The *Protecting Canadians from Online Crime Act* and Law Enforcement Access to Information Held by Third Parties

Prepared For: Legal Education Society of Alberta

Search Warrants

Presented by:

Dane Bullerwell

Pringle Chivers Sparks Teskey

Edmonton, Alberta

For Presentation in:

Edmonton – February 19, 2016

Calgary – February 26, 2016

THE *PROTECTING CANADIANS FROM ONLINE CRIME ACT* AND LAW ENFORCEMENT ACCESS TO INFORMATION HELD BY THIRD PARTIES

A. THE IMPORTANCE OF "THIRD PARTY INFORMATION"

For centuries, law enforcement officials in common law jurisdictions had essentially a single option when they hoped to lawfully access an individual's private documents: they could obtain a search warrant that would allow them to enter a person's home or business. Then, in accordance with the terms of the search warrant, the police could seize and read any private papers they found. This was the state of the law by at least 1765, when King George III's messengers broke down John Entick's door in search of seditious papers. In the ensuing civil lawsuit, Lord Chief Justice Camden demanded to know the legal authority for the messengers' trespass, even where the trespass came under royal imprimatur. As the Lord Chief Justice solemnly intoned: "*Papers are the owner's goods and chattels: they are his dearest property, and are so far from enduring a seizure that they will hardly bear an inspection. … If suspicion at large should be a ground of search … whose house would be safe?*"[1]

Over the latter half of the 20th century the informational privacy landscape evolved dramatically. The law of property and the tort of trespass no longer defined our reasonable expectations of privacy. An increasingly interconnected and information-driven society saw Canadians begin to share vast quantities of highly personal records with third parties. Accountants, bankers, counsellors, and physicians became custodians of vast troves of personal information. Technological developments – most importantly, the proliferation of powerful and interconnected computers – made it much easier for governments and private organizations to collect, store, analyze, and share our personal information. The categories of personal information maintained by third parties quickly multiplied. Phone companies began keeping records of those with whom we spoke. Banks and credit card companies started keeping records of where and when we spent our money. Credit bureaus, advertisers, retailers, and data brokers began collecting enormous troves of information about our finances, purchasing preferences, and personal habits. Our personal information was no longer always kept safely ensconced in our desk drawers and filing cabinets. Instead, private information was increasingly stored in the offices and data centres of governments and businesses.

Informational privacy developments moved into warp speed during the first two decades of the 21st century. Today, it seems as though personal information is created by almost everything and stored almost everywhere. This is in no small part due to the near-ubiquity of computers and the Internet. Nearly everything we do using computers has the potential to create electronic records, and

1 ***Entick v Carrington*** (1765), 95 ER 807 (KB).

computers are embedded inside nearly everything. Technology and privacy guru Bruce Schneier has quipped that "data is the pollution problem of the information age,"[2] since data is a natural byproduct of the socially beneficial aspects of computing.[3] In an era of extraordinarily cheap computing power and seemingly inexhaustible data storage it is now trivially easy for all sorts of hardware, software, and third party services to keep tabs on everything we do, and then squirrel these records away on a hard drive indefinitely. A few everyday, real-world examples – some of which might have shocked the public as recently as a few decades ago – help drive this point home:

- Our cell phones constantly transmit our location to our cell phone companies, which keep historical records of our every movement;
- Map services and GPS wayfinding phone aps (such as Google Maps) transmit our location back to a central server, both to provide users with updates on traffic conditions and to allow for location-based advertising;
- The contents of our cell phones and laptops (including data such as photographs, contact lists, and Internet browsing records) are routinely backed up and stored on servers that are maintained by electronics manufacturers (such as Apple);
- Internet Service Providers (ISPs) keep a record of every website we visited (and when), and the websites themselves also keep records of the pages we access – and even how long we have lingered on particular topics;
- Our emails and most other forms of personal electronic correspondence are stored on computer servers that are maintained by third parties, such as our employers or ISPs;
- Social networking websites (such as Facebook) maintain a database of our friendships, keep track of the events we plan to attend, record the physical locations where we "check in," and store some of our most personal photographs;
- Our health records are maintained in central databases (such as Alberta's NetCare system), which are readily accessible to any number of service providers;
- E-books readers (such as Amazon's Kindle) keep a record of which pages we have read, and newspaper websites maintain records of the stories that have held our attention; and
- Wearable personal fitness devices (such as Fitbits) transmit personal data (such as GPS location data, steps taken, calories burned, and sometimes even a record of when the wearer has sex) back to a corporate server, ready to be analyzed and accessed later.

2 Bruce Schneier, "The Future of Privacy" (6 March 2006), available online: <https://www.schneier.com/blog/archives/2006/03/the_future_of_p.html>.

3 Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (New York: WW Norton & Co, 2015) at pp. 20-32.

The development of "cloud computing" has further muddied the informational privacy waters. While at one time we could at least be assured that third party record-holders would keep our records inside Canada – and therefore remain subject to Canadian privacy law and Canadian rules of criminal procedure – personal data now knows no borders.[4] The computer server where you back up your photographs could as easily be in Cupertino as in Calgary. The web application an Alberta employer uses to manage its payroll might process employees' banking information using Amazon's popular cloud computing service, which runs data centres in jurisdictions as varied as Oregon, California, Virginia, Brazil, Ireland, Germany, China, South Korea, Japan, Singapore, and Australia.[5] The iPhone app that you use to keep track of your fitness regime might store your workout data in Dublin, Dubai, or both places. The physical location where data is stored has lost much of its legal relevance now that information is accessed worldwide, instantaneously and with the click of the mouse.

Although the Internet age's rapid technological developments have improved our quality of life, they have also created privacy risks described using Orwellian language. With so much personal information recorded and shared, it is no longer dystopian science fiction to suggest that, left unchecked, malevolent record-holders, service providers, or governments could use this information to paint a detailed portrait of our most intimate thoughts, movements, and actions. As privacy scholar Prof. Neil Richards has summarized the modern era: "The scope and variety of the types of surveillance that are possible today are unprecedented in human history. This fact alone should give us pause."[6]

Edward Snowden's well-publicized leaks have revealed how electronic surveillance scales exceptionally well. While it was once tedious and expensive for the state or private actors to conduct widespread surveillance, technology has reduced the marginal cost of electronic snooping to near-zero.[7] Surveillance no longer requires undercover officers to follow suspects. Detectives no longer need to spend sleepless nights sifting through bankers' boxes of seized documents. Computers can now take care of many of the boring and repetitive tasks of information collection and analysis.

---

4 On the topic of cloud computing, see generally: Office of the Privacy Commissioner of Canada, *Introduction to Cloud Computing* (October 2011), available online: <https://www.priv.gc.ca/resource/fs-fi/02_05_d_51_cc_e.asp>, and Ann Cavoukian (Information and Privacy Commissioner of Ontario), *Privacy in the Clouds: Privacy and Digital Identity, Implications for the Internet* (28 May 2008), available online: <https://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=748>.

5 See Amazon Web Services, "AWS Global Infrastructure", available online: <https://aws.amazon.com/about-aws/global-infrastructure/> (accessed 31 January 2016).

6 Neil Richards, "The Dangers of Surveillance" (2013), 126 *Harvard Law Review* 1934 at p. 1936.

7 See Schneier, *Data and Goliath* at pp. 33-45.