Canadian Internet Policy and Public Interest Clinic
Clinique d'intérêt public et de politique d'internet du Canada

ONLINE PRIVACY THREATS:

A REVIEW AND ANALYSIS OF CURRENT THREATS

AUTUMN, 2008

Canadian Internet Policy and Public Interest Clinic (CIPPIC)
University of Ottawa, Faculty of Law
57 Louis Pasteur, Ottawa, ON K1N 6N5
tel: 613-562-5800 x2553
fax: 613-562-5417
www.cippic.ca

Acknowledgements

CIPPIC gratefully acknowledges the financial support of the Office of the Privacy Commissioner of Canada for this study.

The study was directed by David Fewer, CIPPIC Staff Counsel. The report was drafted by David Fewer, with contributions from Philippa Lawson. Myriam Gosselin provided administrative support.

The following law students undertook research that supported this report: Janet Lo, Rachel Leck, Mischa Melia-Gordon, Lisanne McCullough, Shahram Bahmadi, Janice Joo, Tamarah Luk, Jocelyn Cleary and Chris Donaldson. CIPPIC thanks these students for their efforts, enthusiasm, and findings. Special thanks to Janet Lo for her diligence and leadership, and to Andrew Coleman for his research.

Canadian Internet Policy and Public Interest Clinic
University of Ottawa, Faculty of Law
57 Louis Pasteur St.
Ottawa, Ontario K1N 6N5
Canada

Tel: 613-562-5800 x.2553
Fax: 613-562-5417

Email: cippic@uottawa.ca

ISBN x-xxxxxx-x-x

This publication is also available on our website at www.cippic.ca.

Table of Contents

Introduction: Online Threats to Privacy

Threats to Canadians' privacy interests from online sources make for headline news in Canada. In February, 2008, Canadian law enforcement authorities arrested 17 Canadians alleging that they had built and deployed massive botnets – networks of hacked and remotely controlled computers – for such diverse harmful activities as identity fraud, data theft, spamming, and denial-of-service attacks.[1] Online commercial sites such as Facebook and MySpace, both of which enjoy significant penetration into the Canadian marketplace, face regular criticism for their treatment of the personal information of consumers' personal information.[2] Even in our personal lives, Canadians are routinely asked to implement security measures, such as downloading and installing software updates and patches, designed to secure our computing environment and, thereby, our personal information.[3]

The nature of these threats is often unclear to the average Canadian. Where do these threats originate? Who wants to invade our privacy? What kind of information do they want, and what do they want to do with it? Equally unclear is the nature of our collective response to these phenomena. Is Canada responding to online threats to protect Canadians? What can individuals do to protect their privacy?

In this Report, we seek to answer some of these questions. This Report discusses the nature of online threats to Canadians' privacy, the motivations for those threats, and regulatory responses to those threats. In Part I, we survey the landscape. What kinds of online threats to privacy do Canadians face? To answer that question, we offer a framework to help the reader understand the nature and scope of these threats. First, we consider the motivations behind privacy threats. In our view, privacy threats may be divided into three broad classifications: those motivated by fraud, those targeting individuals for personal reasons, and those undertaken in commercial contexts. Second, we consider the tools of the trade, the technologies that are often deployed to violate Canadians' privacy interests. Third, we consider specific behaviours that threaten

---

[1] Robert McMillan, "17 arrested in Canadian hacking bust" *InfoWorld* (21 February 2008), <http://www.infoworld.com/article/08/02/21/17-arrested-in-Canadian-hacking-bust_1.html> [McMillan, "17 arrested"].

[2] See, *e.g.*, Stefan Berteau, "Facebook's Misrepresentation of Beacon's Threat to Privacy: Tracking users who opt out or are not logged in" *CA Security Advisor Research Blog* (29 November 2007), <http://community.ca.com/blogs/securityadvisor/archive/2007/11/29/facebook-s-misrepresentation-of-beacon-s-threat-to-privacy-tracking-users-who-opt-out-or-are-not-logged-in.aspx>; MoveOn.org, "Petition: FaceBook Must Respect Privacy" <http://civ.moveon.org/facebookprivacy/> (asking signatories to sign on to the statement, "Sites like Facebook must respect my privacy. They should not tell my friends what I buy on other sites--or let companies use my name to endorse their products--without my explicit permission."); Netcraft, "MySpace Accounts Compromised by Phishers" (27 October 2006), <http://news.netcraft.com/archives/2006/10/27/myspace_accounts_compromised_by_phishers.html>.

[3] Microsoft releases updates to its supported operating systems on the second Tuesday of each month, leading the technology world to dub the date "Patch Tuesday": see Microsoft, "Security Updates" <http://www.microsoft.com/protect/computer/updates/bulletins/default.mspx>; Linda Leung, "Forget about sleeping: It's Patch Tuesday" *Network World* (1 October 2005), <http://www.networkworld.com/news/2005/011005widernetpatchtuesday.html>.

Canadians' privacy interests. These behaviours result from the combination of specific motivations with the tools of the trade.

In Part II, we survey the range of responses to online threats to privacy. We suggest that these responses fall into five categories: government regulation, industry self-regulation, technological responses, international co-operative efforts, and public education.

In Part III, we assess the capacity of Canada's federal private sector privacy legislation, the *Personal Information Protection and Electronic Documents Act*,[4] or PIPEDA, to address online privacy threats. As might be expected from the framework we have deployed, we find that PIPEDA offers only a partial solution to the broader problem of online privacy threats, because of its limitations in both scope and effectiveness. PIPEDA regulates only commercial, private sector activity, and is not designed to address fraudulent activity. Privacy invasions motivated by personal considerations therefore lie beyond its scope. Moreover, while in theory PIPEDA offers potential to address online privacy threats with commercial motivations, in practice we have found that PIPEDA has not quite lived up to its promise.

We conclude with a global assessment of responses to online privacy threats. Given the variety of motivations behind online privacy threats, Canadians should not expect that any single regulatory response will protect us from all such threats. Indeed, threats to online privacy might also come from the law enforcement or state security services. While consideration of those threats to online privacy lies beyond the scope of this Report, we mention them to underline the reality that there is no single solution to all online threats to privacy. Practical protections for Canadians' privacy will continue to come from a variety of sources, including law enforcement, technological solutions, and Canadians' continuing self-education.

[4] *Personal Information Protection and Electronic Documents Act* 2000 *Statutes of Canada* ch.5 <http://laws.justice.gc.ca/en/ShowFullDoc/cs/P-8.6///en> [PIPEDA].

Part I Technologies and Behaviours

One of the challenges facing anyone seeking to understand the nature and scope of online threats to privacy – indeed, of online threats to any interests or values – is to distinguish between threatening behaviour and the tools used to carry out that behaviour.

For better or worse, public attention to online threats has tended to focus on the technologies employed in furtherance of some illicit aim rather than on the illicit aim itself. The Nigerian scam is a very different beast from the initiatives of erectile dysfunction medication marketers, yet both phenomena are often addressed in the popular media under the rubric of "spam". Pill pushers and Nigerian scammers both rely on spamming technologies to achieve their ends, but their motivations (legitimate commerce for the former, fraud for the latter) and behaviours differ (aggressive marketing of pharmaceuticals v. behavioural engineering).

In this Part, we attempt to break down online threats to privacy into their constituent parts. First, we consider the motivations that underlie these threats. Second, we address the tools of the trade: the technologies used in realizing these privacy threats. Third, we identify the behaviours that are currently threatening Canadians' privacy in online environments. Just as a tool, such as a screwdriver, might have a variety of uses, so too may a technological tool support a variety of different privacy threats.

A Motivations: Why Target Personal Information?

There are many different reasons to target others' personal information. Considered broadly, however, we view the motivations of all online privacy threats as falling within three broad categories: (1) fraud, (2) personal attacks, and (3) commerce.

An attack on personal privacy motivated by fraud is one outside the law. Those behind such attacks typically understand that what they are doing violates social norms and likely violates the law. Privacy threats based on personally motivated attacks, in contrast, arise precisely because of the identity of the victim. Typically, these attacks involve someone known to the assailant. They also generally violate the law – although not always. Commercially motivated privacy threats, on the other hand, might or might not involve an appreciation that the behaviour violates normative rules, but otherwise do not involve knowing violations of the law (although, as in the case of nuisance adware, activity might deliberately stray into the "grey zone" of behaviour that may or may not fall afoul the law).

1 Fraud

Fraud lies at the root of the majority of online threats to privacy. Simply, consumers' personal information – their financial data, their identity documents, their passwords and subscription data – have value, and that value is attractive to those operating outside the bounds of the law. It is impossible to accurately measure the size of the annual black market trade in stolen personal information. The Retail Council of Canada estimates that

organized crime, generally, costs Canadians $5 billion a year.[5] Online fraud is estimated to cost Americans $45 billion per year,[6] while a recent survey placed the cost of online fraud in the UK at £580 million annually.[7]

The black marketplace for online fraudsters has become sophisticated and commoditized. The tools of this illicit-trade are no longer the exclusive domain of expert hackers, only: now, "kits" are openly sold on underground bulletin boards and chat rooms.[8] Would-be fraudsters can simply purchase the technology they need to set up their own identity fraud operations. Fraudsters may similarly dispose of the fruits of their efforts on black market websites.[9] If you know where to go, you can simply purchase stolen credit cards on the net. IBM's Gunter Ollman reports as follows:

> It should be no surprise that there are plenty of web sites that buy and sell identity information – most of them focused on credit cards – and any quick Google searches will likely reveal many of the more popular sites. The 'better' sites tend to stay below any of the search-engine radars, and it'll take a little digging to find them (not much though). If you embark on your own investigative path, you'd better brush up on your IRC etiquette and find a good Russian-to-English translator program.[10]

Online fraud is a phenomenon on the rise. The American Federal Trade Commission reports that identity theft complaints, for the 8th year in a row, topped all consumer complaints to the FTC.[11] Phonebusters, Canada's fraud reporting service, reports that Canadians reported over 16 million in losses from identity theft in 2006.[12]

2 Personal Attacks on Privacy

A third motivation for threats to online privacy arises from factors that are particular to the victim. A relationship between two individuals – a couple going through a break-up, an employer and ex-employee, etc. – may cause one party to target the personal

[5] Retail Council of Canada , "Retail Council of Canada Participates in Fraud Prevention Month" (1 March 2007), <http://www.retailcouncil.org/news/media/press/2007/pr20070301.asp>.
[6] Liz Moyer with Tatyana Shumsky, "Like Stealing Credit From A Baby" *Forbes.com* (6 March 2008), <http://www.forbes.com/wallstreet/2008/03/06/credit-card-fraud-biz-wall-cx_lm_0306idfraud08_protect.html>.
[7] Dave Friedlos, "Online fraud to soar to £1.5bn" *Computing* (15 May 2007), <http://www.computing.co.uk/computing/news/2189932/online-fraud-soar-5bn>.
[8] Julie Bort "Attack of the Killer Bots" *PC World* (28 September 2007), <http://www.pcworld.com/businesscenter/article/137797/attack_of_the_killer_bots.html>.
[9] Beth Cox, "The Great Credit Card Bazaar" *internetnews.com* (20 September 2002), <http://www.internetnews.com/ec-news/article.php/1467331>.
[10] Gunter Ollmann, "Psst... wanna buy some credit cards?" *IBM's Frequency X Blog* (12 November 2007), <http://blogs.iss.net/archive/BuyCreditCards.html>.
[11] Federal Trade Commission, "FTC Releases List of Top Consumer Fraud Complaints in 2007" (13 February 2008), <http://www.ftc.gov/opa/2008/02/fraud.shtm>.
[12] Phonebusters, "Identity Theft Statistics" <http://www.phonebusters.com/english/statistics_E06.html>.

information of the other. "Cyberstalking" is perhaps the most common form of this kind of attack on personal information.[13]

Whereas both commercially motivated threats to privacy and attacks on privacy motivated by fraud, at bottom, share a common interest in money, personally motivated attacks seldom focus on financial assets. Rather, the motivations may be more basic: revenge, jealousy, hate, and control. Accordingly, regulatory approaches that might be expected to ameliorate some of the harms associated with fraud and market-based threats to privacy – such as laws regulating use of computing resources, for example – may have little deterrent effect on personally motivated privacy attacks.

3 Commerce

Online marketing is big business. The Interactive Advertising Bureau of Canada reported that in 2006, Canadian online advertising revenues amounted to $1.01 billion dollars, an 80% increase over 2005 figures.[14] This commercial activity pressures Canadians' personal information. This pressure comes from two sources: the value of customer data to businesses, and the danger of security breach, or third party interception of personal data held by commercial interests.

Canadians' personal information is, in itself, valuable to businesses: the more a business knows about its customers, the more effective its marketing potential. New technologies are permitting businesses to collect and exploit personal information in unexpected ways. Consider the adware/spyware phenomenon: the emergence of new technologies permitted businesses to explore new mechanisms for placing advertising before viewers. Exploration of this space involved, at times, straying into "grey" areas in which the law was uncertain. At times, businesses broke the law.[15] By 2008, however, this space had settled as authorities developed rules for acceptable – and legal – behaviour. This is a phenomenon we can expect to repeat as new technologies create new opportunities for consumers and businesses to interact. In fact, we may be witnessing just this dynamic in the context of behavioural advertising. The Federal Trade Commission is currently soliciting comments with respect to a set of draft principles intended to ground a self-regulatory regime for companies engaged in online behavioural advertising – the practice of targeting online advertising at a consumer based upon data collected by tracking the consumer's online activities, often without the consumer's awareness that they are being tracked and targeted.[16] It is hoped that the formulation of sound, self-regulatory principles in this space, and their widespread adoption, will reduce the scope of consumer privacy invasion from commercial pressures.

---

[13] See, *e.g.*, "Safety Tips" of the National Network to End Domestic Violence <http://www.nnedv.org/resources/internetsafety/ >.

[14] Interactive Advertising Bureau of Canada, **"**2006 Canadian Online Advertising Tops $1 Billion Dollars" (30 April 2007), <http://www.iabcanada.com/newsletters/070430.shtml>.

[15] See, *e.g.*, Joris Evers, "Spyware kingpin hammered for $4m" *CNET News.com* (5 May 2006), <http://news.zdnet.co.uk/itmanagement/0,1000000308,39267241,00.htm>.

[16] See Federal Trade Commission, "Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles" (20 December, 2007) <http://www.ftc.gov/os/2007/12/P859900stmt.pdf >.

This increase in businesses' interaction with consumers' personal information has given rise to additional threats to consumers' online privacy: the security breach. This concern links back to fraud, the first motivation we have identified for online threats to privacy. Fraudsters appreciate the value of the personal information held by commercial interests, and that makes those businesses attractive targets. Recent headlines have been filled with stories of security breaches involving the inadvertent disclosure of consumers' personal information.[17] Business-side threats to consumers' privacy include platform-based exploits. Consider social networking sites like Facebook and MySpace, which hold reams of personal information, often provided in a non-commercial context. That information is only as secure as the service-provider's online environment, and we are seeing that these environments can be vulnerable to third party exploits and security breaches.[18]

B The Tools of the Trade

Online threats to privacy make use of a dizzying array of tools to achieve their ends. Few tools are used in isolation; rather, an attacker will combine from their toolkit those tools most suited to the task at hand.

For this discussion, we divide this toolkit into three groups: (1) platforms, which are not so much tools as online interfaces with individuals, (2) tools, by which we mean technologies that enable behaviors that may threaten privacy, and (3) strategies for engaging users in activity that results in threats to privacy.

1 Platforms

Online privacy threats require a medium, a space in which to engage individuals. In the online world, that medium embraces all of the services and content that we experience online. In this Report, we consider the most common such spaces from which online privacy threats emerge: email, websites and social networking spaces. However, almost any online medium in which individuals engage can harbour threats to privacy.

a Email

Email – in its most unwanted form, spam – is, perhaps, the first thing we think of when we consider online privacy threats. Spam was among the earliest of online privacy invasions to make itself felt on the average internet user. Email has become essential to our personal and professional lives. For many, checking email has become as habitual and essential as a morning cup of coffee.

To one seeking to exploit our personal information, an email address is as good as an invitation to enter a target's domicile. That invitation is being taken up by a variety of interests. First, email is the fundamental tool of spam of the plain vanilla, unsolicited commercial variety. Second, spam is a vehicle for soliciting victims for more personal

[17] See, e.g., Scott Bradner, "TJX security lapse: Willfully and with malice of forethought?" *Network World* (22 January 2007), <http://www.networkworld.com/columnists/2007/012207-bradner.html>.

[18] In January 2008, Fortiguard, a security firm, reported that a Facebook widget named "Secret Crush" was being used to social engineer users into installing Zango, a well known adware program: see "Facebook Widget Installing Spyware" *Fortiguard Center* (2 January 2008), <http://www.fortiguardcenter.com/advisory/FGA-2007-16.html>.

attacks, such as phishing (social engineering attacks designed to trick victims into volunteering valuable information, addressed below) and other attacks targeting personal information: a link embedded in an email message, if clicked on by a target, will bring the target to a website wherein a range of additional attacks become possible. Third, email can be a tool for targeted attacks on individuals. If a stalker, for example, obtains a victim's email password, the stalker then has access to tremendously personal information, and can impersonate the victim.

Email has become increasingly complex over time. Today's email client's are capable of supporting html and active code within an email message, which opens individuals to a range of attacks that plain text spam is not capable of.[19]

b Websites

Websites – the content of the web – provide attacks on users' personal information with a staging platform. In this sense, websites, like email, may function as a delivery mechanism for an invasion strategy. That strategy may involve delivery of some form of malware that will actively invade a victim's computer, in which case the website's server-side code will include code that is unwanted or even illegal. Other strategies involve no code. Some social engineering strategies, such as phishing, rely upon simple and familiar interfaces – such as the look and feel of the website of one's bank – to achieve its fraudulent purpose.

More sophisticated phishing attacks, such as "man-in-the-middle" attacks, place an attacker between a victim and a legitimate website – such as a banking website. The victim cannot detect the attacker, and sees his or her bank site – but so does the attacker.[20]

c Social Networking Services

Social networking services are online services that permit users to share information, often personal, and interact with one another. Facebook, MySpace, Bebo, Orkut, LinkedIn, Perfspot, Friendster, and Neighborhood are examples of popular social networking sites. MySpace alone has over 200 million accounts.[21] Facebook's membership is growing at a steady rate, with 67 million active users as of March 2008, and an average of 250,000 new registrations per day since January 2007.[22] Facebook reports that it is the 6th most trafficked site in the United States with more than 65 billion page views per month and more than 14 million photos uploaded daily. Canada is the third largest country on Facebook with more than 7 million active users.

---

[19] Bob Brewin, "DOD bars use of HTML e-mail, Outlook Web Access" *FCW.com* (22 December 2006), <http://www.fcw.com/online/news/97178-1.html>.

[20] See, *e.g.*, Brian Krebs, "Not Your Average Phishing Scam" *Security Fix* (3 January 2007), <http://blog.washingtonpost.com/securityfix/2007/01/not_your_average_amazon_phishi.html> (reporting on an Amazon.com account man-in-the-middle attack propagated through a phishing "kit" available for sale on the Internet's black market).

[21] MessageLabs, "Social Networking: Brave New World or Revolution From Hell? A look at the phenomenon of Social Networking and the implications for Business" (White Paper 2007) at p. 1, <http://whitepapers.zdnet.com/whitepaper.aspx?docid=337546>.

[22] Facebook, "Press Room: Statistics" (March 2008), <http://www.facebook.com/press/info.php?statistics>. "Active users" are defined as users who have returned to the site in the last 30 days.

While social networking presents opportunities for individual empowerment and social good, it also comes with threats to users' privacy. First, social networking sites and the Web 2.0 applications they support can also harbour viruses, worms, Trojans, and spyware that will attack users' computers if given an opportunity.[23] Because of the amount of personal information users post about themselves on social networking sites, these sites are invaluable resources for cybercriminals who plan blended threats. Second, social networking sites present commercial parties with opportunities to access users' personal information in ways that might threaten users' privacy.

Consider Facebook. When a user registers with Facebook, Facebook requests the person's full name, email address, and birthday. When creating their user profile, users are asked to provide personal information such as their gender, hometown, political and religious views, instant messaging screen names, telephone numbers, address, relationship status, schools attended, courses enrolled in, current and previous employers, personal interests and preferences. Facebook also collects users' browser types and IP addresses.[24] Facebook also states that they may "collect information about you from other sources, such as newspapers, blogs, instant messaging services, and other users of the Facebook service through the operation of the service ... in order to provide you with more useful information and a more personalized experience."[25] Several commentators have expressed concerns about the way users share personal information on social networking sites, noting that while these sites are not a private space, users act as though they are private.[26] Information on the internet is uncontrolled – once a person posts their personal information online, it can be copied and distributed without their knowledge.

Security experts fear that user information garnered from individual profiles posted on social networking sites give cybercriminals the ability to deliver malware, adware, and spam to targeted users at unprecedented speeds and effectiveness.[27] This fear is proving well-founded. In January 2008, security vendor Fortinet warned Facebook users that the "Secret Crush" application installed Zango, adware that is labelled by most security vendors as potentially unwanted technology that may engage in consumer tracking for the purposes of targeting advertisements.[28] Upon installation of the "Secret Crush" application, users were informed that they had to invite at least five more friends to Secret Crush before going on, and then were invited to download a "Crush Calculator"

---

[23] ClearSwift, "Demystifying Web 2.0: Opportunity, Threats, Defenses" (White Paper 2007) at p. 5, <http://www.zdnet.com.au/whitepaper/0,2000063328,22313759p-16001383q,00.htm>.
[24] Facebook's Privacy Policy, <http://www.facebook.com/policy.php> [Facebook's Privacy Policy].
[25] *Ibid*.
[26] See the Privacy Commissioner of Canada on social networking: <http://privcom.gc.ca/information/social/index_e.asp> and Privacy Commissioner of Canada, "Fact Sheet: Social Networking and Privacy" <http://privcom.gc.ca/fs-fi/02_05_d_35_sn_e.asp> [Privacy Commissioner of Canada, "Social Networking and Privacy"]. See also Susan B. Barnes, "A privacy paradox: Social networking in the United States*" First Monday* (August 2006), <http://www.firstmonday.org/issues/issue11_9/barnes/>; Rob Killick, "Facebook and the death of privacy" (7 February 2008), <http://www.spiked-online.com/index.php?/site/article/4482/>.
[27] "Experts hammer Web 2.0 security: Security experts fear that social networking sites like Facebook and LinkedIn provide both a delivery vehicle for malware and the info to create targeted attacks" *InfoWorld* (21 February 2008), <http://www.infoworld.com/article/08/02/21/Experts-hammer-Web-20-security_1.html>.
[28] See, *e.g.*, Tenebril, "Spyware Information: Zango" <http://www.tenebril.com/src/info.php?id=451663045>.

application that contained the Zango software. Zango denied involvement with Secret Crush, but Facebook removed the application. Facebook reported that 1.5 million users installed Secret Crush before it was taken down.[29] Similarly, in 2007, a security expert found that a Facebook banner ad served an exploit, running an adware installer with the end result that an Internet Explorer homepage would display additional windows serving ads.[30] Facebook is not the only social networking site to face user security issues. In 2006, adware masked as YouTube videos surfaced on MySpace. When users clicked on what appeared to be a Windows Media Player video with filename "Yootube.info"), they were redirected to a new webpage that invited them to click on a license agreement for the installation of the adware program Zango Cash.[31] Zango's software products have been identified by many security companies as potentially unwanted technologies as they engage in consumer tracking for the purposes of delivering advertisements.[32]

Facebook markets itself as a medium that allows advertisers to "reach the exact audience with relevant targeted ads."[33] However, there are concerns that the race to learn more about users and translate that data into advertising revenues comes with a cost to user privacy. Facebook's Chief Privacy Officer, Chris Kelly, has often protested to the media that internet users no longer expect to remain anonymous online.[34]

2 Tools

Email, website, and social networking spaces provide those who threaten privacy with the space online from which to attack. In this next section, we address the technological tools employed in those attacks.

a Malware, Spyware and DRM

Malware, spyware and DRM we group together as forms of potentially unwanted technologies that attackers may use to threaten individuals' privacy. The Anti-Spyware Coalition (ASC) has defined "spyware" broadly as "potentially unwanted technologies", that is:

> Technologies deployed without appropriate user consent and/or implemented in ways that impair user control over:
>
> - Material changes that affect their user experience, privacy, or system security;

[29] "Facebook dumps Secret Crush application over spyware claim" *CNET News* (7 January 2008), <http://www.news.com/8301-13577_3-9843175-36.html?tag=bl>.
[30] "Facebook banner ad serves an exploit" *CNET News* (14 September 2007), <http://www.news.com/8301-10784_3-9778829-7.html?tag=bl>.
[31] "Adware may be lurking in video on MySpace" *CNET News* (7 November 2006), <http://www.news.com/Adware-may-be-lurking-in-video-on-MySpace/2100-7349_3-6133447.html>.
[32] See note 28, *supra*. See also Ben Edelman and Eric Howes, "Bad Practices Continue at Zango, Notwithstanding Proposed FTC Settlement and Zango's Claims" (20 November, 2006, updated, 8 December, 2006) <http://www.benedelman.org/news/112006-1.html>, noting the "privacy consequencens" to consumers for installing Zango software.
[33] "Facebook Ads", <http://www.facebook.com/ads/?src=gca2>.
[34] "Facebook under fire over targeted advertising*"* Telegraph.co.uk (12 Septembr 2007), <http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/09/11/nface111.xml>.

- Use of their system resources, including what programs are installed on their computers; and/or
- Collection, use, and distribution of their personal or other sensitive information.[35]

The ASC also defines spyware to have a narrow sense, as "*Tracking Software* deployed without adequate notice, consent, or control for the user," and further defines "Tracking Software" as software "that monitors user behaviour, or gathers information about the user, sometimes including personally identifiable or other sensitive information, through an executable program."[36]

"Malware", in contrast, is a general term that encompasses all malicious software. Symantec provides the following definition:

> Malware is a category of malicious code that includes viruses, worms, and Trojan horses. Destructive malware will utilize popular communication tools to spread, including worms sent through email and instant messages, Trojan horses dropped from web sites, and virus-infected files downloaded from peer-to-peer connections. Malware will also seek to exploit existing vulnerabilities on systems making their entry quiet and easy.[37]

From this definition, we can take a broad view of malware as describing different kinds of code, all malevolently authored, that perform some task that it unwanted by its victim. Malware describes code, not a tactic for distribution or a particular exploit.

Malware has, in fact, become professionalized. Malware is now coded by professional software developers, often working for organized crime.[38] Malware authors now employ encryption to make detection more difficult,[39] and, in the spirit of the best defense being a good offense, aggressively target and remove security software[40] and even rival malware.[41] This evolution in the nature of malware behaviour is forcing security experts to change their approach to security, moving from a threat recognition model to a

---

[35] Anti-Spyware Coalition, "Definitions and Supporting Documents" <http://www.antispywarecoalition.org/documents/2007definitions.htm> [ASC, "Definitions and Supporting Documents"].

[36] Anti-Spyware Coalition, "Glossary" < http://www.antispywarecoalition.org/documents/glossary.htm> [ASC, "Glossary"].

[37] Symantec, "Malware: How They Attack" <http://www.symantec.com/norton/security_response/malware.jsp>.

[38] Panda Software, Quarterly Report, April – June 2007 <http://research.pandasecurity.com/blogs/images/PandaLabs-Q2-2007.pdf> at 22 ("Professionalization among malware creators can be seen in the type of tools used and the way in which they are exchanged…. [S]ome competitors presently swap knowledge, tools and products.").

[39] Noah Schiffman, "Metamorphic malware sets new standard in antivirus evasion" *SearchSecurity.com* (8 February 2007), <http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1264968,00.html>.

[40] See, *e.g.*, Lisa Vaas, "Skype Worm Attacks Security Software" *e-Week.com* (11 September 2007), <http://www.eweek.com/c/a/Security/Skype-Worm-Attacks-Security-Software/ >.

[41] Gregg Keizer, "'Storm Trojan' ignites worm war" *Computerworld* (12 February 2007), <http://computerworld.com/action/article.do?command=viewArticleBasic&articleId=9011146&intsrc=hm_list>.

behaviour analysis model.[42] For this reason, Internet security specialists speak of a "blended threat":

> Blended threats combine the characteristics of viruses, worms, Trojan Horses, and malicious code with server and Internet vulnerabilities to initiate, transmit, and spread an attack. By using multiple methods and techniques, blended threats can rapidly spread and cause widespread damage. […]
>
> Effective protection from blended threats requires a comprehensive security solution that contains multiple layers of defense and response mechanisms.[43]

We will return to a consideration of the "blended threat" at the conclusion of Part I.

Digital Rights Management technologies (DRM) are "a system, comprising technological tools and a usage policy, that is designed to securely manage access to and use of digital information."[44] Because DRM systems respond to the instructions of content distributors and not the user, they interfere with the user's computing experience and so fall within the definition of "spyware". When they collect or use users' personal information, they also constitute a privacy threat.[45] Security flaws within DRM systems also render individuals vulnerable to third party attacks.[46]

Third parties may utilize spyware and malware in attacks motivated by commercial or criminal considerations, or in targeted attacks. Privacy threats originating with DRM, in contrast, should only arise in commercial settings as only commercial content distribution interests employ DRM.

b Rootkits, Hi-Jacking and Botnets

The Anti-Spyware Coalition defines a "rootkit" as

> A program that fraudulently gains or maintains administrator level access that may also execute in a manner that prevents detection.… Rootkit commands replace original system command to run malicious commands chosen by the attacker and to hide the presence of the Rootkit on the system by modifying the results returned by suppressing all evidence of the presence of the Rootkit. Rootkits are an extreme form of *System Modification Software*.[47]

---

[42] Alisa Shevchenko, Kaspersky Lab, "The evolution of technologies used to detect malicious code" <http://www.viruslist.com/analysis?pubid=204791972>.
[43] Symantec, *Glossary* <http://www.symantec.com/business/security_response/glossary.jsp>.
[44] Canadian Internet Policy & Public Interest Clinic, *Digital Rights Management and Consumer Privacy* (September 2007), <http://www.cippic.ca/uploads/CIPPIC_Report_DRM_and_Privacy.pdf >, at 4 [CIPPIC, *DRM & Privacy*].
[45] The most notorious such threat is that associated with the infamous "Sony rootkit": see Deirdre K. Mulligan and Aaron K. Perzanowski, "The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident" (2007) 22 *Berkeley Technology Law Journal* 1157 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1072229 > [Mulligan and Perzanowski, "The Magnificence of the Disaster"].
[46] See, *e.g.*, Elia Florio, Backdoor.Ryknos <http://www.symantec.com/security_response/writeup.jsp?docid=2005-111012-2048-99&tabid=1> (identifying malware that exploited vulnerability associated with Sony BMG's XCP copy protection software).
[47] ASC, Glossary, note 36, *supra*.

Sony BMG's XCP DRM merited the widespread criticism it received because it placed a rootkit on users' computers.[48]

The ASC defines a "hijacker" as:

> *System Modification Software* deployed without adequate notice, consent, or control to the user. Hijackers often unexpectedly alter browser settings, redirect Web searches and/or network requests to unintended sites, or replace Web content. Hijackers may also frustrate users' attempts to undo these changes, by restoring hijacked settings upon each system start. [49]

Combined with a rootkit, hijack software permits remote control of a user's computing resources. Pooled together into a network, called a "botnet", remotely controlled computers make for a formidable security threat.

The Congressional Research Service described botnets as follows:

> Botnets, or "Bot Networks," are made up of vast numbers of compromised computers that have been infected with malicious code, and can be remotely-controlled through commands sent via the Internet. Hundreds or thousands of these infected computers can operate in concert to disrupt or block Internet traffic for targeted victims, harvest information, or to distribute spam, viruses, or other malicious code. Botnets have been described as the "Swiss Army knives of the underground economy" because they are so versatile.[50]

These tools, used in concert, are indeed versatile. By conscripting the computing resources of individuals spread across the net, botnet controllers not only access computing resources to which they would not otherwise enjoy access,[51] they can mask their own location and activities. Botnets are routinely used for sending spam[52] and for conducting denial-of-service attacks.[53]

Vint Cerf, Google's Chief Internet Evangelist (and the "father of the Internet"), has estimated that as many as a quarter of the computers around the world have been conscripted into botnets.[54] Trade of botnets is lucrative and recognized as a form of organized crime. Botnet costs are low when compared to financial losses and damages caused to businesses and end users. Smaller botnets are priced between $1 and $40 per compromised PC. Botnets have realized revenues ranging from several hundreds of

---

[48] See "The Magnificence of the Disaster", note 45, *supra*.
[49] ASC, Glossary, note 36, *supra*.
[50] Clay Wilson, Congressional Research Services, "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress" (29 January 2008), <http://www.fas.org/sgp/crs/terror/RL32114.pdf >.
[51] The largest current botnet, that generated by the Storm worm, is estimated to control between 1 and 2 million PCs and have more computing power than IBM's BlueGene. "If you sat them down to play chess, the botnet would win," says Adam Swidler, a senior manager with security company Postini; see Sharon Gaudin, "Storm Worm Botnet More Powerful Than Top Supercomputers" *InformationWeek* (6 September 2007), <http://www.informationweek.com/news/showArticle.jhtml?articleID=201804528>.
[52] John Leyden, "Most spam comes from just six botnets" *The Register* (29 February 2008), <http://www.theregister.co.uk/2008/02/29/botnet_spam_deluge/>.
[53] Sharon Gaudin, "DoS Attack Feared As Storm Worm Siege Escalates" *InformationWeek* (2 August 2007), <http://www.informationweek.com/management/showArticle.jhtml?articleID=201202711>.
[54] Nate Anderson, "Vint Cerf: one quarter of all computers part of a botnet", (25 January 2007) ArtsTechnica <http://arstechnica.com/news.ars/post/20070125-8707.html>.

thousands of dollars to several million US$, and criminals in the underground world can charge $100/day to rent 1,000 bots. Botnets may be used to misappropriate personal information. In May, 2008, the security firm Finjan, Inc. reported discovery of a botnet server storing 1.4 gigabytes of information collected in less than a month and comprising thousands of log files, including 86 from Canadian sources. The data included intensely private data, including patient data, bank customer data, business-related email communications and captured Microsoft Outlook accounts containing email communications.[55]

Canada is estimated to host 15% of bot-infected computers in North America. In July of 2005, Toronto was the most bot-infected city in North America.[56] In February, 2008, Canadian law enforcement arrested 17 individuals alleged to have operated a series of botnets. Police allege that the gang inflicted $45 million in damages through botnets linking almost 150,000 computers in 100 different countries.[57]

c Keyloggers and Scrapers

The Anti-Spyware Coalition defines a keylogger as:

> Tracking Software that records keyboard and/or mouse activity. Keyloggers typically either store the recorded keystrokes for later retrieval or they transmit them to the remote process or person employing the keylogger. While there are some legitimate uses of keyloggers, but they are often used maliciously by attackers to surreptitiously track behavior to perform unwanted or unauthorized actions included but not limited to identity theft.[58]

The ASC defines a "screen scraper" as:

> *Tracking Software* that records images of activity on the screen. Screen Scrapers typically either store the recorded images and video for later retrieval or they transmit them to the remote process or person employing the Screen Scraper. There are some legitimate uses of screen scrapers, but they are often used maliciously by attackers to surreptitiously track behavior to perform unwanted or unauthorized actions that can include identity theft.[59]

Both tools have obvious applications in malicious online threats. These technologies have few applications in exchanges with consumers in legitimate commercial settings. However, such tools do have applications in secure internal environments (where, for example, maintenance of trade secrets is of paramount importance).

These tools are attractive, however, in settings where individuals have been targeted. Consider "Lover Spy", a keystroke logger that surreptitiously installed when a user opened an electronic greeting card. American authorities disapproved, charging Lover

---

[55] "Finjan Discovers Compromised Business & Customer Data of 40 Top-tier Global Businesses" (6 May, 2008) <http://www.finjan.com/Pressrelease.aspx?id=1944&PressLan=1819&lan=3>.
[56] Symantec, "Security Update - July 2005: Worldwide and Americas" (July 2005), <http://www.symantec.com/avcenter/reference/SSU_AMS_07_2005.pdf>.
[57] Tu Thanh Ha, "Ring invaded computers in 100 countries, police say", *The Globe and Mail* (21 February 2008).
[58] ASC, Glossary, note 36, *supra*.
[59] *Ibid*.

Spy's publisher with 35 counts of "manufacturing, sending and advertising a surreptitious interception device" and "unauthorized access to a computing device."[60]

3 Strategies

Having reviewed the medium and technological tools online threats require to carry out the attack, we now turn to the strategies employed by such threats for engaging targets. We have divided these strategies into two rough categories: security exploits – attacks that exploit technological vulnerabilities – and social engineering – attacks that exploit human vulnerabilities.

a Security Exploits

The ASC describes a "security exploit" as simply "A piece of software that takes advantage of a hole or vulnerability in a user's system to gain unauthorized access to the system."[61] Security exploits come in as many flavours as there are applications on the desktop – more, in fact, because a single application may have many, many security vulnerabilities that may emerge over time.

Perhaps the most notorious security exploit is the "ActiveX" installation that enabled "drive-by downloads" of spyware. ActiveX is a Microsoft technology that enables other programs to run within Microsoft's browser, Internet Explorer. Microsoft shipped early versions of Internet Explorer with ActiveX enabled by default. Malware distributors were able to secure installation merely by having the user browse to a website that hosted the malware.[62] The vulnerability was eliminated in later versions of Internet Explorer.

Most such vulnerabilities have to date been addressed by application of patches and security updates.[63] In a Web 2.0 world, however, patches cannot solve all problems. Ordinary citizens now host content managed websites and blogs that themselves feature security vulnerabilities.[64] Users are not yet accustomed to maintaining their own web applications. Similarly, vulnerabilities are being exploited in unusual sources. For example, a number of common web authoring tools that create Shockwave Flash files, such as Adobe's Dreamweaver and Acrobat, share a vulnerability that renders websites that host these Flash files vulnerable to attack.[65]

---

[60] Jeff Williams, "I Know What You Did Last Logon – Monitoring Software, Spyware and Privacy" <http://download.microsoft.com/download/9/9/f/99f9909d-1a67-451f-be55-24ca0ff27a41/I_Know_What_You_Did_Last_Logon.pdf>.

[61] ASC, "Glossary", note 36, *supra*.

[62] See, generally, Gregg Keizer, "Microsoft Hones IE 7's Drive-by-Download Defenses" *Information Week* (15 February 2006), <http://www.informationweek.com/news/showArticle.jhtml?articleID=180202473>.

[63] See, e.g., Microsoft's "Patch Tuesday" program, note 3, *supra*.

[64] See, e.g., Bill Brenner, "New attack methods target Web 2.0, VoIP" *Dark Reading* (17 October 2007), <http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1277386,00.html>; Matt Wirges and Mike Shema, "Securing Web Applications in the LAMP Environment" (23 August 2007), <www.penlug.org/twiki/pub/Home/MeetingAgenda20070823/penlug-presentation-23AUG07.pdf> (describing vulnerabilities in common open source website hosting utilities used in such Web 2.0 utilities as Joomla and WordPress).

[65] Rich Cannings, "XSS Vulnerabilities in Common Shockwave Flash Files" (2 January 2008), <http://docs.google.com/View?docid=ajfxntc4dmsq_14dt57ssdw&pli=1>.

b Behavioural Engineering

"Behavioural engineering", also called "social engineering", is a method of inducing desired behaviour in a target that relies on "smooth talking" or other manipulative behaviour.[66] In the context of online privacy threats, the key to the success of social engineering strategies lies in winning the confidence of the target and convincing them to go against their instincts or better judgment and reveal personal information.

Many of the online threats associated with traditional spam rely on social engineering strategies. For example, the "Nigerian scam", in which a third party offers a commission in return for one's assistance in transferring a large sum of money out of a jurisdiction, relies upon simple human greed and gullibility to succeed.[67] More recently, fraudsters have relied upon spam to set up social engineering attacks targeting personal information in the form of phishing and pharming attacks, which we discuss in detail below.

Spam is not the only medium by which fraudsters employ social engineering strategies to obtain victims' personal information. Trojan horses, defined by the Anti-Spyware Coalition as a "program that appears to do one thing but actually does another", take advantage of a target's needs and wants to deliver malware – be it spyware, a virus or worm, or some other malicious technology. For example, some rogue anti-spyware programs purport to offer consumers protection against spyware, but in fact themselves install potentially unwanted technology. Spy Blaster, one of the most notorious examples of such software, surreptitiously installed on users computers through a security exploit, additionally installed a separate tracking program, and initiated a range of unwanted behaviours on the victim's computer, including opening pop-up windows, hijacking the victim's browser, and opening the user's CD-ROM tray. The software then offered to sell the victim anti-spyware software by providing the victim with a message that read:

> FINAL WARNING!! If your cd-rom drive(s) open. . . You DESPERATELY NEED to rid your system of spyware pop-ups IMMEDIATELY! Spyware programmers can control your computer hardware if you failed to protect your computer right at this moment! Download Spy Wiper NOW![68]

The FTC shut this particular operation down in 2004, and obtained permanent injunctions against the defendants in 2006.[69]

4 Blended Threats

Although we have identified these platforms, tools and strategies separately, our discussion of each should demonstrate that these resources are being combined to achieve

---

[66] Wikipedia has an excellent discussion of the range of activities associated with social engineering scams: Wikipedia, "Social engineering (security)" <http://en.wikipedia.org/wiki/Social_engineering_(computer_security)>.

[67] See, *e.g.*, Royal Canadian Mounted Policy, "C" Division, "Nigerian Letter Scam" <http://www.rcmp-grc.gc.ca/qc/faq/nigeria_e.htm>.

[68] FTC, "FTC Cracks down On Spyware Operation" <http://www.ftc.gov/opa/2004/10/spyware.shtm >.

[69] See *Federal Trade Commission v. Seismic Entertainment Productions, Inc., SmartBot.net, Inc., and Sanford Wallace*, U.S. Dist. Ct., District of New Hampshire Civil Action No.: 1:04-CV-00377-JD (FTC File Nos.: 042 3142; X05 0013) <http://www.ftc.gov/os/caselist/0423142/0423142.shtm>.

attackers' aims. Attackers must conscript bots into a network, and need some form of backdoor, Trojan or rootkit to achieve that aim. That further requires some delivery mechanism – a socially engineered attack, security vulnerability, or an email – to access the user's PC. This multi-capability is being packaged into increasingly robust malware. Malware is becoming sophisticated not only in its delivery vectors, but also in its internal redundancy: if one angle of attack is not successful, the malware may be programmed to attempt alternative angles. This use of multiple attack vectors permits blended threats to multiply very quickly.[70]

C Privacy Invasive Behaviours

Having identified the tools used to threaten privacy online, we now turn to examine the behaviours that apply those tools. We divide these behaviours into three classes to match the differing motivations we identified earlier: (1) fraudulent behaviours, (2) commercially motivated behaviours, and (3) behaviours that target specific individuals (but without fraudulent intent).

1 Fraud

We have divided fraudulently motivated online privacy threats into two general classes, "identity fraud" – fraud that involves some degree of "impostering" – and fraud with purely financial motivations that lack any element of impostering. This division is mostly organizational – the line between identity fraud and other forms of fraud is hypothetical at best.

a Identity Fraud

We define "identity fraud," sometime called "identity theft", as the unauthorized collection, possession, transfer, replication or other manipulation of another person's personal information for the purpose of committing fraud or other crimes that involve the use of a false identity.[71]

Any number of the tools previously identified in this part may play a role in facilitating identity fraud. Malware, trojans, rootkits, backdoors and remote access technologies allow third parties access to users' computers which permits the unauthorized collection of personal information. In this part of the Report, we would like to focus on two social engineering techniques that pose particular problems for consumers: phishing and pharming.

i Phishing

Phishing is a technique for collecting personal information of individuals that combines technological tools with social engineering. Typically, a phishing attack masquerades as a trustworthy organization, such as a financial institution or post-secondary education institution, in an e-mail message or instant messaging communication. The message lures

[70] McAfee, "White Paper – A Brief History of Malware: An Educational Note for Service Providers" (2005), <http://www.mcafee.com/us/local_content/white_papers/partners/ds_wp_telconote.pdf>.
[71] Canadian Internet Policy & Public Interest Clinic, "FAQ: Identity Theft", <http://www.cippic.ca/identity-theft-2/>.

the victim into providing personal information, such as financial account data, to the attacker.[72] Typically, phishers will create an unauthorized replica ("spoof") of a website and institutional email, usually from a financial institution or another organization that deals with financial or other sensitive information. The email uses logos and slogans of legitimate organization. The spoofed email is sent to as many as possible to lure them into the scheme. The email redirects the user to the spoofed website which appears to belong to the organization.

Phishing schemes typically rely on three elements: (1) corporate trademarks and trade names or recognized institutional names and logos, (2) warnings intended to cause users immediate concerns, and (3) the spoofing of "authentication" signifiers. We'll consider each in turn.

First, by reproducing trade-marks and brand names, phishers play off brand recognition and trusted relationships. The phisher may also spoof the look and feel of the target organization's website, and other indicators of validity and security of a website

Second, phishing messages typically offer a warning to create a sense of urgency, such as a warning that failure to respond may lead to account termination, penalties or fees, or other negative outcomes. Sometimes the attacker "offers" a prize or incentive for response. Fear caused by these warnings further clouds judgment of the consumer to determine whether the message is authentic.

Phishing message can also play off of other emotions. Disaster relief emails from phishers are becoming common. Such attacks lead the user to a website that appears to belong to a genuine charity and ask for a donation by credit card. For example, following Hurricane Katrina, phishers posing as the Red Cross sought contributions to aid in rebuilding.[73] Other schemes to convince the user to provide information include:

- An announcement that an online service provider is introducing a security upgrade to increase customer security and protect from fraud. Users are told to log in to the service provider's site and provide authentication information in order to activate and enrol in a new and improved security scheme.
- A notice that one's account information is incomplete or out-of-date, and that it must be updated to maintain service. Users are asked to log in and update their information to ensure their accounts are not cancelled or suspended.
- An email thanking the user for updating their account information at an online service provider website. The email warns that if the user did not initiate the account update, they should follow the link to the website and log in to report the fraudulent activity. The user will follow the hyperlink because they did not previously update their information with the service provider. A similar method involves sending the user an email with an invoice for merchandise with a link to "cancel" the fake order. The user then provides the scammer with credit card information so that the unauthorized transaction can be "cancelled".

---

[72] Canadian Internet Policy & Public Interest Clinic, "Techniques of Identity Theft" (March 2007) at 13, <http://www.cippic.ca/documents/bulletins/Techniques.pdf>.

[73] "Online fraudsters phish for American Red Cross donators, Sophos reports" (5 September, 2005) <http://www.sophos.com/pressoffice/news/articles/2005/09/sa_redcrossphish.html>.

Phishing lures are becoming more contextually aware of their targeted victims. Phishing attempts that target individuals based on context are referred to as "spear phishing".

Third, phishers are spoofing methods for authentication in increasingly sophisticated ways. For example:

- Email spoofing: email address from which spammed email appears to come from is spoofed, making the apparent sender of the email appear to be different from the actual sender's identity.
- The URL presented in the email lure and fraudulent website hook appear official and legitimate.
- Link manipulation permits phishers to employ clever website URLs. Phishers may make a link in an email appear to belong to spoofed organization. This may be through misspelled URLs (*e.g.*, substitution of the number "1" for the letter "l", often called a "homograph attack") or use of subdomains (*e.g.* http://www.yourbank.com.example.com, sometimes called a "cousin domain attack"). Phishers may also use the "@" symbol (*e.g.* http://www.google.com@members.tripod.com).
- Phishers may register domain names that have appearance similar to that of the targeted legitimate site name and use these URLs for phishing sites. Fake or stolen identities are generally used to register domain names used in phishing attacks.
- Phishers may use JavaScript commands to alter the address bar by placing a picture of a legitimate URL over the address bar or by closing the original address bar and opening a new one displaying a legitimate URL.
- Websites look and feel is simple to duplicate. Using simple CSS and HTML, an attacker can reconstruct the bare window's interface and split the screenshot of the browser's navigational tools so they can add a "live" address bar to the simulation by using absolutely positioned text input. CSS allows the attacker to add roll-over to navigation buttons and give the "live" feel because of the visual indication that roll-over supplies. CSS can also be used to mock up hierarchical menus at the top of the screen (standard Windows menu). Similarly, JavaScript may make the interface functional, such that the fake address bar appears as though it is updating the page as per the user-entered URL. JavaScript can also be used to create navigation buttons that cause forward and backward navigation and create menus (though they will not be truly functional). The JavaScript can detect the user's browser type and operating system and spoof the user's browser's appropriate graphic style. Keyboard event listeners can be installed to "ctrl" and "alt" keys and emulate keyboard shortcuts.

Phishing has become a commoditized phenomenon. Kits are available for sale in black market internet sites, including more sophisticated "Man-in-the-Middle" phishing kits.[74] Kits substantially lower the time a phisher needs to launch an attack. Phishers do not need to be technically sophisticated. Phishing offers potentially high rewards with low associated risks and increasingly smaller degrees of technical skill are necessary to

[74] John Leyden, "Man-in-the-Middle phishing kit netted", The Register (12 January, 2007) <http://www.theregister.co.uk/2007/01/12/phishing_kit/>.

launch attacks. The social engineering techniques used in phishing are now being applied to other context. Phone phishing, or "vishing", User receives email message claiming to be from bank, telling them to dial a phone number regarding problems with their bank account. When user dials the number (which is owned by a phisher and provided by Voice over IP service), the user is prompted to enter their account number and PIN. Alternately, consumers are called directly and told to call their customer service number to protect their account. Sometimes the phishers use fake caller ID data to give the appearance that the call comes from a trusted organization.

Phishing has been identified by the Binational Working Group on Cross-Border Mass Marketing Fraud as one of the rapidly growing classes of identity fraud scams on the internet that is causing short term losses and long term economic damage.[75] In 2004, Financial Insights reported that global financial institutions experienced more than $400M in fraud losses from phishing. A U.S. Gartner survey reported that phishing attacks grew at double-digit rates in 2004. In the 12 months ending May 2005, 73 million U.S. adult internet users said they believed they had received an average of more than 50 phishing emails in the past year. Symantec Internet Security Threat Report for September 2006 (detailing 1 January to 30 June 2006): total of 157,477 phishing messages detected, which represents an 81% increase over 86,906 unique phishing messages detected 30 July to 31 December 2005, and a 612% increase over 97,592 unique phishing messages detected in the first six months of 2005.

Canada is not immune to phishing harms. An AOL Canada Study found that nearly 1 of 3 Canadians surveyed received email from a company seeking confirmation of account information. The Anti-Phishing Working Group's May, 2007 Phishing Activity Trends Report found that Canada hosts 3.29% of the world's phishing websites. In June 2004, the Royal Bank of Canada notified customers that fraudulent emails purporting to originate from Royal Bank was asking customers to verify account numbers and PINs through a link provided in the email. The email stated that if the user did not click on the link and enter account information, access to their account would be blocked. Emails were sent within a week of a Royal Bank computer malfunction that prevented customer accounts from being updated. The Royal Bank believes that the phishers were taking advantage of the situation.

Social networking sites are a treasure trove of useful contextual data on its users, such as what is known about who they know. This makes them useful to phishers, who can exploit friend relationships to boost their credibility in an attack. Phishers may use web crawlers and screen scrapers to compile profile information and friend relationships in order to data-mine from social networking sites. Consumer groups warn that fraudsters can use personal information to trick people into revealing PIN numbers and other security information or use personal information collected from social networking sites to apply for credit cards or loans in somebody else's name.[76] Personal information is particularly useful for attacks that spoof particular groups, such as work or friend

---

[75] Binational Working Group on Cross-Border Mass Marketing Fraud, *Report on Phishing* (October 2006) at 7 <http://www.usdoj.gov/opa/report_on_phishing.pdf>.

[76] "Millions vulnerable to identity theft" *Finance Markets* (22 February 2008), <http://www.financemarkets.co.uk/2008/02/22/millions-vulnerable-to-identity-theft/>.

groups.[77] The University of Indiana carried out controlled phishing attacks in 2005, targeting students who left their contact information on social networking sites. They found that when users were contacted by somebody they believed might know them, they were far more likely to provide personal details.[78] MessageLabs warns that spammers and virus-writers set up false profiles and trawl through social networking sites to piece together job titles, phone numbers, and email addresses, compiling information to launch sophisticated, highly targeted attacks on corporate networks.[79] A worm attack in 2006 hijacked MySpace pages, exploiting vulnerabilities in Java support for Apple's Quicktime software to alter legitimate links on the user's MySpace profile to direct users to phishing websites.[80] The Google Security team reported that 95% of new phishing traffic targeted MySpace pages in March 2007.[81]

VeriSign's iDefense security experts warned that the Facebook platform is turning into a prime attack vector for cybercriminals, stating: "The potential is there, and the framework is there."[82] As an example, the team pulled one user's name from Facebook, and within fifteen minutes of doing Google searches, they were able to collect enough information to steal her identity. **S**ecurity vendor Sophos conducted an experiment by creating a fake Facebook account under the name "Freddi Staur" (an anagram for "ID Fraudster"). Freddi randomly selected 200 Facebook users and added them as friends. Of the 200 Facebook users contacted, 87 users accepted Freddi as a friend. 82 of these users gave Freddi access to personal information on their profile. According to the Sophos report, 72% of the respondents divulged one or more email address, 84% of respondents listed their full date of birth, 87% of respondents listed their current address or location, 23% of respondents listed their current phone number, and 26% of respondents provided their instant messaging screenname. In the majority of cases, Freddi was able to gain access to the respondent's photos of family and friends, information about their preferences, hobbies, employer details, and other personal facts such as the names of their spouse or partner and a complete resume. In one instance, Freddi learned the user's mother's maiden name.[83] With all of these details, Freddi was in a position to create phishing emails targeting these users.

---

[77] "Targeted e-mail attacks spoof DOJ, business group" *CNET News* (20 November 2007), <http://www.news.com/Targeted-e-mail-attacks-spoof-DOJ%2C-business-group/2100-7349_3-6219559.html?tag=item>.

[78] "Identity theft: six clicks from a cyber crook" *Telegraph.co.uk* (29 February 2008), <http://www.telegraph.co.uk/connected/main.jhtml?xml=/connected/2008/03/01/dlcrooks129.xml>.

[79] MessageLabs, "Social Networking: Brave New World or Revolution From Hell? A look at the phenomenon of Social Networking and the implications for Business" (White Paper 2007), <http://whitepapers.zdnet.com/whitepaper.aspx?docid=337546> at p. 1.

[80] Websense Security Labs, "Malicious Website / Malicious Code: MySpace XSS QuickTime Worm" Websense Security Labs Alerts (1 December 2006), <http://www.websense.com/securitylabs/alerts/alert.php?AlertID=708 >.

[81] Colin Whittaker, "Thwarting a large-scale phishing attack" Google Online Security Blog (11 June 2007) <http://googleonlinesecurity.blogspot.com/2007/06/thwarting-large-scale-phishing-attack.html>.

[82] "Facebook users open to cyberattacks, ID theft?" *CNET News* (30 July 2007), <http://www.news.com/Facebook-users-open-to-cyberattacks%2C-ID-theft/2100-1029_3-6199559.html?tag=st.nl>.

[83] "Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves" *Sophos* (14 August 2007), <http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html>.

But these fears are not merely hypothetical: in January 2008, Moroccan authorities arrested Fouad Mourtada for "villainous practices" linked to the identity theft of Prince Moulay Rachid, the brother of King Mohammed VI and second in line to the throne. Mourtada allegedly posted a fake profile of the prince on Facebook.[84]

ii Pharming

Pharming is any form of phishing that interferes with the integrity of the lookup process for a domain name.[85] Pharming attacks are also known as "Hostname Lookup Attacks", since these attacks interfere with the integrity of the process for looking up the numeric IP address associated with a domain name. When establishing a connection with a remote computer such as web server belonging to bank or target, hostname lookup is normally performed to translate a domain name such as "bank.com" to numeric IP address such as "198.81.129.100". The conversion of human friendly server names (e.g. www.bank.com) to IP addresses for routing packets is completed through the Domain Name System (DNS). Pharming exploits vulnerabilities in how computers use DNS information to enable the attacker to redirect website traffic to another website run by the attacker. Pharming has the ability to bypass many traditional phishing attack prevention tools and thus may potentially affect a larger segment of an organization's customer base.

Pharming attacks may target vulnerabilities in DNS servers. However, the more common attack is to exploit vulnerabilities in the user's computer. One technique, called "host file poisoning", involves modifying a user computer's local host file, which is used by the computer to see whether the domain or host name is known to the local machine with a predetermined address before consulting DNS. If the domain or host name appears in the host file, the corresponding address will be used without regard to the DNS query for domain. The host file can be modified so that "bank.com" can be made to refer to a malicious address such that the user will see a legitimate looking site and the user will enter confidential information which goes to the attacker. Another local attack involves modifying the system configuration files of the victim's computer to change the DNS server to a malicious server controlled by the attacker. When user navigates to correctly named site, malicious server will send the user to a fraudulent site where confidential information is collected. A third technique, called "DNS cache poisoning", involves "polluting" the user's DNS cache with incorrect information that will be used to direct the user to the incorrect location. The user can misconfigure the DNS cache by providing incorrect information. This can also be done by hacking a legitimate DNS server or by polluting the cache of a misconfigured legitimate DNS server.[86]

These are not simply theoretical exploits. In March 2005, using a rogue DNS server posing as an authoritative DNS server for a particular .com domain, pharmers were able to poison several ISP-level DNS servers and requests for more than 900 unique internet

---

[84] "Moroccan held for alleged royal ID theft through faked profile on Facebook*" The Canadian Press* (11 February 2008), <http://canadianpress.google.com/article/ALeqM5jjIkIKnCJ2iJbUWIq9K0qast0AZQ>.
[85] The US Department of Homeland Security, SRI International Identity Theft Technology Council and the Anti-Phishing Working Group, "The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond" (October, 2006) <http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf>.
[86] *Ibid*. at 11-12.

addresses. More than 75,000 email addresses were redirected.[87] Significant companies have been targeted by pharmers. In 2004, a German teenager hijacked the eBay.de domain name.[88] In January 2005, the domain name for a large New York ISP (Panix) was hijacked to a site in Australia.[89]

b Other forms of Fraud

Online environments are enabling other forms of fraud besides identity fraud. We address two of them that have privacy implications: credit card theft, and asset theft.

i Credit Card Theft

Simple credit card theft is among the most common online crimes. Credit card numbers are among the most highly targeted items of personal information in identity fraud attacks. Many of the tools we have identified in our review of the "tools of the trade" may be employed in attacks seeking credit card numbers.

Stolen credit card numbers are openly shopped on black market websites and chatrooms.[90] In 2007, Symantec reported that 86 percent of the credit card information sold in the online black market originated with US banks, and one percent of came from Canadian banks. Interestingly, Symantec reported that UK cards were worth roughly twice the value of an American card: between $1 and $6 for a US card compared with $2 to $12 for a UK card.[91]

ii Account Hijacking

Account hijacking is another harmful behaviour sometimes associated with identity fraud. Account hijacking occurs when a third party gains unauthorized access to a user's service account. The unauthorized access may occur through a phishing attack, use by someone close to the victim or who is able to find out his or her password, or some other illicit tactic.

The nature of the intended fraud depends upon the nature of the account. A hijacked email account – such as GMail – permits the rogue to pose as the user. A hijacked PayPal or eBay account permits theft or fraud. Consider the following warning, posted by an eBay seller:

> The first hint I had that my ebay account had been hijacked was a message from ebay saying they had closed the 147 auctions I listed that week beacause [*sic*] of suspicious activity with my account. I was furious. A weeks worth of work - completely gone.

---

[87] Paul Roberts, "Pharming Attacks Target the Web" *PCWorld* (1 April, 2005) <http://www.pcworld.com/article/id,120268-page,1/article.html>.
[88] Martin Fiutak, "Teenager admits eBay domain hijack", *CNET News* (8 September, 2004) <http://www.news.com/Teenager-admits-eBay-domain-hijack/2100-1029_3-5355785.html>.
[89] Slashdot, "New York's Oldest ISP Gets Domain-Jacked" (16 January, 2005) <http://it.slashdot.org/it/05/01/16/0027213.shtml?tid=95&tid=172&tid=17>.
[90] Matt Richtel, "Credit Card Theft Is Thriving Online As Global Market" *New York Times* (13 May 2002) <http://query.nytimes.com/gst/fullpage.html?res=9f06eed61739f930a25756c0a9649c8b63>.
[91] Jacqui Cheng, "'I'll take a stolen ID and a small fry.' 'That'll be $14.'" *Arts Technica* (19 March 2007) <http://arstechnica.com/news.ars/post/20070319-ill-take-a-stolen-id-and-a-small-fry-thatll-be-14.html>.

> What really made me mad was - I didn't see anything out of the ordinary. I could still access my account. And, all 8000 of my store auctions were still there. Just the ones listed in the last few days were closed down by ebay. The truth is: None of it made sense. My account still worked, and I could still access everything. Still - Just to be safe, I followed ebay's [*sic*] advice, and changed the password on my email. Then I changed the password on my ebay account. That protected things for now.
>
> Next, I carefully checked my individual listings. And, that's where the trouble was. Mixed among my normal listings were listings for a travel trailer, and several laptop pc's. Definitely not my listings. I cancelled them as I came across them, and began to be much happier with ebay's [*sic*] fraud detection team. What a mess it would have been if those items had sold.
>
> I still have no idea how my account was breached. I am the only one who has the password to my email and ebay account. My network is protected, and I run a firewall.[92]

Account hijacking is of great concern to financial institutions. A 2004 study published by the Federal Deposit Insurance Corporation estimated that almost 2 million American Internet users experienced unauthorized access to a chequing account during the year ending April 2004.[93]

2 Personal Attacks on Privacy

a Cyberstalking

Cyberstalking is one of the most widespread and overlapping forms of personal online harassment. A simple definition of cyberstalking is: "…the use of electronic communication… emails and the internet… to bully, threaten, harass, and intimidate a victim."[94] Cyberstalking can be perpetuated through email, online websites, social networking sites, message forums, and online gaming. Harassment is defined as any behaviour that causes the victim distress, whether intentional or not.

Harassing cyberstalking behaviour can be direct or indirect.[95] Direct harassment includes: transmitting offensive email messages to a victim, making threats, abusing the victim

---

[92] "Scams Phishing Fraud Eabay [*sic*] & Paypal Account Hijacking", Guide ID: 10000000003156811 (8 March 2007), <http://reviews.ebay.com/Scams-Phishing-Fraud-Eabay-amp-Paypal-Account-Hijacking_W0QQugidZ10000000003156811>.

[93] Federal Deposit Insurance Corporation, "Putting an End to Account-Hijacking Identity Theft" <http://www.fdic.gov/consumers/consumer/idtheftstudy/>.

[94] Randy McCall, "Defining Online Harassment and Cyberstalking", in *Online Harassment and Cyberstalking: Victim Access to Crisis, Referral and Support Services in Canada Concepts and Recommendations* (October 5, 2003), p. 3, <http://www.vaonline.org/Cyberstalking%20Concepts%20and%20Recommendations%20(e).pdf> ["Online Harassment and Cyberstalking"]. "Electronic communication" devices identified by McCall include "pagers, cell phones, emails and the internet". Note that stalking behaviour perpetuated online often transmits to other communication mediums. Indirect forms of online personal harassment, such as the online defamation of character, are considered to be "cyberbullying", if perpetuated by a minor; however, if an adult undertakes the same behaviour, it is considered to be cyberstalking, proper. See Netlingo, "Cyberbullying", <http://www.netlingo.com/lookup.cfm?term=cyberbullying>.

[95] *Ibid*., at 3.

through pornographic or offensive materials, transmitting a virus, or damaging the victim's data or equipment. Indirect harassment includes: false accusations of harming reputation, false victimization, attempts to gather information about the victim (advertise for information about individual over the internet), impersonating the victim, encouraging others to take part in harassment of the victim, and ordering embarrassing goods or services on behalf of the victim.

LoverSpy offers a paradigmatic case of direct cyberstalking. LoverSpy was a program created by a San Diego developer, Carlos Enrique Perez-Melara, to infiltrate, monitor, and manipulate the activities of remotely located computers.[96] A cyberstalker used LoverSpy by sending a victim an email accompanied by a seemingly friendly image or movie attachment. As the victim opened the email and its attachment, LoverSpy would covertly download itself onto the victim's computer. Once installed, LoverSpy could, at the direction of the remote cyberstalker, record the victim's keystrokes, display to the stalker web pages, web-page history, and emails of the victim, or act upon the victim's computer, downloading viruses or turning on the webcam. As LoverSpy's use was explicitly nefarious, on August 26, 2005, the San Diego Department of Justice Indicted Mr. Perez, and four others, on a number of charges, related to the program LoverSpy.[97] Among the charges was the "Unauthorized Access to Protected Computers for Financial Gain" and the "[Unlawful] Intercepting [of] Electronic Communications".[98]

Direct cyberstalking can also be much more subtle, either involving software that is not commercially available or involving software that is more legitimate in its application.[99]

Social networking sites provide an example of online applications, with otherwise legitimate purposes, that can be used to facilitate direct and indirect cyberstalking.[100] Social networking sites are vulnerable to abuse by cyberstalkers because of the ease with which the sites enable subscribers, and sometimes non-subscribers, to access large amounts of personal information, usually voluntarily posted by a victim on its "profile". A cyberstalker may use social networking sites to follow a victim's actions, gain contact information, or to enact abuse on the person's identity. In February, 2008, a 20-year-old male was charged with "aggravated cyber-stalking" for uttering threats and posting explicit images, designed to "create fear and embarrassment", on his ex-girlfriend's MySpace profile.[101] Social networks are designed, at least in part, with an eye towards

---

[96] Department of Justice, "Creator and Four Users of Loverspy Spyware Program Indicted" (August 26, 2005), <http://www.justice.gov/criminal/cybercrime/perezIndict.htm>.
[97] *Ibid*.
[98] *Ibid*.
[99] The former category includes freely exchanged software, or software the cyberstalker created. The latter category includes legitimate monitoring software, such as Spectorsoft (http://www.spectorsoft.com/), which, although well intentioned, could be used maliciously. For example, this Yahoo! Q&A forum, accessed April 10, 2008, suggests using SpectorSoft to find out if your boyfriend or girlfriend is cheating on you: Yahoo!, "Resolved Question; How can i be sure my partner is cheating on me?", *Yahoo! Answers*, <http://sg.answers.yahoo.com/question/index?qid=20060710041310AAWeRda>.
[100] There are many other types of online applications that can be used for cyberstalking. Search engines are a commonly used application. As well, forums and message boards are quickly becoming a source of online harassment.
[101] Wftv.com , "20-Year-Old Accused Of Using MySpace For Cyber-Stalking" (February 21, 2008), <http://www.wftv.com/news/15369433/detail.html>.

behaviour that is self-consciously stalker-like, in the sense that social networking sites typically facilitate monitoring behaviour (albeit consensual monitoring behaviour).[102] This ambiguity makes regulation difficult, as it is sometimes difficult to distinguish stalking from innocent participation within the parameters of the rules of the social networking site.[103]

Online gaming provides a new and emerging form of cyberstalking.[104] Hostile game players can carry out a wide range of harassing activities, such as forming alliances, spying, sabotage, bartering, and negotiating treaties. These games allow cyberstalkers to group together to victimize another player and make it impossible for the victim to play the game. Groups may insult or threaten the victim while playing the game, sending threats or offensive messages to the victim. This behaviour may carry over outside of the gaming environment onto websites, blogs, message boards, and elsewhere.

It is difficult to ascertain the exact scope of cyberstalking.[105] This is partly due to the relative modernity of the Internet and the pace at which governments and industry respond to evolving environments. It is also due to the nature of the Internet, which allows cyberstalkers to move relatively anonymously, and in stealth.[106] What is certain is that cyberstalking is widespread and is very traumatizing to its victims. The consensus is that there is "little-to-no difference in the effect of being stalked/harassed on- or offline."[107]

---

[102] This is to say that "stalking" is a term used to describe many unthreatening behaviours facilitated, and usually encouraged, by social networking sites. See Dubow, Byron "Confessions of 'Facebook stalkers'" *USA TODAY* (March 8, 2007) <http://www.usatoday.com/tech/webguide/internetlife/2007-03-07-facebook-stalking_N.htm>; Urban Dictionary, "Facebook Stalking" (December 27, 2005; December 11, 2007) <http://www.urbandictionary.com/define.php?term=facebook+stalking>.

[103] Sometimes, the fact that a victim suffered harassment does not sufficiently prove that the perpetrator was cyberstalking. See BBC.co.uk., "Man cleared of Facebook stalking" (Wednesday, 26 March 2008), <http://news.bbc.co.uk/2/hi/uk_news/england/west_midlands/7315635.stm>.

[104] Catherine Donaldson-Evans, "Online Game Meetings Sometimes End Tragically, but Phenomenon Remains Rare", *Fox News* (December 10, 2007). <http://www.foxnews.com/story/0,2933,316333,00.html>.

[105] There are no authoritative statistics available, and the statistics that are available are either extremely selective or speculative. For example, Who@ provides statistics on Cyberstalking victims, but their statistics only concern people who have contacted them, and who they have helped. Their statistics show that they have aided, in one way or another, 2036 people since the year 2000. Who@'s figures are highest in 2005 and 2006. See Who@. "Online Harassment/Cyberstalking Statistics" <http://haltabuse.org/resources/stats/Cumulative2000-2006.pdf>. Conversely, a Canadian report, written by Victim Assistance Online Resources, speculates (by conjectural use of available statistics on stalking and internet use in Canada) that the real number of cyberstalking is closer to 100,000 people, in Canada alone. See Randy McCall, "Online Harassment and Cyberstalking Statistics in Canada" in *Online Harassment and Cyberstalking*, *supra* note 94, p. 12.

[106] One of the greatest difficulties facing victims of cyberstalking is the anonymity of their harasser. Sometimes, the victim is not sure who got their information, where they got it from, or how they got it. See Tom Zeller Jr., "A Sinister Web Entraps Victims of Cyberstalkers*" New York Time* (April 17, 2006), < http://www.nytimes.com/2006/04/17/technology/17stalk.html>.

[107] Randy McCall, "Why Crisis Intervention and Long Term Support are Important", in *Online Harassment and Cyberstalking*, *supra* note 94, p. 10, <http://www.vaonline.org/Cyberstalking%20Concepts%20and%20Recommendations%20(e).pdf>.

3 Commerce

Legitimate businesses also pressure internet users' privacy interests. We'll address four areas in which consumers face privacy concerns due to activities in the marketplace: (1) direct advertising through spam, (2) advertising through adware, (3) behavioural marketing, and (4) enforcement of rights in content through privacy-invasive digital rights management technologies.

a Spam

Spam may well have been the first significant online privacy threats consumers faced. Email was perhaps the first widely used online communications tool. Everyone owned an email address; at the turn of the century, it seemed that everyone had a spam problem, as well. However, the volume of spam, and ingenuity of spammers, has taken spam from a personal nuisance to a public concern. Spam taxes economic and personal productivity and impedes the efficient use of ISP and personal computing resources. Unchecked, spam will undermine e-commerce by undermining trust in internet communications. From a privacy perspective, spam amounts to the unauthorized collection and use of private contact information. Spam can invade our personal space.

Spam is unsolicited email. While spam is a tool for identity thieves, phishers, malware distributors and other fraudsters, it is also a tool for marketers. It is estimated that unsolicited email comprised 90% of all email sent in 2007[108] – up from 50% in 2003 and only 10% in 2000.[109] Unsolicited commercial email spans everything from pharmaceuticals to directories. The economics of spam provide a strong incentive to spammers to continue the behaviour. The cost of distributing spam is negligible; accordingly, it only takes a tiny number of email views make the venture worthwhile.

Where do spammers obtain their email lists? There are a number of resources. First, businesses may collect email for certain purposes – say, for completing an online purpose, or setting up an account with an ecommerce vendor – and put that information to use for marketing purposes. Second, companies can acquire email addresses from business partners through marketing agreements. Third, spammers may acquire lists of email addresses from third parties tat traffic in such data. Finally, businesses can build such lists themselves – either for their own use or to sell to third parties – through a variety of mechanisms. Some of these mechanisms include strategies for guessing email addresses from particular email domains – such as gmail.com or hotmail.com – and email harvesting software for finding email addresses posted on public websites.

b Adware

Adware is software that automatically displays downloads advertising material to computers users in a manner that is often unexpected or unwanted by computer users. Adware may sometimes employ tracking functions and collect information about computer users to assist in the compilation of personal profiles. Adware may collect information about websites that internet users visit and monitor how users use their

[108] Need cite.
[109] Industry Canada, "An Anti-Spam Action Plan for Canada" (May 2004) [Industry Canada, "Anti-Spam Action Plan"].

computers and what they do at the websites in order to target their advertising more effectively. When they do so in unwanted ways, or without the user's knowledge and consent, adware becomes an online threat to privacy.

Adware that engages in tracking behaviour typically reports back to a central server and stores information in databases. The information is analyzed and used to select the types of advertisements to display to users. Adware publishers can tie personally identifiable information to specific individual users – the publisher is not limited to anonymous usage statistics. This is necessary to ensure that data is collected only once for each user.

Not all adware is a privacy threat. When offered to consumers as a value proposition – say, in return for free software – adware can function as a valuable distribution mechanism. The key is in the content of the proposition. Installed without adequate and effective notice or user consent, adware falls to the level of potentially unwanted technology.[110] The most notorious forms of adware annoy consumers by opening multiple browser windows and displaying pop-up advertisements. From a privacy perspective, adware may be objectionable when it engages in tracking behaviour without user notice or consent.

For a period of time, adware was threatening to reach epidemic proportions. In 2005, Symantec performed an experiment, connecting a brand new computer without security software to the internet and browsing websites directed at children. Within an hour, 359 pieces of adware were found.[111] In 2005, Trend Micro conducted a survey of 500 IT managers found that 95% of companies frequently find adware in their organization. The majority of survey respondents ranked spyware among the top 3 IT priorities for 2005.[112] While a problem for businesses, adware typically targets consumers, not businesses. The most prolific distributors of adware are star/celebrity sites (16.3%), free screensaver sites (11.5%), adult sites (11.4%), and game sites (5.6%). McAfee's SiteAdvisor.com survey found that 97% of internet users could not differentiate between safe and unsafe sites, and the vast majority of users were just one click away from downloading spyware, adware, and other potentially unwanted software.[113]

c Behavioural Marketing

Behavioural targeted marketing is marketing based upon the study of the behaviours, preferences and decisions we all express while acting in the role of consumers.[114]

---

[110] For this reason, the Anti-Spyware Coalition classifies *nuisance* adware – those installed without adequate notice or consent – as potentially unwanted technology. See ASC Glossary, note 36 *supra*.
[111] Symantec, "Internet Security Threat Report", Vol X (September 2006) <http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf > [Symantec, "Internet Security Threat Report"].
[112] Trend Micro, "Threat Management: Challenges and Solutions, Web Threats" (White Paper, February 2007) < http://www.trendmicro.com/NR/rdonlyres/75541153-BFB6-4540-8E12-FD4051DCB28D/22391/WP03_Webthreats070223EU.pdf >.
[113] McAfee, "Adware and Spyware: Unraveling the Financial Web" (2006) <http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_adware.pdf >.
[114] Canadian Internet Policy and Public Interest Clinic, "On the Data Trail: How detailed information about you gets into the hands of organizations with whom you have no relationship" (April 2006) <http://www.cippic.ca/documents/May1-06/DatabrokerReport.pdf >.

Businesses collect this data for their own purposes; however, a support industry has sprung up to support this trade. This industry includes companies that specialize in list management and brokerage, geo-demographic population profiling, database management and analysis, individual consumer profiling, survey-based data-gathering, and multi-source data mining.[115]

The internet offers marketers an unprecedented opportunity to collect data about consumer behaviour, and marketers have designed a number of tools that facilitate these activities. Two that we will address are (1) tracking tools such as cookies and web bugs, and (2) social networking sites.

Cookies are bits of information that a distant party places on the computer of an internet user. Cookies may be temporary, enduring only for the browsing session, or persistent, enduring past the current browsing session, and potentially enduring for years. Google made international headlines in 2007 when it changed the default period of its persistent cookie to 2 years from 50 years. This kind of long range tracking of users raises significant privacy concerns. Persistent cookies may also track – following users around as the user browses other sites on the net. Such tools – called "tracking cookies" – also raise significant privacy concerns.[116] Cookies may also be first party – set by the entity whose website the user browses – or third party – set by a third party to whom the website's proprietor has some relationship. That relationship is usually a marketing relationship. Other tracking tools include the "web bug" – also known as a "gif bug", "pixel tag" or "web beacon" – a visual object embedded in a web page or e-mail that permits a third party to assess whether or not a user has viewed a webpage or e-mail. The object can be a transparent image, or a single pixel, and so invisible to the user.[117]

Both cookies and web bugs permit third parties to gather information about consumers' web surfing activities. This can be tremendously personal information. Third parties can then gather this information, put it together with other information if they choose and sell the information to third parties to conduct increasingly particularized research. Sometimes marketers characterize this data as "anonymous"; however, the information our web browsers provide third parties over the internet permits us to be identified by, at the least, internet protocol addresses, or IP addresses. An IP address is a unique number comprising four numbers (each between zero and 255) separated by periods (*e.g.*, 120.0.54.19). Internet service providers assign each computer a unique IP address while it is connected to the internet. Since ISPs assign IP addresses dynamically, meaning the address may be different each time the computer connects to the internet. Other ISPs assign static ISP addresses, meaning the IP address persists. Since most ISPs maintain network logs, specific IP addresses may, under certain circumstances, be traced back to the account holder.[118] Indeed, the Office of the Privacy Commissioner of Canada has found that IP addresses constitute "personal information" under Canadian privacy

[115] *Ibid*. at 2.
[116] The ASC has identified tracking cookies as potentially unwanted technology: ASC, "Definitions and Supporting Documents", note 35 *supra*.
[117] CIPPIC, *DRM & Privacy*, *supra* note 44 at 39 (citing Wikipedia,'s definition of a "web bug" <http://en.wikipedia.org/wiki/Web_bug>).
[118] CIPPIC, *DRM & Privacy*, supra note 44 at 6-7.

laws.[119] Further, even where IP addresses are not recorded or otherwise tracked, the combination of relatively small amounts of anonymous information can permit a third party to identify individuals. Accordingly, the tracking of usage habits associated with "anonymous" data in fact raises significant privacy concerns.[120]

These tools accordingly provide online marketers with a tremendously rich body of personal information. With adequate notice and effective user consent, such the collection, use and disclosure of such data may not raise privacy concerns – or, to the extent that they do, the risks associated with such activity may be consciously weighed against the benefits offered. However, notice is often inadequate, and consent ineffective. Web tracking behaviours are seldom fully disclosed, and, when they are, they are often buried in "privacy policies" or "terms of use". The user is seldom actively offered those terms.[121]

The range of parties involved in behavioural targeting is expanding. Over the past year, commercial services have begun offering tracking tools to Internet Service Providers that permit them to inspect the traffic of their customers and sell that data to third parties.[122] This stream of data potentially includes all online activities of ISP subscribers, including private communications such as banking and email and instant messaging correspondence. The privacy implications are obvious.[123] These service providers appear to be active in both Europe and North America, including Canada.[124] Privacy advocates have raised concerns with respect to the transparency of the activities of these companies.[125] It is far from clear that consumers are aware of how their personal information is being collected, used and disclosed by ISPs and these service providers.

The commercial pressures on social networking sites also threaten user privacy. MySpace offers an excellent example of how proprietors of social networking spaces employ targeted advertising in ways that threaten consumers' privacy. MySpace launched its HyperTargeting advertising platform to a select group of 50 companies in July 2007.[126] HyperTargeting is an "advertising platform" that uses "the self-expressed

---

[119] See, *e.g.*, Privacy Commissioner of Canada, "PIPEDA Case Summary #315: Web-centred company's safeguards and handling of access request and privacy complaint questioned" (9 August 2005), <http://www.privcom.gc.ca/cf-dc/2005/315_20050809_03_e.asp>.

[120] *Ibid*. at 6-11 for a discussion of this point.

[121] CIPPIC, *DRM & Privacy*, supra note 44 at 38.

[122] See, e.g., Saul Hansell, "The Mother of All Privacy Battles", New York Times (March 25, 2008) <http://bits.blogs.nytimes.com/2008/03/25/the-mother-of-all-privacy-battles/>.

[123] "US Congress questions legality of Phorm and the Phormettes", The Register (16 May, 2008) <http://www.theregister.co.uk/2008/05/16/congress_questions_nebuad/>.

[124] David George-Cosh, "ISPs testing 'digital snoops'" Financial Post (14 April 14, 2008) <http://www.canada.com/topics/technology/story.html?id=7631ad0e-850c-45b1-a818-76cbd30c3edd&k=39045>.

[125] Foundation for Information Policy Research "Open Letter to the Information Commissioner" (17 March 2008) <http://www.fipr.org/080317icoletter.html> (arguing that Phorm's targeted advertising service violates data protection principles).

[126] Duncan Riley, "MySpace To Announce Self-Serve Hyper Targeted Advertising Network" Tech Crunch (November 4, 2007), <http://www.techcrunch.com/2007/11/04/myspace-to-announce-self-serve-advertising-network/>. The first companies to try HyperTexting included: "Procter & Gamble, Microsoft XBOX, Ford, Taco Bell, Universal Pictures, Toyota, Fox Searchlight, XM Satellite Radio, AZJeans.com, and Summit Entertainment." MySpace. "MySpace Completes first phase of 'HyperTargeting By MySpace' Advertising Platform; leading social network passes 50 advertiser milestone for new program"

interests and passions" of MySpace users to supply them with advertising that they will be "receptive" to.[127] HyperTargeting tells the advertiser "exactly what [the user]... is passionate about", allowing advertisers to reach a "significant audience" while targeting "highly specific user interests."[128] The user's interests are tracked through predefined categories from their MySpace profiles, as the profiles are updated. Initially, the platform filtered information from 10 categories: "music, movies, personal finance, gaming, consumer electronics, sports, travel, auto, fashion and fitness"; however, the number of relevant categories is continually growing.[129] On November 5, 2007, MySpace added an additional 100 sub-categories and opened the platform to other advertisers. Although MySpace only uses what it characterizes as "non-personally identifiable information", for its targeted advertising, much of this information is personal in nature (*e.g.* "Personal Finance," "Marital Status," "Education," and "Children"). This privacy issue could be exacerbated as users are moved up "the funnel", and more and more user information is fed to the advertising system.[130] Presently, there are over 1,000 categories, with new categories continually being added.[131] HyperTargeting is only available in the United States, with plans to expand the platform internationally in 2008.[132]

Facebook similarly aggregates user profile information about user preferences to target personalized advertisements and promotions to its users. Advertisements that appear on Facebook are served directly to users by third party advertisers. Third party advertisers receive the user's IP address and "may download cookies to the user's computer or use other technologies such as JavaScript or 'web beacons' ... to measure the effectiveness of their ads and to personalize advertising content."[133] In essence, the personal information of Facebook users as displayed on their profile can be used by third party advertisers to serve more targeted advertising to users.

In addition to targeted banner advertising, Facebook has created a number of programs that allow businesses to customize their presence on Facebook in order to target their intended audience. The most notorious of these is Facebook's Beacon feature, released in November 2007. Beacon publishes actions, by logged-in Facebook users, undertaken on third party websites (owned by partners of Facebook), to the user's news feed and

---

HyperTargeting by MySpace (November 8, 2007).
<http://forum.myspace.com/index.cfm?fuseaction=messageboard.viewThread&entryID=536556&type=friendForum&friendID=272310801&MyToken=1afc7c6b-b9a6-4bc1-a18e-a2d4ca0dd177>.

[127] MySpace, HyperTargeting by MySpace (3 April, 2008), <http://www.myspace.com/hypertargeting>.

[128] Ibid.

[129] MySpace. "MySpace Completes first phase of 'HyperTargeting By MySpace' Advertising Platform; leading social network passes 50 advertiser milestone for new program" HyperTargeting by MySpace (November 8, 2007).

[130] The phrase "up the funnel" is a quote from former Chief Revenue Officer of Fox Interactive Media Mike Barrette. Kate Kaye, "Fox Interactive Media Buys Ad Targeting Firm to Leverage MySpace Profile Data" The ClickZ Network (Feb 22, 2007), <http://www.clickz.com/showPage.html?page=3625077>.

[131] Keith Regan, "MySpace, Facebook Hone Their Advertising Aim"
E-Commerce Times (11/05/07 1:19 PM PT), <http://www.ecommercetimes.com/story/60162.html>.
Business Wire, "MySpace Completes First Phase of "HyperTargeting by MySpace" Advertising Platform" (Nov 5, 2007), <http://findarticles.com/p/articles/mi_m0EIN/is_2007_Nov_5/ai_n21081077>.

[132] Business Wire, "MySpace Completes First Phase of "HyperTargeting by MySpace" Advertising Platform" (Nov 5, 2007), <http://findarticles.com/p/articles/mi_m0EIN/is_2007_Nov_5/ai_n21081077>.

[133] Facebook's Privacy Policy, note 24 above.

mini-feed features of Facebook user profiles.[134] Partners could determine the most relevant and appropriate set of actions from their sites that users could distribute onto Facebook, such as posting an item for sale, completing a purchase, scoring a high score in an online game, or viewing a video. At its launch, Facebook announced that there were 44 websites using Facebook Beacon "to allow users to share information from other websites for distribution to their friends on Facebook", calling it a "new way to socially distribute information on Facebook."[135] Facebook's Beacon partners included eBay, Fandango, CollegeHumor, iWon, echomusic, Blockbuster, Bluefly.com, Joost, LiveJournal, Live Nation, National Basketball Association, NYTimes.com, Sony Online Entertainment LLC, Sony Pictures, TripAdvisor, TypePad, and WeddingChannel.com.

Facebook users protested against the Beacon's release in November 2007. In a campaign launched by online liberal activist group MoveOn.org, nearly 70,000 users signed an online petition calling on Facebook to stop broadcasting users' transactions without their consent.[136] Many users were particularly upset as the Beacon ruined the surprise of Christmas gifts. MoveOn considered the Beacon program to be a "glaring violation of [Facebook] users' privacy" by imposing an opt-out regime instead of an opt-in system.[137]

In December 2007, Facebook shifted from an opt-out to an affirmative opt-in to the Beacon program and added a privacy control that allowed users to turn Beacon off completely. Facebook CEO Mark Zuckerberg admitted that Beacon's release was a mistake and apologized for failing to strike the "right balance" between new features and user privacy.[138]

Shortly thereafter, Computer Associates Security Advisor Stefan Berteau suggested that Facebook misrepresented Beacon to its users, suggesting that Facebook collects information about its users' actions on affiliate sites regardless of whether or not the user chose to opt out.[139] In his experiment, Berteau found that even after logging out of Facebook, information about his online activities linked to his Facebook account name was reported back to Facebook.[140] Berteau's findings conflict with Facebook's Beacon FAQ, which indicates that Facebook affiliates communicate with Facebook only if a user is logged into their account. However, the FAQ also states that "[a]ny information that

---

[134] Facebook, "Facebook Beacon", <http://www.facebook.com/business/?beacon>.
[135] "Leading Websites Offer Facebook Beacon for Social Distribution: Users Gain Ability to Share their Actions from 44 Participating Sites with their Friends on Facebook" (6 November 2007), <http://www.facebook.com/press/releases.php?p=9166>.
[136] "Facebook users light a beacon of protest" *eWeek.com* (21 November 2007), <http://www.eweek.com/c/a/Messaging-and-Collaboration/Facebook-Users-Light-a-Beacon-of-Protest/>. See MoveOn.org's Facebook privacy online petition: <http://civ.moveon.org/facebookprivacy/?rc=fb.privacysuccesspage>.
[137] "MoveOn.org takes on Facebook's 'Beacon' ads" *CNET News* (20 November 2007), <http://www.news.com/8301-13577_3-9821170-36.html>.
[138] Mark Zuckerberg, "Thoughts on Beacon" *The Facebook Blog* (5 December 2007), <http://blog.facebook.com/blog.php?blog_id=company&blogger=4>.
[139] "Facebook's Misrepresentation of Beacon's Threat to Privacy: Tracking users who opt out or are not logged in" *CA (*3 December 2007), <http://community.ca.com/blogs/securityadvisor/archive/2007/11/29/facebook-s-misrepresentation-of-beacon-s-threat-to-privacy-tracking-users-who-opt-out-or-are-not-logged-in.aspx>.
[140] See also "Facebook's Beacon More Intrusive Than Previously Thought*" PC* World (30 November 2007), <http://www.pcworld.com/article/id,140182-c,onlineprivacy/article.html>.

was sent to Facebook's servers will be deleted" if the user clicks "No Thanks".[141] Similarly, Facebook CEO Mark Zuckerberg claimed that if a user opted to turn off Beacon, Facebook would not store actions even when partners sent them to Facebook.[142]

Paul Stephens, director of policy and advocacy with the Privacy Rights Clearinghouse, says that the Facebook Beacon incident serves as a reminder that social networking sites that host personal information about individuals use a lot of the data for business purposes. Users of these sites should be mindful of this, where social networking sites rely on advertising for revenue.[143]

In conjunction with the Facebook Beacon program, Facebook unveiled a "Social Advertising" program called "Social Ads", which allows businesses to set up Facebook profile pages where visitors who take certain actions can trigger the sending of a "Social Ad" to their network of friends.[144] According to the press release:

> Facebook's ad system serves Social Ads that combine social actions from your friends – such as the purchase of a product or review of a restaurant – with an advertiser's message. This enables advertisers to deliver more tailored and relevant ads to Facebook users that now include information from their friends so they can make more informed decisions.[145]

Facebook markets Social Ads to businesses as "advanced targeting by age, location, gender, interests, and more."[146] Dan Solove and William McGeveran express concerns with Facebook's assumption that user consent to be included in the Social Ad program translates into the user's consent to be featured in an advertisement for the advertising partner.[147] McGeveran notes that with all the focus on the Beacon controversy, very little attention was paid to the lack of user control over Social Ads.[148]

Third party applications on Facebook also pose a threat to user privacy. Over 18,000 applications have been built on the Facebook Platform, with 140 new applications added per day. Facebook reports that more than 95% of Facebook members have used at least

---

[141] Facebook Beacon FAQ, <http://www.facebook.com/beacon/faq.php>.
[142] "Facebook Users Can Now Opt Out of Beacon Feature" <http://www.facebook.com/press/releases.php?p=11174>.
[143] "A wake up call for users in Facebook Beacon controversy" *CIO* (6 December 2007), <http://www.cio.com/article/163050/A_Wake_Up_Call_for_Users_in_Facebook_Beacon_Controversy>.
[144] In fact, the Social Ads program predated Beacon by a short period, as Social Ads grew out of an advertising alliance with Microsoft: see Facebook, "Microsoft and Facebook Team Up for Advertising Syndication" (August 22, 2006), <http://www.facebook.com/press/releases.php?p=635>.
[145] "Facebook Unveils Facebook Ads" (6 November 2007), <http://www.facebook.com/press/releases.php?p=9176>.
[146] See "Facebook Ads", <http://www.facebook.com/ads/>. See also "Facebook Social Ads", <http://www.facebook.com/business/?socialads>.
[147] See Daniel J. Solove, "The New Facebook Ads – Starring You: Another Privacy Debacle?" *Concurring Opinions* (8 November 2007), <http://www.concurringopinions.com/archives/2007/11/the_new_faceboo.html>. See also William McGeveran, "Facebook Inserting Users Into Ads*" Info/Law (*8 November 2007), <http://blogs.law.harvard.edu/infolaw/2007/11/08/facebook-social-ads/> and "More Thoughts on Facebook's 'Social Ads'" *Info/Law* (9 November 2007), <http://blogs.law.harvard.edu/infolaw/2007/11/09/more-thoughts-on-facebooks-social-ads/>.
[148] *Ibid*.

one application built on the Facebook Platform.[149] Third party applications threaten user privacy as applications gain access to not just all of a given user's personal information, but to a lot of personal information about a user's friends, many of whom will not have consented to have their information shared with third party applications. While there is a page that allows users to disable their friends' applications from accessing information about them, the page is buried deep in Facebook preferences and information is shared by default.

Facebook's most popular applications have over 24 million users. If a user wants to install an application, he or she must give the application full privileges to access their personal information on Facebook. Data mining through development platforms can potentially affect more people than screen scraping, as it exposes information that might otherwise be hidden (i.e. users with "private" profiles with high privacy settings may install third party applications). As noted by Chris Soghoian, a Ph.D. student in Information Security, it is technically impossible for Facebook to determine whether Developers are saving user data. Once data leaves Facebook's servers, Facebook has no way of knowing what happens to it.[150] Adrienne Felt of the University of Virginia conducted a study on privacy protections for social networking applications in October 2007.[151] In the study, the top 150 Facebook applications were systematically reviewed to determine their information needs. The study concluded that 9% of these applications did not require personal information in order to function. 82% of the top 150 Facebook applications required information that was public in order to function. "Public data" was defined to include such personal information as the user's name, network, and list of friends. Only 9% of these top 150 Facebook applications required data in order to fulfill their function. Yet all of the applications were given full access to user personal information, meaning that over 90% of the top 150 applications on Facebook were given access to information that was not needed to function correctly, including data on users who never signed up for the application (*i.e.* friends of the user). Since the incident of Zango spyware distribution through the "Secret Crush" third party application in January 2008, questions have been raised as to how Facebook should protect users from rogue applications as such applications would pose a great risk to privacy.[152]

d Privacy-Invasive Content Management Using Digital Rights Management Technologies

Digital Rights Management ("DRM") systems technologies are diverse, ranging from encryption and watermarking schemes to complicated tamper-resistant hardware packages enveloping sophisticated rights management architectures. The common purpose among these technologies is their need to identify content and manage its use. In most DRM distributions, these tasks involve a degree of surveillance. DRM doles out

---

[149] Facebook, "Press Room: Statistics" (March 2008), <http://www.facebook.com/press/info.php?statistics>.
[150] Chris Soghoian, "Exclusive: The next Facebook scandal" *CNET.com Blog Surveill@nce St@te* (23 January 2008), <http://www.cnet.com/8301-13739_1-9854409-46.html>.
[151] "Privacy Protection for Social Networking APIs" *University of Virginia* <http://www.cs.virginia.edu/felt/privacy/>.
[152] "Should Facebook preemptively protect users against rogue apps?" *Jonathan Zittrain* (8 February 2008), <http://people.oii.ox.ac.uk/z/2008/02/08/should-facebook-preemptively-protect-users-against-rogue-apps/>.

permissions, then watches that they are observed. Most DRMs feature technological protection measures which govern access to or use of content according to the DRM usage policy. More sophisticated DRMs add a reporting element, what Graham Greenleaf describes as "IP phone home":[153] DRM can collect information about the usage of content, and about the user, and allow for the transmission of that information back to the content distributor or some other third party. Such information may include simple registration data. More troublingly, it may also include a treasure trove of content-usage information: Who is the user? What are her usage habits? What else does she experience? When, where and how does she experience this content? This 'lifestyle' information was described by Justice Lebel of the Supreme Court of Canada as "core biographical information",[154] and by Justice Sopinka elsewhere as:

> [P]ersonal information which individuals in a free and democratic society would wish to maintain and control from dissemination [including] information which tends to reveal intimate details of the lifestyle and personal choices of the individual.[155]

Obviously, DRMs used to track and report on this usage behaviour raises significant privacy concerns. These concerns are more than merely theoretical: the Sony rootkit episode established their validity beyond all doubt.

Sony BMG's DRM software also had significant negative implications for consumers' privacy interests. First, despite statements to the contrary in associated license agreements, the software collected and disclosed consumer behaviour to third parties whenever a CD was placed in a computer. The DRM software would "phone home" to third party websites which would log the consumer's IP address, the date and time, the record the CD identifying information, and download and display banner ads on the user's computer.156 Security software vendors quickly labelled these DRMs as "spyware" and the United States Computer Emergency Readiness Team warned consumers not to install software from any source that would not ordinarily contain software, including audio CDs.157 Security software now routinely searches for and uninstalls Sony BMG DRMs when encountered.[158]

---

[153] Lee A. Bygrave, "Digital Rights Management and Privacy – Legal Aspects" in Eberhard Beckar *et al.,* eds., *Digital Rights Management – Technological, Economic, Legal and Political Aspects (Lecture Notes in Computer Science)* (Berlin, Germany: Springer-Verlag, 2003) 418 at 421.
[154] *Society of Composers, Authors and Music Publishers of Canada v. Canadian Association of Internet Providers,* 2004 SCC 45, at para. 155, LeBel, J., dissenting.
[155] *R. v. Plant*, [1993] 3 S.C.R. 281 at para. 12.
[156] J. Alex Halderman and Edward W. Felten, "Lessons from the Sony CD DRM Episode", Extended Version at 14 (14 February 2006), online: Center for Information Technology Policy, Princeton University <http://itpolicy.princeton.edu/pub/sonydrm-ext.pdf>.
[157] United States Computer Emergency Readiness Team, "First 4 Internet XCP DRM Vulnerabilities" (15 November 2005, updated 16 November 2005), online: United States Computer Emergency Readiness Team, November 16, 2005 – Current Activity <http://www.us-cert.gov/current/archive/2005/11/16/archive.html>.
[158] See, for example, Computer Associate's entry for "XCP" under its Spyware Encyclopedia, online: Computer Associates, eTrust Spyware Encyclopedia – XCP.Sony.Rootkit <http://www3.ca.com/securityadvisor/pest/pest.aspx?id=453096362>.

Nor are the privacy implications of the Sony rootkit unique in the DRM world. In September, 2007, we at CIPPIC published a report, titled *Digital Rights Management and Consumer Privacy*, that surveyed common DRM systems implemented in connection with content in the consumer marketplace. We concluded as follows:

> Fundamental privacy-based criticisms of DRM are well-founded: we observed tracking of usage habits, surfing habits, and technical data.[159]

As content distributors look to new and evermore innovative models for monetizing content, and particularly as distributors move online in greater numbers, we expect these concerns will become more pressing, not less.

[159] CIPPIC, *DRM & Privacy*, supra note 44 at ii.

Part II Responses

The scope and range of online threats to privacy demand response of similar scope and range. Unfortunately, no single regulatory response adequately addresses the full range of privacy threats Canadians face today. On reflection, this should surprise no one. We have already seen that different threats have different motives and so will respond to different regulatory initiatives. For example, while criminal sanctions may deter commercial actors from engaging in certain behaviours, they are insufficient to effectively deter fraudsters – whose underlying motive is already criminal. Arguably, increasing the size of the penalty, or devoting new or greater law enforcement resources toward the behaviour may deter such behaviour, but it won't eliminate. Regardless, devoting more resources to combat online privacy threats may have the effect of diverting resources away from other concerns. The truth is that a range of responses may be required to adequately address the full range of online privacy threats that Canadians face.

Our review of responses to online privacy threats has disclosed a number of different techniques to address these issues. Each has played a role in ameliorating the harm online privacy threats may impose of society. We group these responses into five groups:

- government legislation and regulation;
- international co-operative efforts;
- industry self-regulation;
- technological responses; and
- education efforts.

A Government Legislation/Regulation

Direct government regulation comes to mind first when most of us think about ways to change unwanted marketplace (or black market) behaviour: "There ought to be a law…" Indeed, we do see many different legislative approaches to behaviours that violate privacy. First, there are laws of general application that regulate how one can deal with individuals' privacy in the form of personal information protection. Second, there are the criminal laws. These are again laws of general application, but not focused on privacy. Third, there are issue-specific laws. These laws tend to focus on a specific behaviour related to technology, such as spam or spyware.

1 Personal Information Protection Laws

Following the European lead, many countries have now adopted data protection laws governing public and/or private sector collection, use and disclosure of personal information by governments and corporations. Such legislation varies from comprehensive, cross-sectoral approaches such as the EU *Directive of the European Parliament and of the Council on Privacy and Electronic Communications*[160] and related

[160] See <http://eur-lex.europa.eu/LexUriServ/site/en/oj/2002/l_201/l_20120020731en00370047.pdf>.

member country laws to sector-specific or issue-specific data protection laws such as the U.S. *Gramm-Leach-Bliley Act* or the U.S. *Children's Online Protection of Privacy Act*. All of these laws regulate private sector dealings with individuals' personal information. As such, they are most useful in regulating "legitimate" businesses, and have little utility in deterring fraudulently motivated attacks or behaviours such as cyberstalking, which target the individual without any commercial motivation whatsoever. Regulation of those kinds of behaviour is best suited to the criminal laws.

Canada has taken the former approach, enacting comprehensive data protection laws at the federal and provincial levels. One set of laws addresses the public sector (e.g., the federal *Privacy Act*, and Ontario *Freedom of Information and Protection of Privacy Act*), while another set of laws (the federal *Personal Information Protection and Electronic Documents* Act ("PIPEDA"),[161] as well as similar statutes in Quebec, Alberta and British Columbia) speaks to the private sector. PIPEDA applies to commercial activities under federal regulation as well as in all provinces other than the three mentioned.

PIPEDA, as its title suggests, was developed with the electronic context very much in mind. In fact, it was spurred by the federal government's desire to be a world leader in electronic commerce, and recognition that such a goal required consumer trust and confidence in the electronic medium. The government further recognized that such trust and confidence would not be gained or maintained unless personal data was properly protected, and that such protection was clearly not deliverable by market forces or industry self-regulation.

PIPEDA addresses online privacy threats together with offline privacy threats, through a set of ten principles based on well-established "Fair Information Practices" that are also reflected in the OECD's 1980 *Guidelines*. These Principles include the following:

- "The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means." (Principle 4.4)
- "The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate." (Principle 4.3)
- "Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes." (Principle 4.5)
- "Personal information shall be protected by security safeguards appropriate to the sensitivity of the information." (Principle 4.7)

In addition, subs. 5(3) of PIPEDA limits acceptable purposes, regardless of consent, as follows:

- "An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."

[161] PIPEDA, note 4, *supra*.

These provisions address online privacy threats in a number of ways. First, subs.5(3), if respected, would stop the collection, use and disclosure of personal data by commercially-motivated entities for illegitimate purposes, regardless of any purported consent by the individuals in question.

Second, Principle 4.4 addresses covert and deceptive collection of personal data by requiring that such data "be collected by fair and lawful means". As elaborated in Principle 4.4.2, "The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception."

Third, Principle 4.3's requirement for informed consent is meant to create an obstacle to unrestrained data collection, use and disclosure in the commercial sphere by giving individuals the right to stop such collection, use and disclosure themselves. Principle 4.5 backs up this informed consent requirement by prohibiting use and disclosure for purposes beyond those consented to.

Finally, Principle 4.7's requirement for appropriate security safeguards directly addresses intermediary organizations whose security failures facilitate online privacy invasions by third parties. Similarly, Principle 4.4's limit on collection and Principle 4.5's limits on retention of personal data also address important ways in which otherwise innocent organizations facilitate the privacy invasions posed by others.

These provisions therefore prohibit illegitimate behaviour such as phishing and pharming, as well as legitimate market activity that extends beyond acceptable limits. They apply both to organizations that pose the threats (i.e., that seek to collect and use the information), and to organizations that, wittingly or unwittingly, facilitate the threats through their over-collection of data.

2 Criminal and Quasi-criminal Laws

Canada was one of the first countries to enact criminal laws in the area of computer crime. In 1985, the *Criminal Code*[162] was amended to criminalize mischief in relation to data, theft of telecommunication services, and unauthorized use of a computer. Each of these provisions, along with other provisions of general application, has the potential to address malicious threats to privacy online. It should be apparent, however, that these provisions should usually have no application – except, perhaps, in the worst of cases – to online privacy threats motivated by commercial interests.

Criminal mischief is directed towards wilful destruction or damaging of property or wilful interference with the use of property.[163] The provision reads as follows:

> 430. (1) Every one commits mischief who wilfully
>
> (a) destroys or damages property;
> (b) renders property dangerous, useless, inoperative or ineffective;

[162] *Criminal Code of Canada*, R.S.C. 1985, c. C-46 (as amended) [*Criminal Code*].
[163] *Ibid.*, s. 430(1).

> (c) obstructs, interrupts or interferes with the lawful use, enjoyment or operation of property; or
> (d) obstructs, interrupts or interferes with any person in the lawful use, enjoyment or operation of property.

What constitutes "enjoyment" of property (or the obstruction, interruption, or interference of it) in the offence of mischief is a bit muddied in the case law.[164] Regardless, ss. 430(1) would only provide adequate protection for physical computer items (as s. 428 tells us that "property" is real or corporeal property). There are no statements made in Canadian jurisprudence that would indicate intangibles like "privacy" could or should be protected by these provisions. A related common law tort, trespass to chattels, has in its most extreme interpretations in the United States stretched to cover online access to a server, otherwise available to the public, in a manner that could, if left unchecked, burden the property of the owner in a manner leading to lost customers and lost profits.[165] However, it is difficult to stretch this interpretation of the tort far enough to cover "loss of privacy" or "interference with control over personal information". It would be an even bigger stretch to apply such a definition of "property" in the criminal context.

Mischief in relation to data, in contrast, appears on the surface a likelier criminal provision. Sub-section 430(1.1) provides that:

> Every one commits mischief who wilfully
>
> > (a) destroys or alters data;
> > (b) renders data meaningless, useless or ineffective;
> > (c) obstructs, interrupts or interferes with the lawful use of data; or
> > (d) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.

Sub-section 430(1.1), which was added to fill in where "mischief" left off and protect the lawful and legitimate use of services (and which is directly related "unauthorized use of a computer"), [166] protects "data" which ss. 342.1(2) defines as "representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system." This definition is broad enough to include some forms of "personal information" – such as computer passwords or cryptographic keys – but it is unclear that it captures merely digitized personal information, such as one's

---

[164] See the differing opinions of Justices Fish and Chamberland in writing for the Quebec Court of Appeal in *R. v. Drapeau* 1995 CanLII 5099 (QC C.A.).

[165] See *Ebay, Inc. v. Bidder's Edge*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000). For a critical take on this expansive interpretation of the tort, see Dan Burk, "The Trouble with Trespass", SSRN <http://ssrn.com/abstract=223513>.

[166] Section 342.1(1) on unauthorized use of a computer makes it an indictable offence for anyone who, fraudulently and without color or right, (a) obtains, directly or indirectly, any computer service, (b) intercepts or cause to be intercepted, directly or indirectly, any function of a computer system by means of an electro-magnetic, acoustic, mechanical, or other device, (c) uses or cause to be used, directly or indirectly, a computer system with intent to commit an offence under (a) or (b) or an offence under section 430 (relating to mischief as seen above). It also makes it an offence for those who the fraudulently use, posses, traffic or allow another person access to a computer password that would enable the person to commit offenses (a), (b) or (c).

unencrypted name. No case has yet established that invasion of privacy is captured within the scope of the prohibition. There is very little case law on 430(1.1). Government commentary suggests that these provisions address denial of service attacks and virus transmission, as well as attacks on the computer or network (not the attack on the person).[167]

Sub-section 326(1) of the *Criminal Code* prohibits theft of services. Aimed at the theft of public utilities, this provision provides that "every one commits theft who fraudulently, maliciously, or without colour of right… (b) uses any telecommunication facility or obtains any telecommunication service."[168] "Telecommunication" here means "any transmission, emission or reception of signs, signals, writing, images or sounds or intelligence of any nature by wire, radio, visual or other electromagnetic system."[169] The question, then, is whether this prohibition is broad enough to capture the various services associated with online access. Case law has interpreted this definition narrowly to exclude some computer networks. In *R v. McLaughlin*, a student used a computer terminal on campus to access the central unit of the computing service at the University of Alberta that contained confidential information.[170] The Court of Appeal acquitted the accused on the basis that the computer unit being used was not in itself a "telecommunication facility" "or other electro-magnetic system", thereby precluding the first limb of section 326(1)(b); and the connection was entirely within an "internal" system of the university, even though it involved some 300 terminal outlets. It was, therefore, not a telecommunication facility.

From today's perspective, as technology has changed to allow for distant ("external") access to many users, neither of the above elements, essential to the result in that case, may continue to hold. Sub-section 326(1)(b) could well potentially apply to online fraudsters. However, to apply this provision to online criminals, a court will have to recognize that technology has changed, and apply prohibitions drafted with radio and television transmissions in mind to new technology: the Internet. It is not clear how far the definition of a "facility" might stretch. Is a personal computer a "telecommunications facility"? It may well be that the nature of the invasion will determine the applicability of the prohibition. Where a fraudster simply "steals" personal data off of one's computer, it is questionable whether a prohibition on theft of service would apply. On the other hand, where that personal information is then used for some illicit purpose, such as unauthorized access to a web service such as email, the prohibition may well apply. At best, theft of service is an imperfect tool for addressing online privacy threats.

Sub-section 184(1) of the Criminal Code prohibits "interception" of "private communications," such as telephone or other conversations between two people. In order to be caught by the provision, a defendant's conduct must amount to "interception" – defined broadly to include "listening, recording and acquiring a communication" – and what is intercepted must be "private communications". The requirement that the communication be private may be more difficult to meet in the online context, due to the

---

[167] Public Safety Canada, "Fact Sheet: High Tech Crime" < http://ww2.ps-sp.gc.ca/policing/organized_crime/FactSheets/high_tech_crime_e.asp>.
[168] *Criminal Code*, supra note >, ss. 326(1).
[169] *Ibid.*, ss. 326(2).
[170] (1980), 18 C.R. (3d) 339 (S.C.C.).

requirement that the communication be between persons and a good deal of online communication is indirect.

It is uncertain to what extent this provision would apply to all forms of computer communication. Most jurisprudence on the subject addresses law enforcement search and seizure powers – and most of that deals with in-person or telephone communication. However, the court in *R v. Garafoli* found that electronic surveillance constitutes a search and seizure (and is subject to the reasonableness requirement of s.8 of the Charter), so the applicability of the interception provisions to online activities may not be far off.[171] Furthermore, the saving provisions (under 184(2)) appears to be easily transplantable to the online context (consent and authorization for interception requirements remain the same no matter what the medium), and the related offences of possession of an interception device (191) and disclosure of private communications intercepted (193) also fit within the online context.

Interception activities in the online context might be better covered by sub-section 342.1(1) of the Criminal Code. This provision provides that:

> Every one who, fraudulently and without colour of right,
>
> > (*a*) obtains, directly or indirectly, any computer service,
> > (*b*) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,
> > (*c*) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (*a*) or (*b*) or an offence under section 430 in relation to data or a computer system, or
> > (*d*) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (*a*), (*b*) or (*c*)
>
> is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

Again, this provision is not directed towards misuse of personal information or invasion of privacy, but addresses some behaviours associated with threats to online privacy. For example, this provision may capture "pretexting" associated with cyberstalking where a stalker uses a victim's computer password to access email services or a social networking site. It may also capture social engineering strategies employed in phishing attacks targeting online banking or financial service providers. It is not clear, however, that these provisions would capture "hacking" – the unauthorized access of a computer. Is one's computer, or the data on it, a "computer service"? Does merely accessing data stored on a hard drive amount to an "interception"? Note that paragraph 342.1(1)(c) captures fraudulent use of a "computer system", but only where such use is with intent to commit a crime under paragraphs (a) (obtaining a computer service), (b) (interception of a function of the computer system), or s. 430 (mischief in relation to data).

[171] [1990] 2 S.C.R. 142.

Cyberstalking remains an activity that is not specifically called out in Canada's *Criminal Code*. However, stalking, generally, is addressed by the Code, and its provisions would apply to a stalker using online tools. Sending false messages with the intent to injure or alarm is prohibited by s. 372, criminal harassment is addressed in s.264), and uttering threats is prohibited by s.264.1 of the Code. In combination, these provisions address much of the behaviour associated with cyberstalking. Interestingly, we are beginning to see online harassment addressed at the level of schools, and outside the criminal space. Manitoba recently amended its Public Schools Act to address cyberbullying and the use of electronic devices.[172] The amendment requires schools to include cyber-bullying in its anti-bullying policies and to establish policies for the appropriate use in schools of electronic devices, including email, the Internet, and mobile phones, in their premises.

Canada is also in the midst of addressing identity fraud through the Criminal Code. Bill C-27173 proposes to make it illegal to make, possess, transfer or sell "identity documents," or to knowingly obtain or possess another person's "identity information" with the inference that the intent is to commit a crime such as fraud. Moreover, it proposes to make it an offence to transmit, make available, distribute, sell or offer to sell such information knowing that it will be used to commit an offence. However, this law, as currently proposed in Bill C-27, likely doesn't go far enough to protect online privacy, as it does not address major privacy issues, such as phishing or spyware, nor does it provide law enforcement with the resources it needs to investigate and combat online fraud.[174]

It is interesting to contrast the Canadian criminal provisions with those of the United States. The *Computer Fraud and Abuse Act*[175] (intended to reduce "hacking") elaborates on the Canadian provision related to "unauthorized use of a computer" (also intended to reduce "hacking") and it prohibits the following activities:

1. Knowingly accessing a computer without authorization in order to obtain national security data
2. Intentionally accessing a computer without authorization to obtain:
    - Information contained in a financial record of a financial institution, or contained in a file of a consumer reporting agency on a consumer.
    - Information from any department or agency of the United States
    - Information from any protected computer if the conduct involves an interstate or foreign communication

---

[172] Bill C-24, The Public Schools Amendment Act (Cyber-Bullying and Use of Electronic Devices), 2nd Sess., 39th Leg. (Manitoba), amending ***The Public Schools Act*****,** C.C.S.M. c. P250.
[173] *An Act to amend the Criminal Code* (identity theft and related misconduct). See <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=3125690&Language=e&Mode=1>.
[174] Michael Geist calls for anti-spam legislation (which would include phishing and spyware) and a mandatory security breach notification law so that Canadians are advised when their personal information may be at heightened risk for identity theft. See <http://www.michaelgeist.ca/content/view/2401/125/>. CIPPIC calls for law enforcement resources improvement: see <http://www.cippic.ca/uploads/CIPPIC_Brief_C-27_01Apr08.pdf>.
[175] *Computer Fraud and Abuse Act* 1986 (US) 18 USC 1030 <http://www.law.cornell.edu/uscode/18/1030.html>.

3. Intentionally accessing without authorization a government computer and affecting the use of the government's operation of the computer.
4. Knowingly accessing a computer with the intent to defraud and there by obtaining anything of value.
5. Knowingly causing the transmission of a program, information, code, or command that causes damage or intentionally accessing a computer without authorization, and as a result of such conduct, causes damage that results in:
    - Loss to one or more persons during any one-year period aggregating at least $5,000 in value.
    - The modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals.
    - Physical injury to any person.
    - A threat to public health or safety.
    - Damage affecting a government computer system
6. Knowingly and with the intent to defraud, trafficking in a password or similar information through which a computer may be accessed without authorization.[176]

The CFAA was first aimed at government security rather than at the protection of privacy, and thus was (originally) narrower than the "unauthorized use of a computer" provision in the Canadian *Criminal Code*. The only computers protected were "federal interest" computers—so the Act wasn't of much help to the average citizen. The offences in the CFAA were amended in 1994 and 1996 to cover all computers used in interstate commerce. At the same time, Congress provided for private civil actions to help anyone injured by the criminal activity this statute prohibits. In October 2001, Congress broadened the CFAA to include any computer "located outside the United States that is used in a manner that affects interstate or foreign commerce or communication in the United States."

The CFAA has proven difficult to rely upon for addressing online privacy threats. The CFAA requires proving intent to access, as well as damage of at least $5,000 caused by the unauthorized access, and (at least by implication) that the access is unauthorized. It has also been restrictively interpreted. In *SecureInfo Corp. v. Telos Corp.*, it was held that the defendants had authorization to use a computer system even though such access violated the terms of a license agreement binding the user who provided them with access to the system.[177] In addition, for purposes of prosecution, the law focuses its attention on the actual damage done to computer systems and the specific economic losses stemming from an act of computer fraud or abuse. As privacy is not quite so quantifiable, the effectiveness of the CFAA for addressing online privacy violations is questionable.

The Federal Trade Commission ("FTC") is the other significant American vehicle for addressing online privacy violations. The FTC's mandate is to take action against "unfair

[176] *Ibid* at 1030(a).
[177] 387 F. Supp. 2d 593 (E.D. Va. 2005).

or deceptive acts or practices".[178] Using its authority under Section 5 of the *Federal Trade Commission Act*[179] ("FTC Act"), the FTC has brought a number of cases to enforce the promises made by companies in privacy statements, including promises about the security of consumers' personal information.[180] However, outside of attempting to enforce promises the companies make themselves, the FTC has limited ability to protect the online privacy of consumers, as the FTC has little to work with in terms of a general privacy framework. The FTC is reduced to enforcing aspects of statutes that address the proper handling of personal information.

The anti-pretexting laws of the *Gramm-Leach-Bliley Act*[181] provide one example of such a statute. The Act prohibits "pretexting" – the use of false pretenses, including fraudulent statements and impersonation, to obtain consumers' personal financial information, such as bank balances. The scope of information protected was broadened with the introduction of the *Telephone Records & Privacy Protection Act* of 2006,[182] which prohibits pretexting to buy, sell or obtain personal phone records.[183] How useful these types of laws are in practice is questionable.[184]

Looking internationally, the Council of Europe Cybercrime Treaty provides an international criminal framework for considering criminal law responses to online privacy threats.[185] The Treaty requires ratifying states to adopt legislative and other measures that would establish criminal offences related to illegal access, illegal interception, data interference, system interference, and misuse of devices. Computer related forgery and fraud offences also must be created.[186] According to a scorecard on the Council's Web site, to date 43 countries have signed the Convention. Twenty-one nations have yet to ratify it, and 22 have put the Treaty into force.[187] Although this seems positive from outward appearances (as it purports to protect personal information from fraudsters, etc.), the Treaty has actually been strongly criticized by civil liberties groups,

---

[178] "Unfair" practices are defined to mean those that "cause or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition" (15 U.S.C. Sec. 45(n)).
[179] *The Federal Trade Commission Act*, 15 U.S.C. §§ 41-58 <http://www.law.cornell.edu/uscode/html/uscode15/usc_sec_15_00000041----000-.html>.
[180] A notable case involves TJX. According to the FTC complaint, TJX, with over 2,500 stores worldwide, failed to use reasonable and appropriate security measures to prevent unauthorized access to personal information on its computer networks. See <http://www.ftc.gov/opa/2008/03/datasec.shtm>.
[181] *The Gramm-Leach-Bliley Act (GLBA),* 15 U.S.C. § 6801 et. seq. <http://www.ftc.gov/privacy/glbact/glbsub1.htm>.
[182] *The Telephone Records and Privacy Protection Act of 2006* (H109-4709). See <http://thomas.loc.gov/cgi-bin/query/C?c109:./temp/~c109g2LERP>.
[183] California enacted similar legislation prior to the Federal enactment.
[184] Damon Darlin & Matt Richtel, "Fuzzy Laws Come Into Play in the H.P. Pretexting Case" *New York Times* (19 September 2006), online: <http://www.nytimes.com/2006/09/19/technology/19hewlett.html>.
[185] *Cybercrime Convention* (Eur. T.S. No.185) (November 23, 2001), online: Council of Europe <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.
[186] See Articles 2-8 <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>.
[187] See Convention on Cybercrime scorecard: <http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG>.

privacy experts and industry representatives for giving law enforcement too much power.[188]

According to the Department of Justice, "[m]ost of the required offences and procedures [within the Cybercrime Treaty] already exist in Canada." The Department qualifies that statement by noting that:

> before Canada can ratify the Convention and give it effect, the Criminal Code would need to be amended to include:
>
> - provisions for a production order;
> - provisions for a preservation order; and
> - an offence in relation to computer viruses that are not yet deployed.[189]

On the other hand, some suggest that "there's nothing in the document that indicates (new powers) are needed" and that that the justification for adopting such sweeping changes to Canadian law seems weak.[190] At the least, the criminalization of unreleased "computer viruses" represents a positive development in protecting online privacy.

3 Issue Specific Laws

Some jurisdictions have chosen to adopt specific laws to tackle specific technology related problems. Such laws are helpful in addressing short-term needs prompted by the emergence of a particular technological phenomenon, but run the danger of being rendered irrelevant as the technology supporting the behaviour becomes obsolete, and the underlying behaviour moves on to different technologies not captured by the original law.

Anti-spam laws provide the best known recent technology-specific laws. The American approach to anti-spam legislation, the CAN-SPAM Act,[191] is perhaps the best known anti-spam legislation. The CAN-SPAM Act contains both criminal and civil provisions. Criminal measures include prohibitions on:

(1) accessing a protected computer without authorization to send multiple commercial email messages;

(2) using open relays with intent to deceive in sending multiple commercial email messages;

---

[188] For one example, see the criticisms of the Electronic Privacy Information Center, available online: <http://epic.org/privacy/intl/ccc.html>.

[189] For the Government statement, see <http://canada.justice.gc.ca/eng/cons/la-al/a.html>. The DOJ's desire to bring these amendments to life has been reflected in the Lawful Access proposals (of 2005 and 2007), where "the need for Canada to adopt statutory measures that will permit ratification of the Council of Europe *Convention on Cyber-Crime*" is often cited as an inducement. These proposals, for the most part, have not been met with support from public interest groups which see the proposals as a threat to *Charter* rights. See CIPPIC's FAQ on Lawful access at <http://www.cippic.ca/lawful-access/> and CIPPIC's submissions to the Candian government with respect thereto: <http://www.cippic.ca/uploads/CNAinfo-submission-Oct07.pdf >.

[190] Declan McCullagh, quoting Michael Geist, in "Will Canada's ISPs become spies?" CNET News.com (27 August, 2002) <http://www.news.com/2100-1023-955595.html?tag=fd_top>.

[191] *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003*, 15 U.S.C. § 7709, [CAN-SPAM Act].

(3) using materially false header information in sending multiple commercial email messages;

(4) falsely registering email accounts or domain names in connection with sending multiple commercial email messages; and

(5) falsely claiming to be the registrant of internet protocol addresses for sending spam.[192]

Civilly, the CAN-SPAM Act includes numerous provisions enforced through federal court lawsuits brought by certain federal agencies, including the FTC and Department of Justice, state Attorneys General, and ISPs. These include prohibitions on false or misleading transmission information and deceptive subject lines,[193] detailed opt-out requirements,[194] and requirements to provide a notice of advertisement or solicitation, a valid physical postal address,[195] and warning labels on sexually-explicit commercial email.[196] The Act also renders sellers liable, under certain circumstances, for the activities of spammers promoting the seller's wares or services.[197] The Act designates as "aggravated" violations specific spamming techniques used to increase spam volumes, such as "harvesting," "dictionary attacks," automated creation of multiple sender accounts, and computer hijacking.[198] Finally, the Act called for the FTC to study the feasibility of a "Do Not Spam" registry, which the FTC concluded was unworkable in the absence of authenticated email.[199]

The FTC's 2005 Report to Congress on the efficacy of the CAN-SPAM Act claimed that the Act had two significant benefits. First, by establishing liability for particular behaviour, the CAN-SPAM Act has forced "legitimate" marketers to adopt "best practices" that improve upon the standard of behaviour consumers encountered prior to the legislation's enactment. Second, the Act has provided the FTC, state law enforcement agencies and ISPs with a new tool for enforcement that the FTC claims has "enforcement efficacy".[200] However, the FTC Report acknowledged that both the evolution of technology and the global nature of spam worked to limit the effectiveness of the legislation.

The CAN-SPAM Act has been criticized for adopting an "opt-out" approach to spam, rather than an "opt-in" approach. Critics argue that CAN-SPAM does not stop email, but instead merely sets the conditions for its continuance. For example, the Coalition

---

[192] *Ibid*., 18 U.S.C. § 1037 (a) (1) – (5).
[193] *Ibid*., 15 U.S.C. § 7704 (a) (1) – (2).
[194] *Ibid*., § 7704 (a) (3) – (4), (5) (A) (ii).
[195] *Ibid*., § 7704 (a) (5) (A) (i), (iii).
[196] *Ibid*., § 7704 (d).
[197] *Ibid*., § 7705.
[198] *Ibid*., § 7704 (b).
[199] Federal Trade Commission, "National Do Not Email Registry: A Report to Congress" (June 2004) at 1 <http://www.ftc.gov/reports/dneregistry/report.pdf>: "[A] National Do Not Email Registry, without a system in place to authenticate the origin of email messages, would fail to reduce the burden of spam and may even increase the amount of spam received by consumers."
[200] Federal Trade Commission, "Effectiveness and Enforcement of the CAN-SPAM Act: A Report to Congress" (December 2005) <http://www.steptoe.com/publications/384a.pdf>.

Against Unsolicited Commercial Email (CAUCE) argued "This legislation fails the most fundamental test of any anti-spam law, in that it neglects to actually tell any marketers not to spam. Instead, it gives each marketer in the United States one free shot at each consumer's e-mail inbox."[201] The Act also offers no redress for consumers as, notably, it lacks a private right of action.

The EU Directive on Privacy and Electronic Communications Directive, in contrast to the American approach, requires member states to legislate opt-in regimes. The Directive specifies that:

> (40) Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the recipient. For such forms of unsolicited communications for direct marketing, it is *justified to require that prior explicit consent of the recipients is obtained before such communications are addressed to them* [emphasis added].[202]

While consumer and privacy advocates prefer opt-in regimes to opt-out regimes, the truth is that the majority of spam originates from illegitimate actors whose practices are not influenced by marketplace framework legislation. So long as internet infrastructure continues to permit spammers to hide spam's origins, spam will continue to challenge consumers' privacy interests.[203] From a regulatory perspective, cross-border co-operation and enforcement and public-private information sharing partnerships with ISPs have had a more significant impact on spam than laws have.

The Canadian regulatory response to spam – or, rather, the lack of one – perhaps reflects this reality. Despite extensive consultations through an Anti-Spam Task Force resulting in recommendations for anti-spam legislation (in the context of a general, technology-neutral law that addresses internet threats),[204] the Canada's federal government has failed to introduce such laws. Notwithstanding the federal government's failure to legislate, better practices within ISPs, technological advances and better consumer education in the years since the Anti-spam Task Force have all combined to keep the problems associated with spam in check.

Spyware is another area that has attracted technology-specific legislation. Legislative activity in the United States has focused at the state level. California's *Consumer Protection Against Computer Spyware Act*[205] is typical of many of these laws, as

---

[201] CAUCE, "Statement on House Spam Bill Vote" ¶ 1 (22 Nov. 2003) <http://www.cauce.org/news/>.
[202]EU Directive on Privacy and Electronic Communications Directive, 2002/58/EC.
[203] See, e.g., Evangelos Moustakas, Prof C. Ranganathan, Dr. Penny Duquenoy, "Combating Spam Through Legislation: A Comparative Analysis of US and European Approaches" at 1: <http://research.microsoft.com/users/joshuago/conference/papers-2005/146.pdf>:
"The antispam solution involves also updating the e-mail system so that spammers will not be able to hide the origins of their e-mail messages. The key technical element for that is authentication."
[204] Task Force on Spam, "Stopping Spam: Creating a Stronger, Safer Internet" (May 17, 2005) at 13 <http://www.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00248e.html>.
[205] Cal. Bus. & Prof. Code, § 22947 (West Supp. 2006).

California was the first state out of the gate with consumer protection laws addressing spyware issues and many states followed California's model. The first thing to be said about the California law is that it addresses only the most egregious behaviours associated with spyware. Most of its prohibitions address only "deceptive" or intentional conduct, rather than applying more broadly to articulating a general standard of care to which software publishers must adhere. For example, with respect to spyware's impact of privacy, the California statute provides that:

> 22947.2. A person or entity… shall not, with actual knowledge, with conscious avoidance of actual knowledge, or willfully, cause computer software to be copied onto the computer of a consumer in this state and use the software to do any of the following:
>
> … (b) Collect, through intentionally deceptive means, personally identifiable information that meets any of the following criteria:
>
> > (1) It is collected through the use of a keystroke-logging function that records all keystrokes made by an authorized user who uses the computer and transfers that information from the computer to another person.
> >
> > (2) It includes all or substantially all of the Web sites visited by an authorized user, other than Web sites of the provider of the software, if the computer software was installed in a manner designed to conceal from all authorized users of the computer the fact that the software is being installed.
> >
> > (3) It is a data element described in paragraph (2), (3), or (4) of subdivision (k) of Section 22947.1, or in subparagraph (A) or (B) of paragraph (5) of subdivision (k) of Section 22947.1, that is extracted from the consumer's computer hard drive for a purpose wholly unrelated to any of the purposes of the software or service described to an authorized user.[206]

Note that the Act also defines "personally identifiable information" exhaustively and narrowly as:

> (1) First name or first initial in combination with last name.
> (2) Credit or debit card numbers or other financial account numbers.
> (3) A password or personal identification number required to access an identified financial account.
> (4) Social Security number.
> (5) Any of the following information in a form that personally identifies an authorized user:
> > (A) Account balances.
> > (B) Overdraft history.
> > (C) Payment history.
> > (D) A history of Web sites visited.
> > (E) Home address.
> > (F) Work address.
> > (G) A record of a purchase or purchases.[207]

[206] *Ibid*., s. 22947.2(b).
[207] *Ibid*., s. 22947.1(k).

Similarly, the Act provides that:

> 22947.3. A person or entity … shall not, with actual knowledge, with conscious avoidance of actual knowledge, or willfully, cause computer software to be copied onto the computer of a consumer in this state and use the software to do any of the following:
>
> (b) Modify any of the following settings related to the computer's access to, or use of, the Internet:
>
> (1) An authorized user's security or other settings that protect information about the authorized user for the purpose of stealing personal information of an authorized user.[208]

The end result of these protections amounts to a prohibition against the collection of certain classes of personal information through installation of software by intentionally deceptive means or through intentional modification of a user's privacy settings.

By placing these prohibitions in a general consumer protection code, California's anti-spyware legislation creates a private right of action amendable to class action. A number of actions have used the statute's prohibitions as the basis for class claims, including in response to the Sony BMG "rootkit"[209] and to address the behaviour of the notorious adware publisher, DirectRevenue.[210]

Canada has not taken the step of addressing spyware legislatively. Canadian consumer remain restricted to combating spyware through laws of general application such as provincial consumer protection statutes and the misleading advertising provisions of the *Competition Act*,[211] as well as contract and tort law. There have been no judgements in spyware cases in Canada. A class action against Sony BMG in respect of the "rootkit" copy protection technology was settled without a finding of law.[212]

In response to the perceived territorial inadequacies of the existing legislative framework for addressing online threats, Congress in 2006 passed the US SAFE WEB Act to address harms to American interests originating outside of the United States.[213] The Act is essentially a long-arm statute targeting deceptive practices that originate outside of the United States but harm interests in the United States. The US SAFE WEB Act expands the jurisdiction of the Federal Trade Commission to address "unfair or deceptive acts or practices" that involve "foreign commerce" that "cause or are likely to cause reasonably foreseeable injury within the United States" or involve "material conduct occurring

---

[208] *Ibid*., s. 22947.3(b).
[209] "Sony BMG Settles California Case", ConsumerAffairs.com (December 19, 2007) <http://www.consumeraffairs.com/news04/2006/12/ca_bmg.html >.
[210] See Order Granting Final Approval of Settlement, *Battaglia* v. *DirectRevenue, LLC*, No. 05-CV-02547-LKK-PAN (JFM) (E.D. Cal. 2005) <http://classactiondefense.jmbm.com/battagliaclassactiondefense_fao.pdf >.
[211] R.S.C. 1985, c. C-34, as amended.
[212] Michael Geist, "Rootkit Settlement Gives Consumers Short Shrift" (18 September, 2006), *Toronto Star* <http://www.thestar.com/article/96146>.
[213] *Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers across Borders Act of 2006*, 109th Congress, 2nd Sess., S.1608 <http://thomas.loc.gov/cgi-bin/query/C?c109:./temp/~c1091vX0K3> [*US SAFE WEB Act*].

within the United States".[214] The Act also includes extensive information sharing and cross-border investigative assistance mechanisms, permitting the FTC to address and participate in cross-jurisdictional and multi-jurisdictional threats.

Congress passed the Act with the encouragement of the FTC.[215] A 2005 FTC briefing in support of the legislation stated:

> The US SAFE WEB Act would greatly aid the Federal Trade Commission (the "Commission" or "FTC") in its efforts to protect U.S. consumers from global fraud by (1) improving the FTC's ability to cooperate with foreign counterparts in specific cases and investigations; (2) improving the FTC's ability to gather information; (3) enhancing the FTC's ability to obtain monetary consumer redress; and (4) strengthening the FTC's enforcement cooperation networks.[216]

The US SAFE WEB Act amounts to a significant expansion of the FTC's investigatory powers and jurisdiction. This expansion was premised on the need for civil law enforcement to respond to the emergence of a global Internet with tools and powers that are able to look beyond the borders of the United States. The FTC's 2005 Recommendation to Congress identified consumer harms associated with spam, spyware and phishing as threatening harms the FTC should guard Americans against, and argued that the FTC's civil investigatory powers inadequately matched the global nature of these threats.[217] The FTC went so far as to draft a case study to demonstrate how new investigative and co-operative powers in the US SAFE WEB Act could assist the FTC in investigation and enforcement of a spyware case.[218]

In a nod towards accountability, the Act includes an obligation for the FTC to report to Congress on its use of and experience with these new powers within three years of enactment.[219]

While an analysis of the merits and shortcomings of the investigatory powers of Canada's consumer protection agencies lies beyond the scope of this Report, it should be obvious that Canada's patchwork consumer protection regime, grounded largely in provincial jurisdiction, faces challenges addressing multi-jurisdictional online threats. Provincial authorities need the tools offered by the US SAFE WEB Act to share information with other law enforcement and consumer protection agencies. Canada's consumer protection agencies could also benefit from clarification that their jurisdiction extends to address harms to interests in the province from off-shore online threats.

---

[214] *Ibid*., s. 3.
[215] Federal Trade Commission, "The US SAFE WEB Act: Protecting Consumers from Spam, Spyware, and Fraud – A Legislative Recommendation to Congress" (June 2005) <www.ftc.gov/reports/ussafeweb/USSAFEWEB.pdf>.
[216] Federal Trade Commission, "An Explanation of the Provisions of the US SAFE WEB Act" at 2 http://www.ftc.gov/reports/ussafeweb/Explanation%20of%20Provisions%20of%20US%20SAFE%20WEB%20Act.pdf>.
[217] Federal Trade Commission, "The US SAFE WEB Act: Protecting Consumers from Spam, Spyware, and Fraud – A Legislative Recommendation to Congress" (June 2005) at i <www.ftc.gov/reports/ussafeweb/USSAFEWEB.pdf>.
[218] Federal Trade Commission, "How the US SAFE WEB Act Would Help the FTC: A Hypothetical Spyware Case" <http://www.ftc.gov/reports/ussafeweb/spyware%20hypo.pdf>.
[219] US SAFE WEB Act, note 213 *supra*, s. 14.

B International Cooperative Efforts

Recognizing that threats to privacy are not deterred by boundaries, nations have to international for to co-ordinate responses to online threats. At present, this process seems ad hoc, in the sense that while there is international will to manage online privacy threats collectively, this will is manifested in approaches undermined by a silo effect. Practical considerations in many cases have compelled states to look beyond their borders. The realities of international commerce and the interconnectedness of telecommunications systems require consistency and co-ordination across borders.

The United Nations has been an active forum for international co-operation on cybersecurity issues. The Declaration of Principles at the World Summit of the Information Society in Geneva on December 12, 2003, included a commitment to build confidence and security in the use of Information and Communication Technologies (ICTs). This declaration included recognition that:

> 35.Strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs. A global culture of cybersecurity needs to be promoted, developed and implemented in cooperation with all stakeholders and international expert bodies. These efforts should be supported by increased international cooperation. Within this global culture of cyber-security, it is important to enhance security and to ensure the protection of data and privacy, while enhancing access and trade. In addition, it must take into account the level of social and economic development of each country and respect the development-oriented aspects of the Information Society.
>
> 36. While recognizing the principles of universal and non-discriminatory access to ICTs for all nations, we support the activities of the United Nations to prevent the potential use of ICTs for purposes that are inconsistent with the objectives of maintaining international stability and security, and may adversely affect the integrity of the infrastructure within States, to the detriment of their security. It is necessary to prevent the use of information resources and technologies for criminal and terrorist purposes, while respecting human rights.
>
> 37. Spam is a significant and growing problem for users, networks and the Internet as a whole. Spam and cyber-security should be dealt with at appropriate national and international levels.[220]

These Declarations matured into a Plan of Action, which included the observation that "Confidence and security are among the main pillars of the Information Society", and adopted the following resolutions:

> b) Governments, in cooperation with the private sector, should prevent, detect and respond to cyber-crime and misuse of ICTs by: developing guidelines that take into account ongoing efforts in these areas; considering legislation that allows for effective investigation and prosecution of misuse; promoting effective mutual assistance efforts; strengthening institutional support at the international level for preventing, detecting and recovering from such incidents; and encouraging education and raising awareness.

[220] World Summit of the Information Society, *Declaration of Principles*.

> c) Governments, and other stakeholders, should actively promote user education and awareness about online privacy and the means of protecting privacy.
>
> d) Take appropriate action on spam at national and international levels. […]
>
> f) Further strengthen the trust and security framework with complementary and mutually reinforcing initiatives in the fields of security in the use of ICTs, with initiatives or guidelines with respect to rights to privacy, data and consumer protection.[221]

The Organization of American States' General Assembly adopted a common cybersecurity strategy in 2004.[222] The OAS' Inter-American Telecommunication Commission (CITEL), the main forum in which OAS governments and the private sector meet to coordinate regional efforts to develop the Global Information Society according to the mandates of the General Assembly established at the Summits of the Americas, has established a Working Group on Policy and Regulation Considerations to permit OAS states to discuss and exchange information on emerging telecommunications policy and regulatory matters arising from the existing and the evolving telecommunications environment.[223] This Working Group has established a Rapporteur Group on Cybersecurity & Critical Infrastructure, whose mandate is to study the security aspects related to communication network development, its role in supporting other critical infrastructures, the role of the private sector in securing the communication network, and domestic and regional approaches required in the Americas Region on this matter.[224]

APEC, the forum for Asia-Pacific Economic Cooperation, has also taken a role in encouraging international co-operation in addressing online privacy threats. APEC's Telecommunications and Information Working Group held workshops in 207 on malware and network security, and in 2006 hosted a Symposium on Information Privacy and Protection in E-Government and E-Commerce. The Working Group also developed a "Cybersecurity Strategy" in 2002[225] and a "Strategy to Ensure Trusted, Secure and Sustainable Online Environment" in 2005.[226]

The International Telecommunications Union, or ITU, has also been an active site for international co-operation on security issues. The ITU has been entrusted with implementing The UN World Summit of the Information Society's Plan of Action as it

---

[221] World Summit of the Information Society, *Plan of Action* (12 December 2003).
[222] "Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity" (adopted 8 Jun 2004) AG/RES. 2004 (XXXIV-O/04) <http://www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm>.
[223] <http://www.citel.oas.org/citel_i.asp>.
[224] <http://www.citel.oas.org/ccp1-tel/Cybersecurity.asp>.
[225] APEC, Cybersecurity Strategy, Doc no telwg26/BFSG/22 (August 2002) <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN012298.pdf >.
[226] APEC, Strategy to Ensure Trusted, Secure and Sustainable Online Environment <http://203.127.220.112/content/apec/apec_groups/working_groups/telecommunications_and_information.downloadlinks.0004.LinkURL.Download.ver5.1.9>.

relates to Information and Communications Technologies. To that end, the ITU has adopted a Global Cybersecurity Agenda.[227]

The Agenda is built on 5 pillars: (1) legal framework, (2) technical measures, (3) organizational structures, (4) capacity-building, and (5) international cooperation.

The Agenda has 7 main goals:

(1) Elaboration of strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures;

(2) Elaboration of strategies for the creation of appropriate national and regional organizational structures and policies on cybercrime;

(3) Development of a strategy for the establishment of globally accepted minimum security criteria and accreditation schemes for software applications and systems;

(4) Development of strategies for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives;

(5) Development of strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organizational structures to ensure the recognition of digital credentials for individuals across geographical boundaries;

(6) Development of a global strategy to facilitate human and institutional capacity-building to enhance knowledge and know-how across sectors and in all the above-mentioned areas; and

(7) Advising on a potential framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above-mentioned areas.

ITU sections have been working hard at meeting this Agenda. The ITU-Standardization (ITU-T) group has established study groups addressing security guidance and manuals. Activities Related to Cybersecurity[228] The ITU-Development (ITU-D) Applications and Cybersecurity Division's activities have included advancing the use of ICT-based networks, services and applications, and promoting cybersecurity in developing nations.[229]

The Organization for Economic Co-operation and Development (OECD) has also been an active forum for international co-operation on online privacy issues. The OECD is an international organization with more than 30 Member Countries. Some describe the OECD as the arena in which the first transatlantic conflicts over privacy protection took

[227] International Telecommunications Union, Global Cybersecurity Agenda <http://www.itu.int/osg/csd/cybersecurity/gca/>.
[228] See <http://www.itu.int/cybersecurity/ITU-T/>.
[229] See <http://www.itu.int/ITU-D/cyb/cybersecurity/index.html>.

place.[230] These conflicts are represented in the preface of the OECD Guidelines[231], which highlights the need to reconcile attitudes that are "fundamental but competing" in order to "advance the free flow of information between Member countries." While the Guidelines don't actually define privacy, they do it concede it to be a fundamental human right worthy of protection. The principles emerged from various international instruments (including the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, open for signature on 28 January 1981), but the debate on how the principles should be brought into practice (through EU Directives or otherwise) continues to this day. The principles are:

- Collection Limitation,
- Data Quality,
- Purpose Specification,
- Use Limitation,
- Security Safeguards,
- Openness,
- Individual Participation, and
- Accountability.

The Guidelines make no distinction between normal data and sensitive data (unlike the 1981 Council of Europe Convention). The Guidelines are also voluntary and do not impose any penalties for non-compliance (also unlike the 1981 Council of Europe Convention). While some question how effective a voluntary regime can be, others see the Guidelines as a means to "justify self-regulatory approaches rather than as a method to promote good data protection practices through the advanced industrial world."[232] Regardless, the Guidelines have had enormous influence on subsequent approaches to fair information practices, including influencing the CSA Code that forms the core of PIPEDA's obligations in respect of personal information.[233]

The Organization for Economic Co-operation and Development continues as an active forum for international co-operation on online privacy issues. The OECD *Working Party on Information Security and Privacy* (WPISP), working under the direction of the Committee for Information, Computer and Communications Policy (ICCP) "develops policy options by consensus to sustain trust in the global networked society."[234] The WPISP has set up an active network of experts from government, business and civil society to monitor trends, share and test experiences, analyze the impact of technology on information security and privacy, and provide policy guidance. To help implement the

---

[230] Bennett & Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (Burlington, VT: Ashgate, 2003) Chatpter 4 at 74-77 [Bennett and Rash, *The Governance of Privacy*].
[231] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, adopted on 23 September 1980.
[232] Bennett and Rash, *The Governance of Privacy*, s*upra* note > at 77.
[233] Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (Aspen: Aspen Publishers Inc., 2002) at chapters 1 and 2.
[234] See <http://www.oecd.org/document/46/0,3343,en_2649_34255_36862382_1_1_1_1,00.html>.

Privacy Guidelines in the electronic world, the WPSIP, in co-operation with industry, privacy experts and consumer organizations, has recently developed the OECD Privacy Policy Statement Generator. The Generator, which has been endorsed by the OECD's 30 member countries, aims to offer guidance on compliance with the Privacy Guidelines and to help organizations develop privacy policies and statements for display on their Web sites.[235] The WPISP was also early in producing consumer privacy guidelines. In 1997, the OECD published its "OECD Cryptography Guidelines: Recommendations of the Council"[236] and followed that in 1998 with its Ministerial Declaration on the Protection of Privacy on Global Networks.[237] More recent work includes 2003's "Privacy Online: OECD Guidance on Policy and Practice"[238] and the "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"[239] and the "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" in 2004.[240]

The OECD has released several reports related to online privacy, including "Privacy Online: OECD Guidance on Policy and Practice" (2002), "Making Privacy Notices Simple: an OECD Report and Recommendations" (June 2006), and "Report on Cross-border Enforcement of Privacy Laws" (October 2006).[241] The OECD is also holding a series of meetings on "the Future of the Internet Economy".[242] One of the goals of the upcoming Ministerial meeting in Seoul is to discuss how to "[s]afeguard individual privacy while encouraging the deployment of services and devices that tailor information to individuals or allow them to participate in online social networks."

The OECD's Directorate for Science, Technology and Industry has also been very active for a long time producing guidelines, briefs, and recommendations for protecting consumers. The Directorate's Committee on Consumer Policy in 1999 produced the "OECD Guidelines for Consumer Protection in the Context of Electronic Commerce",[243] and in 2003 issued "Guidelines for Protecting Consumers From Fraudulent and Deceptive Commercial Practices Across Borders", which focus significantly on online issues.[244] More recently, in 2006 the Council produced a Policy Brief, entitled "Protecting Consumers from Cyberfraud"[245]

The OECD has been an international leader in addressing spam issues. In 2006, the OECD published the "OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws Against Spam".[246] The OECD subsequently established a Task

[235] See <http://www.oecd.org/document/39/0,3343,en_2649_37441_28863271_1_1_1_37441,00.html >.
[236] <http://www.oecd.org/document/34/0,3343,en_2649_34255_1814690_1_1_1_1,00.html>.
[237] <http://www.oecd.org/dataoecd/39/13/1840065.pdf>.
[238] <http://www.oecd.org/document/49/0,3343,en_2649_34255_19216241_1_1_1_1,00.html>.
[239] <http://www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html>.
[240] <http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html>.
[241] See <www.oecd.org/sti/security-privacy>.
[242] See <http://www.oecd.org/site/0,3407,en_21571361_38415463_1_1_1_1_1,00.html >.
[243] <http://www.oecd.org/document/51/0,3343,en_2649_34267_1824435_1_1_1_1,00.html>.
[244] <http://www.oecd.org/document/50/0,3343,en_2649_34267_2514994_1_1_1_1,00.html>.
[245] <http://www.oecd.org/dataoecd/4/9/37577658.pdf>.
[246] <http://www.oecd.org/document/27/0,3343,en_2649_34223_37965659_1_1_1_1,00.html>.

Force on Spam which produced in 2005 an "Anti Spam Regulation"[247] and in 2006 a Report that included an "Anti-Spam Toolkit of Recommended Policies and Measures."[248]

APEC, the Asia-Pacific Economic Cooperation, has also been an active forum for addressing privacy issues. Decisions made within APEC are reached by consensus and any commitments made by 1 or more of the 21 Member Economies are completely voluntary.[249] In 2004, APEC members adopted the APEC Privacy Framework, the Forward to which states that: "the potential of electronic commerce cannot be realized without government and business co-operation to develop and implement technologies and policies which … address issues including privacy."[250]

There are nine information privacy principles in the Privacy Framework:

- Preventing harm
- Notice
- Collection limitation
- Uses of personal information
- Choice
- Integrity of personal information
- Security safeguards
- Access and correction
- Accountability

Following the articulation of the Framework, APEC prepared the Pathfinder Project, implementation guidelines for the Privacy Framework, in September of 2007.[251]

It is interesting to compare the APEC Privacy Framework with the OECD Privacy Guidelines. The OECD Guidelines call for "Openness", "Purpose Specification" and "Data Export Limitation"; the APEC Privacy Framework does not (although the APEC Framework's "Notice" and "Choice" combined could, arguably, compare with the OECD Guidelines' "Purpose Specification", and the APEC "Accountability" principle could compare, in some respects, with the OECD's "Data Export Limitation" principle). The APEC Framework also adds "Preventing Harm" and "Choice" principles, which do not appear in the OECD Guidelines. The APEC Framework is non-prescriptive: the implementation guidelines offer several options for giving effect to the Framework. Enforcement and remedial requirements are similarly left open. As APEC is primarily a forum for trade, it is no surprise that the framework focuses on preventing the misuse of

[247] <http://www.oecd.org/dataoecd/29/12/35670414.pdf>.
[248] Report of the OECD Task Force on Spam <http://www.oecd.org/dataoecd/63/28/36494147.pdf>.
[249] For more information about the Asia-Pacific Economic Cooperation, see: <http://www.apec.org/content/apec/about_apec.html>
[250] The APEC Privacy Framework was a result of the Ministerial Meeting in Santiago, Chile (in Nov 2004) <http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf>
[251] *Ibid.*

personal information (seen in the Preventing Harm principle) rather than protecting the privacy as a right of the individual.

Building on many of these international efforts, government and public agencies from 27 countries, including Canada, met with private sector representatives in London in October, 2004, to discuss international spam enforcement cooperation. The meeting culminated in the London Action Plan, a multi-stakeholder commitment to promote international spam enforcement cooperation and address spam related problems, such as online fraud, phishing, and malware.[252] While stopping short of imposing binding obligations on participants, the Action Plan is nonetheless notable for a number of features designed to offer a continuing means of addressing ongoing spam-related harms. These features include commitments by participating governments and agencies and private sector participants to employ "best efforts" to, among other things, regularly share information about legislative and law enforcement developments, education initiatives, public-private initiatives, investigative techniques, technological developments, and training initiatives.[253] Canadian participants include Industry Canada and the Office of the Privacy Commissioner of Canada.[254] Canada's private sector participates in the Action Plan through involvement in private sector coalitions such as the Messaging Anti-Abuse Working Group, which includes companies such as Bell Canada.[255]

The London Action Plan appears to be fulfilling its promise, and is active on education and law enforcement fronts. With respect to education, Action Plan participants host annual workshops, the most recent – the 3rd, held jointly with the European Union Contact Network of Spam Authorities – in Washington D.C., in October, 2007.[256] On the collaboration front, participants continue to meet by teleconference every 2 months. More significantly, the Plan has produced collaboration efforts among the American Federal Trade Commission, the Australian Communications and Media Authority, and OPTA (Onafhankelijke en Post en Telecommunicatie Autoriteit, the Dutch communications regulator), and produced cross-EU spam enforcement cases. Plan participants have also met with law enforcement representatives of Nigeria, China and Russia – all hotbeds of spam activity.

C Industry Self-Regulation

Government action is not the only mechanism for addressing online privacy threats. Industry self-regulation can assist Canadians by establishing best practices and drafting industry guidelines. Of course, these forms of regulation will do little to address fraud or malicious invasions of privacy. However, they can be effective in minimizing threats to online privacy that originate with commercial actors.

---

[252] The London Action Plan, <http://www.londonactionplan.com/?q=node/1>.
[253] "The Plan in Detail", <http://www.londonactionplan.org/?q=node/1>.
[254] London Action Plan, "LAP Member Organizations" <http://www.londonactionplan.com/?q=node/5>.
[255] See Messaging Anti-Abuse Working Group, "Member Roster" <http://www.maawg.org/about/roster>. MAAWG joined the Action Plan in February of 2008: "MAAWG Joins The London Action Plan to Expand Cross-Border, Public-Private Anti-Spam Cooperation" (February 5, 2008) <http://www.maawg.org/news/maawg080205>.
[256] Joint London Action Plan-EU Contact Network of Spam Authorities, "Collaborative Ventures to Fight Online Threats" (9 October, 2007); see: <http://open.nat.gov.tw/OpenFront/report/show_file.jsp?sysId=C09602813&fileNo=004 >.

1 Marketing Associations

Industry marketing associations publish best practices and guidelines to help shape regulation of their industry. The Internet Advertising Association, based in the United States, is the marketing association most active in the area of online privacy. This group is a frequent participant in public consultations on online privacy and the initiatives of other organizations. In Canada, the Direct Marketing Association is the organization most active.[257]

Privacy advocates have been critical of these groups, and critical of industry self-regulation, generally. Chris Hoofnagle, wrote of the American experience of self-regulation as a means of privacy protection as follows:

> We now have ten years of experience with privacy self-regulation online, and the evidence points to a sustained failure of business to provide reasonable privacy protections.[258]

2 Technology Associations

The Anti-Spyware Coalition (ASC) is an example of an industry association that has online safety as a core value. The ASC is a coalition of technology security software distributors, academics and consumer groups that work to build consensus about definitions and best practices in the debate surrounding spyware and other potentially unwanted technologies. The ASC has drafted a number of documents that have proven useful in creating greater certainty around the permissible bunds of online marketing. ASC documents to date include "Definitions and Supporting Documents" (defining terms for behaviours and technologies relevant to spyware), a "Best Practices Suggestion Document" (describing good notice and consent practices), and "Risk Model Description" (a set of behaviours that anti-spyware publishers use to inform the decision about whether to flag a piece of software as potentially unwanted by the consumer).[259]

The Anti-Phishing Working Group (APWG) is a coalition of organizations representing stakeholders (apart from consumers) that work together to address the harms associated with phishing. In July, 2006, the APWG published its "Anti-Phishing Best Practices for ISPs and Mailbox Providers."[260]

The Messaging Anti-Abuse Working Group, or MAAWG, is another coalition of technology stakeholders working within the online space. MAAWG focuses on preserving electronic messaging from abuse while ensuring the deliverability of legitimate messages.[261] MAAWG members comprise internet service providers, network operators, security firms and consumer advocates.[262] MAAWG addresses messaging abuse through technological approaches, industry collaboration and engaging with lawmakers in public policy initiatives.[263] MAAWG has been very active in promoting good practices amongst communications facilities providers and service providers.

---

[257] See <http://www.dmachoice.org/emps.html>.
[258] Chris J Hoofnagle, Privacy Self Regulation: A Decade of Disappointment (4 March 2005).
[259] See <http://www.antispywarecoalition.org/documents/index.htm>.
[260] See "Best Practices" <http://www.antiphishing.org/reports/bestpracticesforisps.pdf >.
[261] Messaging Anti-Abuse Working Group, "Introducing MAAWG" <http://www.maawg.org/home/>.
[262] Messaging Anti-Abuse Working Group, "Member's Roster" <http://www.maawg.org/about/roster/>.
[263] Messaging Anti-Abuse Working Group, "About MAAWG" <http://www.maawg.org/about/>.

MAAWG co-published with the Anti-Phishing Working Group a guide to "Anti-Phishing Best Practices for ISPs and Mailbox Providers".[264] Other Publications include a White Paper on email authentication

BITS Forum is a financial service industry consortium made up of 100 of the largest financial institutions in the US. BITS provides intellectual capital and fosters collaboration to address emerging issues "where financial services, technology, and commerce intersect". BITS has been active addressing phishing issues among members.[265]

On the spam front, the Anti-Spam Technical Alliance, which includes major technology companies such a Yahoo! and Microsoft, and also major American ISPs such as EarthLink and AOL, produced an "Anti-Spam Technical Alliance Technology and Policy Proposal."[266]

The Internet Service Provider's Association, an association of ISPs, has also addressed spam and other online privacy threats. ISPA members are subject to the ISPA Code, which includes guidelines on spam. [267] The ISPA has also worked with the London Action Plan to analyze spamming practices and routine offenders.

Individual firms can also do a great deal to combat online privacy threats. Security software and application providers make a great deal of information available on their websites that can influence how the marketplace behaves. McAfee published an anti-phishing guide in 2004[268] and security company Trend Micro followed in 2006 with its own Best Practices document on phishing.[269]

D Technological Responses

Technology itself can be a tremendous regulator of behaviour. Perhaps no range of responses has had a greater impact on the threat posed by online privacy invasion than the tools parties have adopted across the internet to improve security. These include tools that focus on the user's browsing and computing experience, tools at the level of the ISP, and tools at the level of the online service provider.

Technological tools that improve user privacy include both tools that focus on security and improved security features in operating systems and applications. Anti-virus software has long been a mainstay of user computers. Anti-virus software has traditionally focused on definitions – identifiable malicious code – that describe destructive viruses and worms. However, over the past five years, the range of security

---

[264] "Anti-Phishing Best Practices for ISPs and Mailbox Providers" (Version 1.01, July 2006) <http://www.maawg.org/about/publishedDocuments/MAAWG_AWPG_Anti_Phishing_Best_Practices.pdf >.
[265] See <http://www.bitsinfo.org/index.html>.
[266] (22 June 2004) <http://www.earthlink.net/about/press/pr_asta_tech/asta_tech.pdf>.
[267] < http://www.ispa.org.uk/html/about_ispa/ispa_code.html>.
[268] "Anti-Phishing: Best Practices for Institutions and Consumers" McAfee Technical Report #04-004 (Sept 2004) <http://www.mcafee.com/us/local_content/white_papers/wp_anti_phishing.pdf>.
[269] "Best Practices Series: Phishing" Trend Micro White Paper Series, (November 2006) <http://us.trendmicro.com/imperia/md/content/us/pdf/wp01_phishing_061127us.pdf>.

tools available to internet users – and necessary for a safe computing experience – has greatly expanded. In addition to anti-virus software, Internet users should now also use anti-spam tools, anti-spyware tools, and a firewall. Anti-spam tools assist consumers in filtering spam out of the stream of legitimate email individuals receive. Anti-spyware tools identify known potentially unwanted technologies, flag them for the user, and permit the user to control whether or not those technologies are permitted to install on the user's computer (or remove them if already installed). Both of these technologies combine user control – the user sets the settings for the tool and ultimately determine whether a specific communication will be permitted through – with the expertise of the service provider in identifying potentially problematic communications. Firewalls, on the other hand, restrict access to the computer to permitted channels. This guards against third parties accessing a user's desktop through unwatched channels. Recently, anti-phishing tools, usually in the form of browser-linked blacklists of known phishing websites, have been added to the user's security toolbox. Combined, this suite of security tools has helped users regain a significant measure of control over their online experience.

However, these tools – particularly anti-spyware and anti-virus tools – are reactive. They can only identify threats once they have been seen "in the wild". Many privacy threats exploit technological vulnerabilities. Recently, with the professionalization of the malware authoring trade, the time between the discovery of vulnerabilities and the time in which some malware appears in the wild exploiting that vulnerability – has shrunk to zero. Accordingly, no security tool is invulnerable. A "zero day exploit" may slip through even the most tightly guarded security screen. Security firms are responding with behavioural analysis – identifying potentially harmful behaviour in software rather than relying on definitions. However, the process is an arms race, and at best imperfect.

Developers have also recently significantly improved security in operating systems and applications. In particular, beginning with Service Pack 2 of Microsoft's Windows XP operating system, technology firms began implementing much improved security at the user level. Automatic updates and more attention to security at the design level have greatly improved the security of many of the most common applications on users' desktops.

Greater attention to security at the ISP level has also greatly improved internet security. ISPs routinely filter out enormous quantities of spam before it ever reaches the customer's network or desktop. ISPs also communicate with their customers, suggesting that they close open ports and warning them that leaving servers open to relay and forward messages also permits their systems to be hijacked by fraudsters as proxy e-mail servers and bots.[270]

E Public Education

Finally public education plays a large role in minimizing harms associated with online privacy threats. Greater awareness among internet users about both the nature of privacy threats facing them online and the tools that they can use to protect themselves has helped

[270] See, *e.g.*, Industry Canada, "Anti-Spam Action Plan", note 109 *supra*.

ameliorate the magnitude of harm inflicted by those who threaten our privacy online. Public authorities have played a role here, but so too have private organizations.

1 Public Initiatives

A number of Canadian organizations have created excellent public education materials on online threats, including threats to privacy. The website of the Office of the Privacy Commissioner of Canada includes public education materials on privacy rights and practices that impact on those rights, including many of the behaviours detailed in this report. For example, the Privacy Commissioner of Canada released a Facts Sheet on social networking and privacy, as well as an excellent Youtube video on the same topic.[271] Provincial privacy officers have their own resources as well. Industry Canada has also prepared a comprehensive website promoting awareness of online privacy issues among Canadians called "Privacy Town".[272]

Canadian law enforcement has created a number of tools for addressing online privacy threats. RECOL: Reporting Economic Crime Online, is a secure, online fraud reporting website.[273] The RCMP has prepared a guide to online safety titled "Practical Information and Scams Protection: A Canadian Practical Guide."[274] The Competition Bureau has also made consumer protection information available online.

Other government organizations have made good information available to the public. Public Safety Canada has published a number of guides online, including materials on "internet safety",[275] phishing,[276] and mass-marketing fraud.[277]

Finally, Canada's Taskforce on Spam, a public-private partnership led by Industry Canada, has published excellent materials on protection against unwanted spam.[278]

Canada is not alone in crafting consumer protection materials. For example, the Federal Trade Commission in the United States has published excellent materials on online safety. The FTC's "On Guard Online" initiative offers consumers a wealth of useful information for protecting themselves against privacy invasion and fraud.

2 Private Initiatives

Private organizations in the non-profit and commercial sectors publish materials on online privacy protection.

Non-profit groups are very active in citizen education. Our own organization, CIPPIC, places public education at the core of its mandate and publishes and updates on its website a series of FAQs and other documents that seek to provide neutral and useful

[271] Privacy Commissioner of Canada, "Social Networking and Privacy" note 26 above.
[272] Industry Canada, "Privacy Town" <http://www.ic.gc.ca/epic/site/oca-bc.nsf/en/ca01304e.html>.
[273] See <https://www.recol.ca/intro.aspx?lang=en >.
[274] See <http://www.rcmp-grc.gc.ca/scams/canadian_practical_guide_e.htm#online>.
[275] See <http://www.safecanada.ca/topic_e.asp?category=3>.
[276] See <http://publicsafety.gc.ca/prg/le/bs/phish-en.asp>.
[277] See <http://publicsafety.gc.ca/prg/le/bs/massmfr-en.asp>.
[278] See <http://strategis.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00248e.html>.

information on online privacy threats and what individuals can do to protect themselves against privacy invasion, as well as how to seek assistance if an invasion has occurred.[279]

Other non-profit organizations based in the United States with an exceptional amount of useful online privacy-related information include the Electronic Frontier Foundation, EPIC, and the Center for Democracy and Technology. The Berkeman Center at Harvard University runs the Badware initiative, a blacklist program that identifies potentially unwanted technologies. Consumer group NextAdvisor published a Facebook Identity Theft Protection Guide.[280]

Commercial actors are also active consumer educators. In Canada, those institutions most active include those businesses most affected by online privacy invasions: financial institutions and ISPs. Both groups of organizations put significant resources into educating their customers on Internet safety. ISPs offer their customers security suites as a value-added part of their service. Financial institutions offer consumers advice on how to secure their systems against invasion and safe online computing practices.

The group of companies most active in promoting consumer awareness of online privacy threats, however, remains the technology industry itself. Members of the security vendors – Symantec, McAfee, Trend Micro, and Sophos, amongst many others – are at the core of consumer protection on the Internet. It is their job to keep abreast of new threats, strategies, and security exploits. Their publications have provided us with much of the material we have relied upon in understanding online privacy threats and preparing this report. Consumer facing materials run the gamut, from "state of the art" reports, such as Symantec's bi-annual *Internet Security Threat Report* to application-specific reports. For example, a number of organizations have published "best practices" for protecting personal information on social networking sites. Sophos has published "Best Practices" for privacy settings on Facebook.[281]

[279] See <http://www.cippic.ca>.
[280] NextAdvisor, "Facebook Identity Theft Protection Guide: 6 tips to protect your identity on Facebook" (4 March 2008) <http://www.nextadvisor.com/blog/2008/03/04/6-tips-to-protect-your-identity-on-facebook/>.
[281] Sophos, "Facebook Best Practice" <http://www.sophos.com/security/best-practice/facebook.html>.

Part III PIPEDA and Online Threats to Privacy

As noted above, PIPEDA addresses online privacy threats through a number of provisions that put limits on organizations' collection, use, retention and disclosure of personal information in the course of commercial activities. These limits apply to organizations regardless of their motives: malicious or innocent. They apply to purposes as well as practices, prohibiting the collection, use and disclosure of personal data for inappropriate purposes. However, their effectiveness is compromised by a number of factors.

A Limited Applicability

PIPEDA applies only to organizations in the course of commercial activity. (On the other hand, the three provincial statutes apply to non-commercial entities as well). Thus, online privacy threats from stalkers or others acting in a non-commercial context are, other than in Alberta, B.C. and Quebec, not addressed by privacy legislation in Canada. This goes for provincially regulated employers as well, with respect to privacy-invasive activities affecting their employees in the provinces other than the three listed above.

B Vagueness of Key Provisions

PIPEDA suffers from vagueness with respect to a number of key provisions including those applicable to the online privacy threats discussed above. Organizations take advantage of these grey areas by pursuing questionable activities on the grounds that they are not clearly prohibited. Troublesome grey areas include the following:

1 Do IP Addresses Constitute "Personal Information"?

Targeted behavioural marketing proceeds on the basis that linking details about an individual's online behaviour, exhibited preferences, and online communications to an IP address alone (no name or contact info) does not constitute a privacy risk and is not prohibited by privacy laws. Similar activities that link behavioural data to IP addresses underlie many of the privacy risks described above. PIPEDA's definition of "personal information", "information about an identifiable individual…", has proven to be remarkably unhelpful in resolving this issue, despite a few published findings on point by the Privacy Commissioner. Does "identifiability" require a name? Can it be said that an individual is "identifiable" once a certain amount of information about that person is gathered into a profile, even if such information does not include name or contact information? Until these questions are answered, PIPED A will remain largely ineffective in addressing online privacy threats such as behavioural profiling.

2 What Information is "Necessary" for Targeted Marketing Purposes?

As noted above, Principle 4.4 of PIPEDA limits the collection of personal data to that which is "necessary" for the stated purposes. But in the context of direct marketing, there are no clear limits on what is "necessary" – in fact, the more information about your customer (or potential customer), the better. Virtually all data about an individual

consumer, from the marketer's perspective, is "necessary" because of its potential to assist in effective targeting. Principle 4.4 provides no guidance on how to distinguish between what is necessary and what is not, other than prohibiting the "indiscriminate" collection of personal data.

3 What Purposes would a Reasonable Person Consider Inappropriate in the Circumstances?

By limiting the purposes for which personal data can be collected, use or disclosed, subsection 5(3) sets out a critical limit on an otherwise largely consent-based regime. This "bottom line" protection has proven to be an important component of PIPEDA's data protection regime, relied upon by the OPC in numerous published findings.[282] However, it relies upon an objective determination of "appropriateness" that will no doubt be difficult to achieve in many situations with any significant degree of social consensus. In other words, reasonable persons may well disagree on whether a given information collection, use or disclosure is appropriate in the circumstances. This would certainly seem to be the case with respect to much of the information-based marketing activity that occurs online, especially with respect to children.

CIPPIC has proposed that subs.5(3) be supplemented with examples, for greater certainty regarding the application of the provision to specific circumstances such as the collection and use of children's data for commercial purposes.[283]

4 What Measures Constitute "Appropriate Security Safeguards"?

Principle 4.7's requirement that organizations protect personal data by security safeguards "appropriate to the sensitivity of the information" has the advantage of being flexible to deal with different security risks as well as with the evolving nature of both the risks and the security measures available to organizations at any given time. However, it is remarkably broadly-worded, allowing for disagreement even among experts on what particular measures are appropriate in a given situation. Privacy commissioner determinations in specific published cases are gradually providing guidance in this respect, but such decisions are few and far between. In the meantime, organizations must determine for themselves how this principle should be implemented in terms of specific hardware, software, and other solutions to protect their customers from online privacy threats.

C The Limits of Consent as a Tool of Data Protection

PIPEDA relies to a large degree on informed consent as a tool by which individuals can control the collection, use and disclosure of their personal information so as, for example,

---

[282] See, *e.g.*, Privacy Commissioner of Canada, "PIPEDA Case Summary #276: The privacy implications of pay per view and piracy prevention measures," (2 September 2004) <http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040902_01_e.asp>; see also *Eastmond v Canadian Pacific Railway*, 2004 FC 852 <http://www.canlii.org/en/ca/fct/doc/2004/2004fc852/2004fc852.html>.

[283] Canadian Internet Policy & Public Interest Clinic, *Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up?* (CIPPIC, May 2006) <http://www.cippic.ca/documents/bulletins/compliance_report_06-07-06_(color)_(cover-english).pdf> [CIPPIC, *Are Retailers Measuring Up?*].

to limit their exposure to online privacy threats. As many commentators have pointed out, however, consent is a very weak tool given the realities of business and consumer behaviour, and the often extreme imbalance of power as between the data gatherer/user and the individual data subject.[284] CIPPIC's 2006 study of online retailer compliance with PIPEDA's consent (and other) requirements provides strong evidence of the weakness of consent as a data protection tool.[285]

Consent is a particularly weak tool when it can be assumed, as is the case under PIPEDA. Other than in situations involving "sensitive data" or where a reasonable person would expect to be asked for permission, the Act explicitly permits the reliance by marketers and others on "implied consent", obtained through "opt-out" methods. Such methods assume the individual's consent even when there is no factual basis on which to rest such an assumption, and shift the burden onto the individual to refute the assumption by proactively indicating his or her refusal through some means such as a check-box, email, or postal mail request. Opt-out consent is a notoriously poor reflection of actual consumer preferences,[286] and is widely used by marketers and others precisely because of its tendency to overstate consumer consent.

D Missing Protections

Although PIPEDA approaches the problem of online privacy threats through a number of provisions addressing all aspects of data collection, use and disclosure, it lacks at least one important protection: a clear requirement for notification of data security breaches to affected individuals, as well as relevant authorities and the public at large. Interestingly, this is one element of data protection law in which Canada lags the U.S.A., where the majority of states now have legislated breach notification requirements. Data breach notification serves two distinct functions: first, by raising the risk of negative publicity, it creates stronger incentives for organizations to take strong security measures to prevent data breaches in the first place. Second, by requiring notification to affected individuals forthwith upon discovery of a breach, it allows such individuals to take measures to prevent or mitigate damages caused by identity thieves or others who may have taken advantage of the breach. CIPPIC has been calling for a data breach notification requirement in Canada for several years.

---

[284] Lisa Austin, Lisa Austin, "Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices" (2006), 44 *Canadian Business Law Journal* 21 <available at SSRN: http://ssrn.com/abstract=1169162>, Jaqueline Burquel and Valerie Steeves, Broken Doors: Strategies for Drafting Privacy Policies Kids Can Understand (March, 2007) at 62 <http://www.idtrail.org/files/broken_doors_final_report.pdf> (citing I. Pollach, "A typology of communicative strategies in online privacy policies: Ethics, Power and Informed Consent" (2005) 62 *Journal of Business Ethics* 221 in support of the conclusion that business' information collection practices are often conducted on the basis of policies that preclude informed consent).

[285] CIPPIC *Submission to Industry Canada on PIPEDA Reform Issues* (January 15, 2008).

[286] See, *e.g.*, Ian Kerr et al., "Soft Surveillance, Hard Consent," *Personally Yours* 6 (2006):1-14; Eric Johnson, Steven Bellman and Gerald Lohse, "Defaults, Framing and Privacy: Why Opting in ≠ Opting Out," *Marketing Letters* 13(1) (2002): 5-15.

E Weak Domestic Enforcement

Perhaps the greatest weakness of PIPEDA in addressing online privacy threats is its notoriously weak enforcement regime. First, the Act is designed to encourage well-intentioned businesses to respect consumer privacy by establishing policies and procedures that protect personal data from abuse. It is not designed to deal with bad actors who seek to exploit consumers and who pay little heed to the law. In particular, it gives the Commissioner no powers to enforce the law against recalcitrant businesses other than through publicity (which is effective only with respect to companies that care about such publicity) and costly court actions.

But even in respect of established businesses who value their reputations among regulators and consumers, the record to date suggests poor levels of compliance. CIPPIC's 2006 study of online retailers, conducted with funding from the OPC, indicates widespread non-compliance with PIPEDA's requirement for consent, among others.[287] The study, the first ever significant survey of business compliance with the Act, assessed a total of 64 retailers, including large as well as small organizations. This may not be surprising, given that there are no penalties for most forms of non-compliance under the Act unless an individual (or the Commissioner) takes the matter to Federal Court and obtains a court order for damages. Individuals can do this only after they have complained to the Commissioner and obtained a report on their complaint, which reports typically take 16 months.[288] But it will be the very rare individual for whom the cost of a court action is worth the potential damage award. There is no provision for class actions, no provision for punitive damages, and no protection from adverse cost awards for complainants who act responsibly and have a *bona fide* complaint under PIPEDA. Hence, it is no surprise that few cases have been brought in Federal Court under PIPEDA. This is simply not an effective enforcement mechanism.

Others have noted that under the current regime, "regulated parties are able to ignore the Commissioner's decisions with impunity",[289] "[business] implementation of the PIPED Act has been *ad hoc* at best and non-existent at worst",[290] companies found in violation of the Act remain non-compliant,[291] and "for many organizations privacy compliance has ceased to be a serious legal obligation. Instead, for many it is considered a business risk that carries no realistic expectation of serious financial consequences or diminished reputation — a risk that can be managed through minimal compliance and contrition if caught".[292] Based on the known facts, which have not be contradicted, there can be little dispute that the current model is insufficiently effective and that change is needed.

---

[287] CIPPIC, *Are Retailers Measuring Up?*, note 283 above.
[288] Privacy Commissioner of Canada, 2006 Annual Report <http://www.privcom.gc.ca/information/ar/200607/2006_pipeda_e.asp>
[289] BCCLA, *Securing Compliance, Protecting Privacy: The PIPEDA Enforcement Evaluation Project* (March 2006), p. 83.
[290] "*Implementing PIPEDA: A review of internet privacy statements and on-line practices",* University of Toronto Centre for Innovation Law and Policy (May 6, 2005), quote from Executive Summary; <http://pipedaproject.rcat.utoronto.ca/>
[291] John Lawford, *Consumer Privacy under PIPEDA: How are we doing?* (PIAC: Nov.2004), pp.44-55.
[292] Michael Geist, "Rising to the Privacy Reform Challenge", *Toronto Star* (Oct.25, 2004).

In its submissions to the Parliamentary Committee,[293] CIPPIC proposed a number of amendments designed to improve industry compliance with the Act. These included:

- Commissioner use of the subs. 20(2) power of publicity to "name and shame" organizations who fail to comply with the Act;
- greater Commissioner use of audit powers both for random "spot checks" and for more in depth audits of organizations against whom complaints have been made;
- providing the Commissioner with order-making powers (as is the case in all three provinces with similar data protection laws);
- establishing a new Tribunal with order-making powers, to which complainants and/or the Commissioner can take unresolved complaints and obtain damages;
- providing individuals and classes of individuals with a statutory right of action through which they can hold organizations accountable and obtain damages;
- allowing organizations (e.g., CIPPIC) and groups of individuals to lodge complaints and obtain injunctive relief on behalf of others;
- allowing for punitive as well as compensatory damages; and
- treating wilful contraventions of the Act and/or failure to comply with Commissioner orders as offences, subject to financial penalties.

CIPPIC noted in its submissions that these options are not mutually exclusive, and that a combination of approaches is likely to be most effective. Unfortunately, however, neither the Parliamentary Committee nor Industry Canada appear interested in reforming PIPEDA in ways that would give it more teeth. The Committee (and the government in its response) addressed only two of CIPPIC's proposals: giving the Commissioner order-making powers, and making Commissioner use of the subs.20(2) "naming" power mandatory in cases of non-compliance (Recommendations 18 and 19 of the Committee Report). Both were rejected by the Committee, and subsequently by the government. None of CIPPIC's remaining six proposals for more effective compliance incentives and enforcement of the Act were even acknowledged by the Committee or the government, despite the fact that they offer low cost and potentially effective means of improving compliance with the Act.

F Challenges with Cross-Border Enforcement

Many, indeed most, of the threats outlined earlier in this report operate in cyberspace, across state borders. This creates tremendous challenges for law enforcement authorities as well as individual consumers who wish to pursue online entities based in other jurisdictions. Such challenges are no less for the Privacy Commissioner in respect of PIPEDA enforcement than they are for other agencies seeking to protect consumers from cross-border fraud and other illegal activities.

Although the Commissioner can in many cases gather sufficient evidence through simple online investigations to render a finding under PIPEDA (and thus avoid the difficulties

[293] Canadian Internet Policy & Public Interest Clinic, *Submission to Industry Canada on PIPEDA Reform Issues* (January 15, 2008).

involved in attempting to exercise investigatory powers extra-territorially), that finding will have even less influence over a foreign-based entity than it will over an entity based in Canada. And even if the finding were confirmed by the Federal Court in a binding court order, such orders are much more difficult to enforce extra-territorially than within Canada.

Perhaps the most promising approach to cross-border enforcement of privacy laws is cooperation with foreign government agencies with similar mandates, such as the FTC in the U.S.A., and competition authorities and data protection commissioners in Europe and elsewhere. We understand that efforts are underway to facilitate such international cooperation through the OECD, APEC, and other organizations (see above).

Conclusion: Meeting the Threat

There is no one online threat to Canadians' privacy; rather, there are many, with different objectives and from different sources. Similarly, there is no single technology that can protect Canadians' privacy online – there are many, and each is imperfect and offers only partial protection. These features of online privacy threats mean that there can be no single solution to the problem of protecting Canadians against online predation. Rather, online privacy protection will come about by addressing online privacy threats from multiple angles.

First, one must take responsibility for one's own protection. This involves, first, educating oneself about the nature of online privacy threats implicit in one's online activities, and, second, adopting good security practices. As this report has seen, many organizations make good information on online safety available to individuals. Similarly, there are many tools available to the public for securing their desktops. Every internet user should use anti-virus, anti-spyware, and anti-phishing tools as well as a firewall. Individuals operating online websites or servers should take steps to ensure that those spaces are secure against third parties who might seek to use those resources to, for example, send out spam.

Second, organizations must take responsibility for their customers and patrons by protecting them against online privacy invasions. Banks and ISPs already make resources available to consumers to educate them on online risks. Self-regulatory bodies can help ensure that organizations adopt best practices that place security first. Technology firms can continue fighting fraud and other online threats with innovative and affordable security tools that internet users can use to protect themselves.

Third, our governments, law enforcement agencies, and consumer and citizen protection agencies can address online privacy threats in a variety of ways. Public education materials from trusted sources such as law enforcement and the privacy commissioners' offices carry the weight of their offices, and are often the first place consumers will turn to for guidance on how to protect themselves. Enforcement of existing laws, and creation of new laws where warranted, can obviously have a tremendous impact on wrongful online activity. Government can also play a leading role in bringing about change without legislation. As the Canadian government did with the Anti-Spam Task Force, the government can bring stakeholders together to encourage the adoption of measures – whether self-regulation, best practices, or consumer education – necessary to battle specific online privacy threats. Government can also look internationally to other nations for solutions. Online threats to privacy know no borders; accordingly, solutions to many of the challenges facing Canadians online can only come about with international co-operation amongst many nations.