, online: ReedSmith <http://www.reedsmith.com/library/search_library.cfm?FaArea1=CustomWidgets.content_view_1&cit_id=26419> at p. 18.

[209] It goes without saying that this dynamic can also make it difficult for individuals to determine which privacy rules – those of the social media provider or those of the third-party – are applicable in respect of certain information or activities.

For example, organizations ought to consider whether a social media site is granting access to more information than is reasonably needed. A study of Facebook applications in 2008 suggested that third-parties had access to far more information than needed for their purposes:

> We found that applications generally do not need the extensive personal information that is available to them. Although two-thirds of applications depend on public friend data, far fewer require access to private data. Public data refers to information used publicly for identification or searching.
>
> […] Only 14 applications require any private data, meaning that over 90% of applications have unnecessary access to private data. Of the 14 applications that use private data, four clearly violate the Facebook Terms of Service: they pull user data and add it to an in-application profile, making it visible to other application users who would not otherwise have the ability to view it.[210]

An organization collecting personal information through Facebook might argue that Facebook is accountable for the amount of user information that is provided to the organization and that Facebook users have consented to such disclosures so long as they are made in compliance with the terms of service and other rules governing the Facebook platform. However, it is important to note that an organization may be held accountable for *inter alia* collecting too much information, despite compliance with Facebook's rules, and that Facebook may also be held accountable for *inter alia* disclosing too much information. Organizations using social media services should not expect that mere compliance with a social media provider's terms of service and privacy policy will alleviate the need to consider privacy legal requirements. In other words, organizations should not rely on the social media provider to effectively address the organization's own privacy compliance.

Organizations also need to consider their contractual obligations to social media providers. Terms of service can impose different obligations on an organization than the obligations that may apply under privacy laws. For example, Facebook's Statement of Rights and Responsibilities (the "Statement"), last updated December 21, 2009, states *inter alia* that any organization that creates a "Page" on Facebook is subject to certain privacy restrictions: "If you

---

[210] Adrienne Felt & David Evans, "Privacy Protection for Social Networking Platforms", Paper presented to Web 2.0 Security and Privacy 2008 in conjunction with 2008 IEEE Symposium on Security and Privacy. Oakland, CA. 22 May 2008.

collect user information on your Page, Section 9 of this Statement also applies to you."[211] Section 9 provides as follows in pertinent part:

> 2. Your access to and use of data you receive from Facebook, will be limited as follows:
>
> 1. You will only request data you need to operate your application.
> 2. You will only use the data you receive for your application, and will only use it in connection with Facebook.
> 3. You will have a privacy policy or otherwise make it clear to users what user data you are going to use and how you will use, display, or share that data.
> 4. You will not use, display, or share a user's data in a manner inconsistent with the user's privacy settings.
> 5. You will delete all data you received from us relating to any user who deauthorizes, disconnects, or otherwise disassociates from your application unless otherwise permitted in our Developer Principles and Policies.
> 6. You will delete all data you received from Facebook if we disable your application or ask you to do so.
> 7. We can require you to update any data you have received from us.
> 8. We can limit your access to data.
> 9. You will not transfer the data you receive from us (or enable that data to be transferred) without our prior consent.
>
> 3. You will not give us information that you independently collect from a user or a user's content without that user's consent.
>
> 4. You will make it easy for users to remove or disconnect from your application.
>
> 5. You will make it easy for users to contact you. We can also share your email address with users.
>
> 6. You will provide customer support for your application.
>
> 7. You will not show third party ads or web search boxes on Facebook user profiles or Pages.
>
> […]

[211] Facebook, Statement of Rights and Responsibilities, Last Updated December 21, 2009, <http://www.facebook.com/terms.php>.

> 13. You will comply with all applicable laws. […]
>
> 17. We can analyze your application, content, and data for any purpose, including commercial (such as for targeting the delivery of advertisements and indexing content for search).

To provide a sense of the potential impact of the privacy-related terms of service above, Facebook claims that there are more than 3 million active Pages on its platform.[212] The number of Pages on Facebook is greater than the total number of small businesses in Canada.[213] Although not every one of the three million Pages on Facebook involves the collection of user information by an organization, it is likely that many if not most of the Pages do. Facebook is intended to facilitate information sharing.[214]

Section 15 of the Facebook Statement serves as a reminder of one of the many reasons why organizations need to review and consider the terms of service of all sites or services that they utilize: "If anyone brings a claim against us related to your actions, content or information on Facebook, you will indemnify and hold us harmless from and against all damages, losses, and expenses of any kind (including reasonable legal fees and costs) related to such claim."

The Beacon case, referenced earlier in this paper, is a good example of why organizations need to carefully consider their role and responsibilities in collecting, using and disclosing personal information through social media sites. As described earlier, Facebook's Beacon program had shared individuals' information by default, without requiring them to opt-in to the program. Specifically, the Beacon program broadcasted a Facebook user's interaction with third-party websites to the newsfeeds of the user's friends in Facebook. The third-party sites controlled which actions taken by a user would generate "news" on the feeds of the user's friends on Facebook.[215] As a result, in the public relations and legal responses that followed the launch of Beacon, Facebook was not the only target. Class action suits stemming out of the Beacon program were brought against Facebook and a third-party advertiser, Blockbuster. In *Harris v.*

---

[212] Facebook, Press Room, Statistics, online: <http://www.facebook.com/press/info.php?statistics>.

[213] The Business Register of Statistics Canada maintains a count of business establishments and publishes results twice a year. As of December 2007, there were more than 2.3 million business establishments in Canada. See Industry Canada, "Key Small Business Statistics – July 2008)" (August 17, 2009), online: <http://www.ic.gc.ca/eic/site/sbrp-rppe.nsf/eng/rd02300.html>.

[214] *Supra* note 46.

[215] Electronic Privacy Information Center, "*Harris v. Blockbuster*" online: EPIC <http://epic.org/amicus/blockbuster/default.html> [EPIC, "Harris"].

Blockbuster, Inc.,[216] the plaintiffs alleged that Blockbuster had violated the *Video Privacy Protection Act*[217] by publishing the movie rental activities of Beacon users on the Facebook platform.

The interplay between privacy legal requirements and social media providers' terms of service will undoubtedly give rise to important privacy issues in future, particularly as social media services take on an increasingly prominent role for both individuals and the organizations that wish to reach them through such services.

(B) Social norms and default settings

Have social norms – the "principles or rules people are expected to observe, [representing] the dos and don'ts of society"[218] – about privacy changed in the information age? It appears that many people are more willing, or at least able, to share information about themselves than in the past. Younger generations also appear to be particularly interested in tools that enable information sharing; a recent survey reported that 25% of children aged 8-12 in the United Kingdom have a profile on at least one of Facebook, Bebo and MySpace.[219] Yet, it is important to question what, if anything, our uptake of new and emerging technologies tells us about social norms about privacy.

Facebook now claims to have 400 million users (including several fictitious accounts created by the author of this paper for research purposes); 5.9% of the world's population is on Facebook. Although that is a staggering number of people, the norms of Facebook users (if any can be distilled) can hardly be said to be representative of social norms around the world. At least 94.1% of the world population is not participating in Facebook, many of them likely by choice.

---

[216] (622 F. Supp. 2d 396) ["*Harris*"].

[217] This act was passed in 1988 and prohibits companies from disclosing information related to their customers' movie rentals.

[218] R.P. Appelbaum et al., "Confomity, Deviance, and Crime." in *Introduction to Sociology*, (New York: W. W. Norton & Company, 2009) at 173.

[219] OfCom, "UK Children's Media Literacy", online: <http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/ukchildrensml/>.

Further, even among Facebook members it can be difficult to draw conclusions about the norms, if any, that exist on that platform in light of the significant impact of default privacy settings. Consider, for example, the following commentary on the numbers that came out of Facebook's December 2009 privacy changes:

> For those who missed it, Facebook asked users to reconsider their privacy settings. The first instantiation of the process asked users to consider various types of content and choose whether to make that content available to "Everyone" or to keep their old settings. The default new choice was "Everyone." Many users encountered this pop-up when they logged in and just clicked on through because they wanted to get to Facebook itself. In doing so, these users changed all of their settings to public, many without realizing it. When challenged by the Federal Trade Commission, Facebook proudly announced that 35% of users had altered their privacy settings when they had encountered this popup. They were proud of this because, as research has shown, very few people actually change the defaults. But this means that 65% of users changed their settings to public.
>
> If one believes that no one cares about privacy, one might think that Facebook users consciously made their content public. But I've spent a lot of time browsing Facebook's "Everybody" feed since the privacy setting debacle in December and I don't think a lot of what I'm seeing is meant to be public. So I started asking non-techy users about their privacy settings on Facebook. I ask them what they think their settings are and then ask them to look at their settings with me. I have yet to find someone whose belief matched up with their reality. That is not good news. Facebook built its name and reputation on being a closed network that enabled privacy in new ways, something that its users deeply value and STILL believe is the case. Are there Facebook users who want their content to be publicly accessible? Of course. But 65% of all Facebook users? No way.[220]

To take another example, researchers and regulatory authorities recently took an interest in the discovery of vast amounts of confidential business information and personal health information, among other sensitive information, found on peer-to-peer ("p2p") file sharing

[220] Danah Boyd, "Making Sense of Privacy and Publicity", Keynote address to SXSW, Austin, Texas, March 13, 2010, online: <http://www.danah.org/papers/talks/2010/SXSW2010.html>.

networks.[221] It is commonly known that some p2p software systems have default settings which may result in individuals sharing information on their computers without their knowledge. Accordingly, when employees install p2p software at work, or when they or their family members install such programs at home, they can inadvertently share sensitive information with an entire p2p network. The effect of default settings and functions in p2p software on inadvertent sharing of medical information was specifically addressed in a recent study published in the Journal of the American Medical Informatics Association:

> Coerced sharing feature: The user interface makes it quite difficult to disable the sharing of the folder used to store downloaded files. In some cases, hidden functionality makes it quiet difficult to stop sharing. For example, in a recent version of Limewire, a new "Individually Shared Files" feature was added, which allows the user to select which files can be shared individually rather than sharing whole directories. However, if the user un-shares the directory, that does not stop sharing the files inside it because they are also individually shared. Therefore, the user would also have to go in and unshare each individual file in the directory.[222]

It is also apparent from the examples discussed in this paper that individuals vehemently object when organizations' practices – particularly unexpected default settings – diverge from individuals' privacy expectations. At root, the principles of knowledge, consent and control (that are the foundation of PIPEDA and other privacy laws) arguably continue to most closely reflect social norms about privacy, including in the context of new technologies.

The Information and Privacy Commissioner of Ontario had the following to say in response to Zuckerberg's statement reproduced at the outset of this paper:

> The human condition requires connection: We are social animals who seek contact with each other. We also seek privacy: moments of solitude, intimacy, quiet, reserve and control – personal control. These interests have co-existed for centuries and must continue to do so, for the human condition requires both.

---

[221] See *e.g.* Khaled El Emam, et al., "The inadvertent disclosure of personal health information through peer-to-peer file sharing programs" (2010) 17 JAMIA 148; Ned Smith, "File-sharing software reveals user's private info: Some P2P programs automatically share everything on your computer", MSNBC (16 March 2010), online: <http://www.msnbc.msn.com/id/35893007/ns/technology_and_science-security/>; Elinor Mills, "FTC warns 100 organizations about leaked data via P2P" Cnet (22 February 2010), online: <http://news.cnet.com/8301-27080_3-10457932-245.html>.

[222] El Emam, *ibid.* at 150.

> The fact that social media are growing exponentially does not negate that equation. What this explosion in technology does raise, however, is whether it is possible to preserve the notion of data protection in the online world. Can we continue to control and protect the personal information we share with others in social media, or are such media essentially becoming public spheres?
>
> […]
>
> It is not that privacy has stopped being the norm; it is that privacy is a dynamic that is a complex function based on an individual's needs and choices – choices that must be respected and strongly protected if we are to maintain freedom and liberty in our society. This will largely depend on the measures taken by both online social networks to embed easily accessible, privacy-protective controls into their offerings, and the willingness of people to use them.[223]

New technologies, including internet-based and other mobile and communications technologies, play an increasingly prominent role in the day to day lives of many of the world's citizens. Internet access is widely viewed as a fundamental human right.[224] Yet, one in five people report that threats to privacy on the internet cause them the most concern, outweighed only by concerns about fraud and violent and explicit content.[225] Individuals clearly do not expect that they must check their privacy expectations at the on-ramp to the information superhighway – individuals do not consider many internet-related activities to be taking place in public spaces. Nor would it be desirable that they be required to do so. An internet connection is not the end of the story when it comes to internet access as a human right; it is the beginning. The privacy-related conditions under which individuals are able to access and utilize the internet are critically important. The increased prevalence of and sharing of personal information on the internet and by other means suggests that, for both organizations and individuals, the stakes in how privacy is handled matter more now than ever before:

> […] personal information has become the principal commercial asset of social networking sites and free online search engines. This asset has spawned a whole new economic sector – the

---

[223] Cavoukian, *supra* note 2.

[224] BBC, "Internet Access is a 'Fundamental Right'" BBC (8 March 2010), online: <http://news.bbc.co.uk/2/hi/technology/8548190.stm> (reporting on a new global poll regarding internet access).

[225] *Ibid*.

> tracking, profiling and targeting of consumers for various types of behavioural advertising.
>
> And those are just some of the legitimate uses. Personal information also has tremendous value to spammers, identity thieves, fraudsters and other cyber-crooks.
>
> For all these reasons, personal information requires more protection than ever before.
>
> Without adequate protection, the risks are significant – to consumer confidence, to global business, and, of course, to some of the very fundamental rights that Canadians expect.[226]

Without effective privacy protections, individuals may be reluctant to sign up for innovative new services. On the hand, too much privacy can eliminate one of the key sources of revenue for organizations offering such services. As noted in the Facebook case, requiring individuals to give up a certain amount of personal information for relatively non-invasive online advertising was accepted by the OPC as being a reasonable requirement to gain access to a free service such as Facebook. This dynamic has created a tension in many online services between the desire to cater to individuals' privacy requirements and the need of organizations to collect, use and disclose personal information in order to offer the service. Where there are disconnects between individuals' perception – their privacy expectations, knowledge and consent – and the reality of how a service is operated, however, organizations can expect that privacy laws, market forces, and social norms will step in.[227]

---

[226] See generally, Jennifer Stoddart, OPC, "The Future of Privacy Regulation", Remarks at the 11th Annual Privacy and Security Conference, February 10, 2010, Victoria, British Columbia, online: <http://www.priv.gc.ca/speech/2010/sp-d_20100210_e.cfm>.

[227] FTC, *supra* note 55 ("In recent years we have witnessed an explosion of "free" online content and services that collect, integrate, and disseminate data. Examples include web mail, blogs, mapping and location based services, photo sharing, desktop organization, social networking, instant messaging, and mobile applications. These technologies offer valuable benefits, but not all consumers understand how the business model works. Consumers repeatedly pay for "free" content and services by disclosing their personal information, which is used to generate targeted advertising or for other commercial purposes. Once data is shared, it cannot simply be recalled or deleted – which magnifies the cumulative consequences for consumers, whether they realize it or not. This potential disconnect between consumer perception and business reality is troubling, and it merits increased Commission attention.")

(C) The role of the law and the future of privacy policies

Privacy laws have proved to be remarkably resilient when it comes to the issues posed by new technologies. PIPEDA received Royal Assent a decade ago in 2000. Fewer people were on the internet in 2000 than there are users of Facebook today.[228] While there is no question that PIPEDA faces challenges and can always be improved, its technology-neutral stance and reliance on foundational principles of control, knowledge and consent are as relevant and effective today as they have ever been.

On the other hand, in a world where everyday activities involve personal information crossing borders; where devices and technologies make it difficult to understand and observe where, when and how personal information is collected, used and disclosed, and by whom; where it can be confusing for organizations and individuals alike to understand what counts as "personal information" and what does not; and where children are present in the market, the bounds of national privacy laws premised on knowledge and consent are under increasing strain. Location-based services, behavioural advertising and cloud computing, among other developments, will only continue to apply pressure.

In the United States, a recently-formed coalition – called Digital Due Process[229] – of businesses, academics, public interest groups and others, including ACLU, AT&T, Google, Microsoft, the Center for Democracy and Technology, and the Electronic Frontier Foundation, have recently called on Congress to update the American *Electronic Communications Privacy Act* to reflect the myriad technological developments that have transpired since that law was passed into force in 1986. A white paper on the coalition website describes part of the driving force for change as follows: "[c]hanges in technology since 1986 have made it difficult to apply ECPA in a manner that comports with the reasonable expectations of individuals, potentially eroding user willingness to entrust private information to third-party service providers in the United States."[230] Certainty about privacy protections in cloud computing is obviously one of the considerations motivating the Digital Due Process Coalition.

---

[228] See Internet World Stats, <http://www.internetworldstats.com/stats.htm>.

[229] <http://www.digitaldueprocess.org>

[230] J. Beckwith Burr, "The Electronic Communications Privacy Act of 1986: Principles for Reform" (2010), online: <http://www.digitaldueprocess.org/files/DDP_Burr_Memo.pdf>.

In addition to developments in the United States, many stakeholders are calling for privacy regulation to go global in the form of a global standard of privacy protection and enforcement. With information crossing many borders and with organizations doing business in multiple jurisdictions where privacy laws may be different, there is a desire for the certainty and consistency that a global standard and enforcement could bring. Common standards have the potential both to enhance global privacy protection and to facilitate transborder data flows. A variety of global initiatives are underway.[231]

Increasingly, questions are also being raised about whether (privacy-policy based) consent is an appropriate model for the protection of privacy in the fast-moving technological environment where attention spans are short and where technical information about how personal information is collected, used and disclosed can be challenging to understand. Lengthy, standard-form privacy policies and terms of service arguably do little to achieve effective consent.[232] Although internet users are increasingly savvy, and many appear ready, willing and able to publicly dissect every change that Facebook makes to its privacy policies, some have suggested that there may be better alternatives to addressing knowledge and consent in the information age. In the behavioural advertising context, for example, some have:

> …highlighted the need for additional disclosure mechanisms beyond the privacy policy and suggested various options, such as: (i) providing "just-in-time" notice at the point at which a consumer's action triggers data collection; (ii) placing a text prompt next to, or imbedded in, the advertisement; and (iii) placing a prominent disclosure on the website that links to the relevant area within the site's privacy policy for a more detailed description.[233]

---

[231] See generally, Jennifer Stoddart, "The Future of Privacy Regulation" *supra* note 226; Tom Pullar-Strecker, "UN treaty on privacy possible" The Dominion Post (April 5, 2010), online: <http://www.stuff.co.nz/technology/3546868/UN-treaty-on-privacy-possible/>.

[232] See, *e.g.*, Jon Leibowitz, FTC, Remarks at the FTC Town Hall Meeting on "Behavioral Advertising: Tracking, Targeting, & Technology" at 4-5 (Nov. 1, 2007), <http://www.ftc.gov/speeches/leibowitz/071031ehavior.pdf >.

[233] FTC, *supra* note 172. On this topic, in November 2009 Google launched Google Dashboard in an effort to provide "transparency, choice and control" to individuals about the data associated with their use of 20 different Google products and services. See Google, "Transparency, choice and control – now complete with a Dashboard!" (November 5, 2009), online: <http://googleblog.blogspot.com/2009/11/transparency-choice-and-control-now.html>. Google claimed that "Dashboard summarizes data for each product that you use (when signed in to your account) and provides you direct links to control your personal settings" and that "[t]he scale and level of detail of the Dashboard is unprecedented". While Dashboard is a welcome development and shows potential for helping to achieve the goals of transparency, choice and control, some feel that it could have gone

Consent models of privacy protection, including PIPEDA, are arguably particularly ill-suited to protect children, who are unable to give consent in a variety of other legal contexts. Indeed, children's privacy is widely expected to be a key area of regulatory and policy focus in future.[234] It is notable that a large proportion of children under 12 in the United Kingdom already have profiles on social networking sites.[235] Children can be particularly vulnerable to behavioural advertising and other practices enabled by new technologies, given that they may be more likely to be manipulated into divulging personal information and are less likely to understand the consequences of sharing information with marketers.[236] Effective legal solutions are not obvious. In the United States, the *Children's Online Privacy Protection Act of 1998* ("COPPA") attempts to protect the online privacy of children by requiring verifiable parental consent before a child's personal information could be collected. It is widely accepted, however, that COPPA has been far from perfect in protecting children's privacy as the practicality of obtaining "verifiable" parental consent is difficult to enforce. Similarly, COPPA only restricts personal information that can identify an individual child and not the collection of aggregate data. Subject to whether such aggregate data is *truly* anonymous, forms of behavioural advertising to children are thus arguably still possible under privacy laws.[237]

Finally, it is without question that one of the greatest challenges for privacy law in the future will be one of the foundational definitions upon which privacy regulation is built – the definition of "personal information" or "personal data", sometimes called "personally identifiable information". This question is critical because privacy laws typically will not apply at all when the information at issue does not fit the applicable definition of "personal information". In the context of behavioural advertising, for example, some have argued that targeted advertisements pose no privacy threat because the organizations at issue do not know

---

further than it did. See *e.g.* Stan Schroeder, "Google Dashboard: Now You Know What Google Knows About You" Mashable (5 November 2009), online: <http://mashable.com/2009/11/05/google-privacy-dashboard>.

[234] Children's' privacy was a focus of the first round of PIPEDA reform. See also, the working group of Canadian Privacy Commissioners and child and youth advocates, "There ought to be a law: Protecting children's online privacy in the 21st Century" (19 November 2009), online: <http://www.gnb.ca/0073/PDF/Children'sOnlinePrivacy-e.pdf> at p. 8.

[235] OfCom, *supra* note 219.

[236] See the working group of Canadian Privacy Commissioners and child and youth advocates, "There ought to be a law: Protecting children's online privacy in the 21st Century" (19 November 2009), online: <http://www.gnb.ca/0073/PDF/Children'sOnlinePrivacy-e.pdf> at p. 8.

[237] *Ibid*. See also, *infra* note 246.

individuals' names or other identifying information.[238] However, there are many reasons to believe that seemingly anonymous information can be capable of identifying individuals[239], particularly when associated with a unique identifier or an IP address and a time.

PIPEDA defines "personal information" as "information about an identifiable individual."[240] The OPC has stated that for information to be "personal information", the individual must be "identifiable" or "capable of being identified", but not necessarily identified.[241] For example, the OPC has held that computer internet protocol (IP) addresses can be considered personal information.[242] Similarly, in *Gordon v. Canada (Health)*[243], the Federal Court adopted the following interpretation of "information about an identifiable individual": "Information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information."[244] The OPC described the facts of this case as follows:

> … the Court agreed with a refusal by Health Canada to disclose the 'province' field of the Canadian Adverse Drug Reaction Information System (CADRIS) database. The Court held that disclosure of the province field, when combined with other data-

---

[238] See *e.g.* Phorm, Phorm Service Privacy Policy (Updated February 13, 2008), online: <http://privacy.phorm.com/policy_services.php> ("The Phorm Service is designed to avoid collection of any Personally Identifiable Information of the user ("PII"), namely information that can be directly associated with that specific person or entity, e.g. a name, a postal address, a phone number, or an email. Phorm Service uses only Non-Personally Identifiable Information ("non-PII"), such as search terms, URLs and keywords. Phorm Service does not store or retain this information. This information is used to understand broad categories of that consumer's interests; the Phorm Service matches this with existing advertising categories ("category match"), then immediately discards this information. It is important for consumers to know that even the limited retained category match information cannot be used to identify any specific person or entity. By way of example, Phorm Service will retain only information about predefined categories of interest associated with a randomly generated ID (category matches) such as "ID #45678 is interested in IPODs."); Wendy Davis, "Watchdogs Ask FTC To Probe 'Behavioral Targeting On Steroids'" Media Post News (April 8, 2010), online: <http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=125732&nid=113056>.

[239] See *e.g.* Robert McMillan, "Researchers can ID anonymous Twitterers" *IT World* (March 26, 2009), online: <http://www.itworld.com/security/65168/researchers-can-id-anonymous-twitterers>.

[240] Section 2.

[241] PIPEDA Case Summary #349.

[242] PIPEDA Case Summary #315.

[243] 2008 FC 258 (CanLII).

[244] Emphasis added. Although this case arose under different legislation, the court adopted the definition of personal information urged by the Commissioner. In applying PIPEDA, and consistent with past Commissioner findings on the meaning of "personal information", it is expected that the Commissioner will utilize the definition adopted by the court in this case.

> fields already released as well as other publicly available information (such as obituaries, for example), would "substantially increase the possibility" that particular individuals could be identified. This was especially the case for unique or quasi-unique individual reports in smaller provinces or territories.[245]

Thus, the Commissioner has challenged the notion that anonymized information will always fall outside the definition of "personal information": "Although user profiles may be anonymized, it is still possible to link a profile to an individual. Profiles that are based on detailed marketing categories can potentially lead to the identification of an individual."[246] The use of unique identifiers across data fields has permitted identification of individuals in other contexts. The searches that individuals type into a search engine, for example, can be used to identify them when combined with one another and with a unique identifier to show which searches were submitted by the same individual. In a well-known case, the search strings of an anonymous individual that AOL identified as "No. 4417749" led journalists to an individual named Thelma Arnold.[247] 'Anonymized' geo-location data has been found to be similarly capable of identifying people.[248]

CONCLUSIONS

Privacy issues are present at the heart of many new developments in communications law, policy and practice. As highlighted by the examples discussed herein, new and emerging technologies frequently pose challenges for privacy laws and regulatory authorities and raise fundamental questions regarding social norms about privacy. Boyd reminds us of the importance of reflecting carefully on the complete picture at the intersection between privacy and new technologies and of how important it is that we get the balance right:

---

[245] See *Leading by Example: Key Developments in the First Seven Years of the Personal Information Protection and Electronic Documents Act (PIPEDA)*, online: <http://www.priv.gc.ca/information/pub/lbe_080523_e.cfm>.

[246] Review of the Internet traffic management practices of Internet service providers: Submission of the Office of the Privacy Commissioner of Canada to the Canadian Radio-television and Telecommunication Commission (CRTC) (February 2009), online: <http://www.priv.gc.ca/information/pub/sub_crtc_090218_e.cfm>. See also Robert McMillan, "Researchers can ID anonymous Twitterers" IT World (March 26, 2009), online: <http://www.itworld.com/security/65168/researchers-can-id-anonymous-twitterers>.

[247] Declan McCullagh, "AOL's disturbing glimpse into users' lives" cnet (August 7, 2006), online: <http://news.cnet.com/AOLs-disturbing-glimpse-into-users-lives/2100-1030_3-6103098.html>.

[248] Dan Goodin, "Scrubbed geo-location data not so anonymous after all" The Register, (21 May 2009), online: <http://www.theregister.co.uk/2009/05/21/geo_location_data/>.

> Observing people's data traces gives no indication of whether or not they are trying to be public or private. You need to understand their intentions, how they're interpreting a technological system, and what they're trying to do to make it work for them. Each of you - as designers, as marketers, as parents, as users - needs to think through the implications and ethics of your decisions, of what it means to invade someone's privacy, or how your presumptions about someone's publicity may actually affect them. You are shaping the future. How you handle these challenging issues will affect a generation. Make sure you're creating the future you want to live in.[249]

As is already becoming evident as demonstrated by the examples discussed in this paper, technology will play a key role in how privacy conflicts of the future are resolved. New technologies are often a cause of privacy concern but increasingly they are also a part of the solution. Further, while practical and legal solutions to some of challenges at the nexus between privacy and new technologies can be vexing for organizations, individuals, regulatory authorities and policy makers alike, meaningful adherence to privacy fundamentals – knowledge and consent in particular – will go a long way to reconciling individuals privacy rights and norms with the need of organizations to collect, use and disclose personal information. Given the importance of personal information to all participants in the information age, meaningful adherence to these privacy fundamentals will be a critical fuel of future innovation and an essential measure of success in communications law, policy and practice.

[249] Boyd, *supra* note 220.