Deputizing the Private Sector

Requiring the Collection of Personal Information by
Non-Governmental Entities for Law Enforcement or Other Purposes

Robert Gellman, Stephanie Perrin and Jennifer Barrigar
Digital Discretion Inc.

May 2015

An Independent Research Report Commissioned by the
Office of the Information and Privacy Commissioner of Alberta

Digital Discretion Inc.
P.O. Box 183, 155 MacFarlane Street
Pakenham, ON, K0A2X0
www.digitaldiscretion.ca
stephanie@digitaldiscretion.ca

Table of Contents

Executive Summary

The collection of personal information for public policy purposes always raises privacy issues. Who collects and maintains the information is one of those issues. Government may collect personal information itself or it may require a non-governmental entity to do the collection. Because different privacy laws apply to the government than to the private sector, the choice has consequences for the privacy rights of individuals.

The focus of this report is on the decision to ask a private sector entity to collect data rather than requiring a government agency to do the collection. What factors should be considered when evaluating a choice about who should undertake a personal information collection?

Part I sets out in more detail the background, the stakes and the framework for discussion.

Part II briefly reviews issues raised by the *Canadian Charter of Rights and Freedoms*.

Part III offers specific examples of information collection choices made in Canada and elsewhere. Many of the examples are some form of "know your customer" (KYC) obligation, where the law requires a business to collect and maintain identifying and other information about customers, often including information that would not be collected otherwise. The privacy terms of these laws vary considerably.

Part IV begins by discussing the circumstances and elements to consider when evaluating an information collection decision. It suggests privacy measurement standards that will help to identify and assess the privacy consequences of asking a private sector entity to collect personal information, rather than having a government agency collect the information. The fifteen standards are stated as either/or propositions, but each is more likely to be applied along a sliding scale.

Part IV concludes by focusing on processes and procedures for conducting an evaluation of a decision. The goal is to offer methods, approaches, and courses of action for privacy regulators, legislators or others to consider when evaluating choices about personal information collections. It is a checklist of ideas, although each idea may not be appropriate in every case.

I. Introduction

Alberta's *Freedom of Information and Protection of Privacy Act* (FOIP Act) establishes standards for the protection of personal information as well as citizen access to government information. General information policy statutes recognize, as they must, that the need for privacy and for access must yield at times to competing interests and policies. Without doubt, the legislature may identify overlapping public concerns, weigh the merits and determine how to change the law in light of new developments. Rulemaking and other administrative activities may also seek to adjust privacy in some way. Nevertheless, piecemeal changes that alter well-crafted, high-level policies present their own challenges and consequences.

The purpose of this report is to explore one major category of proposals that may affect implementation of Alberta privacy law and practice. When the legislature chooses to impose a personal data processing obligation on a non-governmental entity rather than on a government entity, privacy consequences – intended and unintended – may follow from the decision, especially if the choice involves a deviation from the general privacy rules that would otherwise apply. Administrative requirements for information collection through regulations, contracts, joint activities and other mechanisms can shift aspects of personal data processing to a non-governmental entity too, with consequences for privacy.

The important point is that the choice of who does the collection may determine which privacy law applies and therefore the privacy rights and procedures available to citizens. The choice of information collector is consequential. This report seeks to assist privacy regulators, legislators and others in evaluating those consequences for decisions about the collection of personal information.

The important point is that the choice of who does the collection may determine which privacy law applies and therefore the privacy rights and procedures available to citizens.

The focus here is narrow, but there is a broader context. Jon Michaels, an American law professor has written broadly about privatization, the contracting out of government services to the private sector. His writings take a much bigger bite of the issue than this report's more narrow focus. However, his observation that privatization can alter policies that might be otherwise applicable has some relevance here.[1]

Michaels calls these activities "workarounds", government contracts that allow an outsourcing agency to achieve public policy goals that, but for the outsourcing, would be impossible or much more difficult to attain in the ordinary course of operations. In the Canadian context, we need to consider whether the "workaround" might be depriving citizens of rights guaranteed by the Charter, or whether an agency deputized the private sector to do a task that either would not pass the

[1] Jon D. Michaels, *Privatization's Pretensions*, 77 University of Chicago Law Review 717 (2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1696309.

legislature, or was otherwise impossible under existing law or policy. For our purposes, whether workarounds intentionally achieve particular results or whether the results are incidental, the effects on privacy can be the same. The point is that the shifting of functions, whether by legislation, privatization or otherwise, can change the way privacy laws apply and affect the rights of individuals.

If the government requires a non-governmental entity to collect personal information, that assignment may be neither unusual nor inherently sinister. A legitimate law enforcement, national security, public health or other purpose may be accomplished through a non-governmental entity. The government may tell others to undertake an information collection activity function rather than undertake the function on its own for a variety of reasons. The reasons may include efficiency, impossibility of government doing the function itself, or creating a barrier or arms' length relationship between the information and government in the interest of privacy. A decision to accomplish an information collection through a non-governmental entity is the starting point for discussion here, and it is not our purpose to consider, evaluate or question justifications for the decision. Our focus is on identifying and evaluating the privacy consequences of that decision with the goal of informing the debate.

When the easy privacy answer – do not collect personal information at all – is not acceptable, one question may be who should undertake the task, government or someone else. An example will make the point clearer. Assume that a government sees the need to monitor cars entering commercial parking garages. The legislature could direct a government agency to erect an automatic license plate recognition camera on a public street to record each car entering or leaving a merchant's garage. Alternatively, the legislature could direct the garage owner to record the same information using its own capabilities and then to hold the records for possible use by the police or other government authorities. In both instances, the same information is collected, but the privacy consequences differ.

If, for example, an Alberta government agency collected the personal data on its own, the activities of the agency would be subject to all the laws, procedures and rights of data subjects in the FOIP Act. However, the privately collected information is subject to the privacy rules in the *Personal Information Protection Act* (PIPA). (For a comparison of Alberta's FOIP Act and PIPA, please see the appendix.) Regardless of the choice made, the decision could include additional deviations – enhancing or undermining privacy – from otherwise applicable privacy rules. Separate sectoral laws on privacy may also be factors that influence the decision. The purpose here is to identify and focus on the privacy consequences of these types of data processing choices.

Before we proceed, here are some preliminary matters relating to boundaries and definitions. Personal information management includes activities related to the collection, use and disclosure of information. All of these activities may be relevant at times to our discussion, but our primary focus is on collection of personal data because collection initially raises concerns, with other privacy processing and consequences following collection decisions.

Government may impose an information collection function on another entity through various means. Some activities may represent a formal delegation of a government responsibility. Some collections may be the result of legislation or regulation. Some collections could come in the form of contracts, joint efforts or other assignments. The common thread is that a non-governmental entity

(typically a private sector company) undertakes the collection of personal information rather than the government doing the collection itself.

We note that issues of cost and unfunded mandates are relevant to these decisions, but they fall outside the immediate zone of interest of this analysis. Nevertheless, insufficient funding for proper information management may add additional risk, particularly in situations where there are new responsibilities.

The appendix to this report includes a summary table of Alberta's FOIP Act and PIPA. If we paused to review the legislative differences in detail, the discussion would exceed our charge, provide little value to provincial privacy regulators, and overwhelm the rest of this report. In any given context, evaluating the manner in which privacy laws apply requires deconstructing the elements of the data processing and matching the elements to the relevant laws. It is enough here to note that there are two general privacy laws (plus other sectoral laws not expressly considered here) with somewhat differing standards. Assigning an information collection function to government or to the private sector may apply one law rather than the other. Some services contracted out by the government may remain subject to the FOIP Act. The possibility also exists that both laws may apply in some fashion to a joint activity, or that an activity could escape coverage under the scope of a particular choice.

Another consequence of personal data collection is a tendency for data compilations to attract new uses and new users. Governments have historically been somewhat constrained in their ability to process personal data, usually by constitutional limits, enabling legislation, privacy legislation, expenditure justification or public concern. Those constraints do not always prevent new uses of personal data within government. Private sector companies have different limits on their personal data processing than government agencies and may have different incentives to find new ways to exploit data. They are accountable to shareholders, not citizens.

Another consequence of personal data collection is a tendency for data compilations to attract new uses and new users.

In identifying and evaluating the privacy consequences of an information collection decision, this report reviews examples from Alberta, the rest of Canada and other jurisdictions. We also offer a set of standards to help distinguish between collection decisions that are potentially more consequential for privacy and those that are less so. The final section also discusses processes and procedures that might be useful in evaluating collection proposals. A systematic approach to evaluation focuses attention on the most important issues and leads to more consistent and more complete responses.

Determining the scope of our discussion is a final preliminary matter. We need to identify data collection choices that affect personal data and that have the potential to be more consequential from a privacy perspective. Some government activities affect private sector (and governmental) data activities in indirect ways. For example, a statute of limitations for contract disputes has the effect of setting a standard for record keeping. This type of general legislative policy draws a line that needs to be drawn. For our purposes, it falls at the lower end of the privacy scale because those who contract with consumers are likely to keep personal information related to those contracts until the

possibility of legal action has passed. The statute of limitations does not assign collection as much as it draws a line around it.

On the other end of the scale are laws that expressly require a business to collect more consumer information. These so-called "know your customer" (KYC) rules result in the creation of personal information pools that would likely not exist but for the KYC requirements. This information is subject to private sector privacy rules rather than the governmental privacy rules. Many but not all of the examples in this report are forms of KYC requirements.

On the other end of the scale are laws that expressly require a business to collect more consumer information.

Another category involves mandatory collection of data that a record keeper would collect and maintain regardless of any government requirement. Consider a rule that obliges a physician to report to a public health authority information about a patient with a communicable disease. The physician would maintain diagnostic and treatment information regardless of the public health reporting requirement. The report itself may well be consequential to the patient in a variety of ways, including privacy. For present purposes, however, the privacy interest here falls at the lower end of the scale because the reporting does not significantly change the applicable privacy regime for the physician's record. The mandated information collection and reporting is not material for our purposes.

Government purchasing activities may also indirectly affect private sector activities. The government's use of the telephone system supports the production of telephone directories with personal information. However, the directories would exist regardless of the government's patronage so the government's actual influence on data processing is marginal at best. The same may be true for when the government purchases some personal information or personal information services. An agency looking for a current address of an individual may use the resources of a data broker. The data broker offers its services to all, and the government is just another customer, not assigning government functions to anyone.

The situation could be different if the government hires a contractor to manage a government program involving the processing of personal information. If the contractor operates the program under the same privacy rules applicable to the government, the activity might not be of great interest here. If, however, the contractor can process some or all of the personal information without regard to the FOIP Act, the change in the applicable privacy regime from the FOIP Act to PIPA would be of greater interest for that reason.

Greater complexity can result because activities do not always fall cleanly into a "government box" or a "private sector box". As later examples show, some personal information processing is the consequence of joint activities that result in different flavors of joint processing that may be voluntary, contractually based, expressly required by law or otherwise. For some activities, only detailed deconstruction of data flows and statutory obligations will identify the privacy differences with precision.

We offer an additional thought about risks. Notwithstanding the high profile debates about outsourcing personal data processing to international businesses, having a private sector company

processing the data may not be intrinsically more risky than having government employees perform the tasks. The private sector may have better security, training and service standards. An examination of the likely risks may be appropriate.

We have not found a clear line or simple test that will automatically distinguish a personal information activity that is consequential from one that is not. Awareness of the general concerns, vigilance in looking for proposals and actions that affect privacy and the general privacy framework, and good judgment are valuable attributes in this endeavour.

II. Charter Application to Information Sharing Decisions

The *Canadian Charter of Rights and Freedoms*[2] (Charter) protects the fundamental rights and freedoms of persons against state action. Section 32 provides:

> 32. (1) This Charter applies
>
> a) to the Parliament and government of Canada in respect of all matters within the authority of Parliament including all matters relating to the Yukon Territory and Northwest Territories; and
>
> b) to the legislature and government of each province in respect of all matters within the authority of the legislature of each province.

The Supreme Court of Canada (SCC) interpreted this clause to mean that the Charter applies to all laws created by the executive, administrative, legislative[3] and judicial[4] branches of government. Although the Charter applies to rules and regulations created by government actors, it does not cover common law situations between individuals or private actors.[5]

In a situation where government deputizes or otherwise offloads information collection, use or disclosure to third parties, there are two potential avenues by which that seemingly private actor might fall under the Charter. The first is where the actor is held to be a government actor itself. The second is where, despite the nature of the organization, the activity is in furtherance of a government program or policy.

Government actors are determined by reviewing the institutional or structural links between the body and the government, using the "effective control" test. This test examines: (1) whether a law

---

[2] *The Constitution Act, 1982*, Schedule B to the Canada Act 1982 (UK), 1982, c 11, http://canlii.ca/t/ldsx.

[3] *RWDSU v. Dolphin Delivery Ltd.*, [1986] 2 S.C.R. 573.

[4] *R. v. Rahey* [1987] 1 S.C.R. 588.

[5] Despite finding that the Charter did not apply to such situations, the Court suggested that interpretation and application of the common law should be in accordance with the principles and values set out in the Charter even though the Charter did not govern the situation, *RWDSU v. Dolphin Delivery Ltd.*, [1986] 2 S.C.R. 573.

directs how the institution will operate; (2) the degree of involvement between governance and government (e.g., does the government appoint the majority of the institution's board of directors?); and (3) the degree of independence from government. Under this analysis, crown corporations and public agencies are government actors. A community college in British Columbia is a government actor,[6] but under other circumstances both a university and a hospital had sufficient independence to avoid classification as government actors.[7]

There is also the possibility that a body may not be a government actor and yet an activity could be covered by the Charter because the activity is in furtherance of government powers or policies as shown by the exercise of statutory authority. This was the case in *Eldridge v. British Columbia (Attorney General)* [8], where the failure of a hospital to provide sign language interpretation for the deaf community was challenged as contrary to the equality provisions of the Charter. Although the hospital was not a government body, the SCC concluded that the Charter applied to the activity because the hospital acted under statutory authority. While the legislation required only that the hospital determine what benefits to provide, it was the assertion of statutory authority that brought this under the rubric of the Charter, meaning that the hospital's decisions had to be consistent with the Charter. In the decision in *Eldridge*, LaForest references his own statement in McKinney that: "[i]t would be strange if the legislature and the government could evade their Charter responsibility by appointing a person to carry out the purposes of the statute".

The Charter may apply to a seemingly non-governmental body when either (a) the alleged Charter breach comes as part of the exercise of statutory authority; or, failing that, (b) where the "effective control" test characterized the body as essentially governmental after all.

III. Personal Information Collection Examples

Examples of information collection choices provide a better and deeper understanding of the issues and current practices. These examples come from a wide variety of jurisdictions and illustrate choices made in the past with respect to the structure and location of personal data processing activities. Whether the privacy consequences received attention when the decisions were made is unknown. Many, but not all, of the examples are some form of KYC requirements, but the specific purposes vary somewhat. Other examples of collections serve other objectives such as monitoring school vaccinations, law enforcement or public safety, and a variety of highway travel purposes. Many other examples exist. The goal here is to establish a firm foundation for the discussion in Part IV of this report that addresses privacy standards for assessing decisions as well as procedures for evaluating them.

---

[6] *Douglas/Kwantlen Faculty Assn. v. Douglas College*, [1990] 3 S.C.R. 570.

[7] *McKinney v. The University of Guelph* [1990] 3 S.C.R. 229; *Stoffman v. Vancouver General Hospital* [1990] 3 S.C.R. 483.

[8] *Eldridge v. British Columbia (Attorney General)* [1997] 2 S.C.R. 624.

A. FINTRAC

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) is responsible for the collection, analysis and disclosure of information to assist in the detection, prevention and deterrence of money laundering and terrorist financing in Canada and abroad. FINTRAC operates under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.[9] The Act imposes collection duties on multiple private sector organizations. For our purposes, we select from the list of organizations only financial entities, money services businesses, real estate brokers, and dealers in precious metals and stones to serve as exemplars.[10]

Some provisions of the Act require affirmative reporting to FINTRAC of activities such as large transactions and suspicious transactions. At a high level of generality, these reporting requirements are similar to governmental reporting requirements by employers (e.g., wage reporting about employees) and many other examples. To accomplish express statutory purposes, it is common for governments to require non-governmental entities to report personal information. For information about individuals[11] that must be affirmatively reported to a government agency, the information in the hands of the recipient agency becomes subject to the privacy requirements generally applicable to government.[12] We can set aside reported information held by government agencies as beyond the focus of this report. However, it will be true that entities making reports to government – especially reports of large or suspicious transactions – will maintain copies of those reports. The additional privacy consequences of that maintenance over and above records that would be otherwise maintained are not easy to assess.

Other provisions of the Act call on private entities subject to FINTRAC to collect and maintain information in connection with their activities. The details vary, and the description here is selective. Banks must keep account operating agreements, client credit files and cleared cheques. Money services businesses must keep records about money transfers, sale of money orders and traveler's cheques and client credit files. Real estate brokers must keep client information including name, address and date of birth. Dealers in precious metals and stones must keep business relationship records for the purchasing and selling of precious jewelry, metals and stones.

An entity subject to FINTRAC must also ascertain the identity of an individual who is a customer. These are KYC requirements. Ascertaining identity requires an entity to review a birth certificate, driver's licence, passport, record of landing, permanent resident card, or other similar document issued by a provincial, territorial or federal government and that contains a unique identifier

---

[9] SC 2000, c 17, http://laws-lois.justice.gc.ca/eng/acts/P-24.501/.

[10] The Financial Transactions and Reports Analysis Centre of Canada maintains numerous documents describing FINTRAC data collection and reporting requirements at http://www.fintrac.gc.ca/intro-eng.asp.

[11] Information collected about legal persons other than individuals is not within the scope of this report.

[12] Records obtained by FINTRAC are subject to disclosure limits. See FINTRAC, *Guideline 1: Backgrounder* at 6.4 (2010), http://www.fintrac.gc.ca/publications/guide/Guide1/1-eng.asp#s6-4.

number.[13] An entity must maintain records and provide them to FINTRAC within 30 days of a request. An entity must also keep many required records for five years after completion of a transaction, closing of an account or similar event.

The client identification requirements of FINTRAC result in the collection of identification numbers or copies of documents that might not otherwise be kept or maintained. Even if the law does not require maintenance of copies of identification documents, entities with conservative legal staffs may insist on maintaining copies as specific evidence of compliance. Similarly, the requirement to keep client identification information up to date – an activity that varies with an entity's risk assessment of the client – may result in collection and maintenance of additional personal information. An entity that interacts infrequently with clients is more likely to maintain outdated personal information. A FINTRAC covered entity may also have a tendency to keep personal information longer than required.

The application of money laundering requirements to a broad range of businesses means that we cannot fully explore the privacy consequences here. Banks would, even without formal requirements, collect and keep some information about clients as a routine part of their operations. Banks also generally have trained staff (e.g., privacy officers and security officials), maintain high levels of computer and other security, undergo regular audits and interact with customers on a regular basis. As a result, privacy and security practices at banks are likely to be better than elsewhere. Some money services businesses may have controls that are more like banks, but much may depend on the size of the business. Real estate brokers are likely to vary in size more than banks. Their institutional capacities to protect information are also likely to be variable. They may only interact with clients intermittently, perhaps with years between contacts. Client relationships for brokers may be more unstable than for banks. Dealers in precious metals and stones will also vary in size, have different patterns of interactions with clients, maintain limited security capabilities and have variable effective privacy resources. Employees of the dealers may have little privacy awareness and training. Data subjects seeking notice, access or correction are likely to find the capabilities of the different regulated entities to be widely variable.

FINTRAC regulations tell regulated businesses to maintain an effective record-keeping system to enable FINTRAC access to records in a timely fashion.[14] The regulations are silent on any privacy obligations that attach to records kept by regulated entities because of FINTRAC reporting or mandated record keeping so standard private sector privacy legislation rules apply. As in the case of banks, the federal *Personal Information Protection and Electronic Documents Act* would apply. The maintenance of identification information or copies of identification cards may exacerbate the consequences of a data breach by providing potential identity thieves with additional useful

[13] An entity can use a social insurance number (SIN) card to ascertain the identity of an individual, but entity cannot provide the SIN number to FINTRAC in any report.

[14] See, e.g., FINTRAC, *Guideline 6I: Record Keeping and Client Identification for Dealers in Precious Metals and Stones* at § 7 (2014), http://www.fintrac.gc.ca/publications/guide/Guide6/6I-eng.asp#s77.

information.[15] In some cases, the information maintained because of FINTRAC requirements would be substantially the same even without FINTRAC. However, the recording and maintenance of information in other cases may be novel. If so, data subjects will find their personal information in the hands of additional third parties, data may be more readily accessible to government agencies with limited procedural protections, and the privacy risks may be generally enhanced and expanded. FINTRAC retention rules may also result in the maintenance of some personal information for a longer period than might otherwise apply.

B. Bar Patrons

A different form of a KYC obligation arises with the verification of age of patrons of bars. This common practice is sometimes subject to regulation. In Alberta, the *Gaming and Liquor Act* allows but does not require licensed premises to collect limited personal information from patrons.[16] When collection occurs, a licensee can only keep a patron's name, photograph and age (but not date of birth). A licensee may not scan an identification card if it collects additional information. Information collected is subject to PIPA. The full range of privacy obligations and protections under PIPA applies with additional limits specified in the *Gaming and Liquor Act*. A licensee may only use the information collected to decide whether to allow an individual into the premises. Other uses require consent. A licensee may disclose the information to police upon request or under specific circumstances to other bars. A licensee must provide notice to patrons, must protect the information against loss, theft or improper use, and must grant patrons access to their own information. A licensee may retain personal information for as long as is reasonable for legal or business purposes.[17]

A law in the state of Utah in the United States (U.S.) requires a licensee serving alcohol to check the age of younger-looking patrons by verifying the validity of proof of age electronically.[18] The verification system must be able to store name, date of birth, age, expiration date of the identification card, gender, and time and date of scanning. Security measures must ensure that a licensee only uses the information for purposes of verifying age and that the period for data retention is only seven days after the date of scanning. A licensee may not retain the information for mailing, advertising or promotional activity, and may not use the information to make inappropriate personal contact with

---

[15] This point is included in a recent report from the State of California on medical identity theft. The report approves of the collection of identification details, including a photograph, for use in identifying patients. However, the report expressly advises against maintaining a copy of an identification card. California Department of Justice, Medical Identity Theft Recommendations for the Age of Electronic Medical Records 14 (2013), http://bit.ly/1eup6NO.

[16] RSA 2000, c G-1, § 69.2 (2013), http://www.canlii.org/en/ab/laws/stat/rsa-2000-c-g-1/latest/rsa-2000-c-g-1.html.

[17] See generally, Office of the Information and Privacy Commissioner of Alberta and Alberta Gaming and Liquor Commission, *Guidelines for Licensed Premises: Collecting, Using and Disclosing Personal Information of Patrons* (undated), http://aglc.ca/pdf/liquor/Licensed_Premises_Guidelines.pdf.

[18] Utah Code § 32B-1-407, http://le.utah.gov/code/TITLE32B/htm/32B01_040700.htm.

the individual. The licensee may disclose records to law enforcement or other investigative agencies in accordance with law.[19]

In both examples, special privacy rules apply to the collection of information by bars. Alberta limits collection and applies PIPA to what is collected with some additional restrictions on use. No general state or federal privacy law applies in Utah, but the statute and administrative rules limit collection (albeit not as strictly as in Alberta). Utah requires erasure of the information within a week, and it expressly prohibits uses for marketing uses and personal contact with the patron. The specialized collection activity required by both laws comes with some additional privacy protections beyond those otherwise applicable. This contrasts with FINTRAC where no additional privacy measures apply to the businesses collecting the information.

C. Narcotics and Over-the-Counter Medications

Canadian law provides that a pharmacist who dispenses a controlled drug (e.g., a narcotic) must record information about the prescription, the patient and the practitioner.[20] Recording of any prescription, like the recording of any medical treatment, is routine practice by health professionals. The legal requirement for maintaining these records is compatible with practice and is of no special interest here.

We can contrast recording of prescription information with the recording of the sale of over-the-counter medications. The latter are not routine, but examples exist. In the U.S., some laws regulate the sale of some non-prescription products. For instance, the reason for limiting sales of some cough remedies is they contain a chemical used in the production of methamphetamine, a dangerous and illegal recreational drug. The law requires a seller of such non-prescription cough syrups to take steps to control sales. These requirements include obtaining a photographic identification card from the purchaser and collecting the purchaser's name and address and the time and date of the sale. The seller must also obtain the purchaser's signature. The seller must keep the recorded information for at least two years.[21] The rules provide that the sale records must be made available "as appropriate" to federal, state and local law enforcement agencies.[22] The rules also impose a privacy obligation on the seller. The information collected may not "be accessed, used, or shared for any purpose" other than for compliance purposes and product recalls.[23]

---

[19] Utah Admin. Code, R81-5-18 (2014), http://www.rules.utah.gov/publicat/code/r081/r081-05.htm#T16.

[20] Food and Drug Regulation, C.R.C., c.870, G.03.007 (2014), http://canlii.ca/en/ca/laws/regu/crc-c-870/latest/crc-c-870.html.

[21] 21 U.S.C. § 830(e).

[22] 21 C.F.R. §1314.45(a) (2014), http://www.ecfr.gov/cgi-bin/text-idx?SID=10ecd81a7448445b72bface9b0b94f98&node=21:9.0.1.1.15.2.50.7&rgn=div8.

[23] Id. at § 1314.45(b).

The U.S. controls on cough syrup purchases are a form of KYC obligation, but with a somewhat different focus. The rules impose limits on sales to the same individual by a given retailer, and the retailer can use the records for that purpose. Because of the widespread availability of the controlled product, a customer can move from one retailer to another to purchase amounts over the limits. The records allow enforcers to track sales across many retailers. Those subject to FINTRAC and to bar patron identification requirements also collect basic KYC identification information, but mandatory recording includes other data (i.e., details of transactions under FINTRAC and age for bar patrons).

The personal information recorded in the U.S. when dealing with cough syrup purchases is only name and address, transaction information, and a signature. While the buyer must present an identification card, the circumstance suggests that copying of the card or even recording the ID number may not be routine, although the law does not expressly prohibit address copying. Verification of credentials is challenging.

The records of cough syrup sales appear to be available to law enforcement officials without any special procedure or prerequisite. On the other hand, the law provides that a seller may not use or disclose the record for any purpose other than law enforcement.[24] The use and disclosure restriction for the required "logbook" is much more privacy protective than that for most transaction records in the U.S., including records of health transactions.[25] However, the rules do not include other privacy elements normally provided for health records, such as notice, security, rights of access or correction, or accountability measures for data subjects. This is a mixed result from a privacy perspective.

D. Video Surveillance Cameras

Use of closed circuit television (CCTV) cameras for surveillance of individuals is now commonplace in Canada and elsewhere. The Office of the Information and Privacy Commissioner of Alberta (OIPC) and the federal Office of the Privacy Commissioner guidance on the use of video surveillance is readily available.[26] Mandatory use of CCTV cameras for recording of individuals in commercial locations is not widespread. Some examples exist. Because CCTV activities have

---

[24] The rule expressly regulates use and disclosure of the information in the required "logbook", but the rule is silent about related transaction records.

[25] Federal rules about the privacy of health records do not apply to records about the sale of over-the-counter medications. See 45 C.F.R. Parts 160-164 (2014), http://www.ecfr.gov/cgi-bin/text-idx?SID=ca74716a4475092dea51f16a2e8bb285&node=45:1.0.1.3.75&rgn=div5.

[26] See http://www.oipc.ab.ca/pages/PIPA/Publications.aspx?id=221 for OIPC guidance, and http://www.servicealberta.ca/foip/documents/SurveillanceGuide.pdf for its recommended use in Service Alberta, *OPC Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities* (2006), https://www.priv.gc.ca/information/guide/vs_060301_e.asp; *Guidelines for Overt Video Surveillance in the Private Sector* (2008), https://www.priv.gc.ca/information/guide/2008/gl_vs_080306_e.asp; *OPC Guidance Documents: Guidance on Covert Video Surveillance in the Private Sector* (2009), https://www.priv.gc.ca/information/pub/gd_cvs_20090527_e.asp.

expanded dramatically in recent years, more requirements for mandatory recording may be forthcoming.

Under the United Kingdom's (U.K.) *Licensing Act 2003*, the police may ask the licensing authority to make CCTV installation a condition of obtaining a license for serving alcohol.[27] The U.K.'s *Data Protection Act 1998* applies to the CCTV images if individuals are identifiable. The licensee can turn images over to the police if necessary for investigating or preventing a crime or apprehending or prosecuting an offender.

In the U.S., mandatory use of CCTV cameras is rare. In Collinsville, Illinois, a municipal ordinance requires every convenience store and gun shop to install and operate a surveillance camera continuously to record all persons entering the business or near the cash register. The business must retain a recording for 30 days. The recordings must be available to the police chief.[28] The ordinance is otherwise silent on use and disclosure of images and on all other privacy issues. As is common in the U.S., no general privacy law or sectoral law applies to the personal information obtained by video recording.

Surveillance can result from joint public-private efforts. A program announced in Milwaukee, Wisconsin uses public and private funds to install cameras in commercial areas. The business installing a camera controls the camera and footage, but police have the right to monitor and review video for public safety purposes.[29]

These first two examples of mandatory cameras fit at different ends of a data protection spectrum for CCTV images. In one case, standard privacy law applies, and in the other, no privacy law applies at all. The Collinsville law allows for overwriting of the images after 30 days, but it does not mandate erasure of older images. In the U.K., the Information Commissioner's Office advises that the law allows retention of images for as long as necessary to meet the purpose of recording them.[30] With the rapid development of facial recognition technology, the ability to derive names and other personal information from an image may be more common in the near future. Important issues regarding CCTV images are the policy for police or other governmental access and whether any formal process or procedure is a prerequisite.

An analyst for the libertarian Cato Institute in Washington, DC, argues that government should not operate or control public surveillance cameras. Instead, he proposes that the government rely on

---

[27] See Information Commissioner's Office, *CCTV in pubs –FAQs* (2009), http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/CCTV_IN_PUBS.ashx.

[28] Collinsville, IL Code of Ordinances, Chapter 5.78 - SURVEILLANCE CAMERAS (23009), http://library.municode.com/index.aspx?clientId=14033.

[29] Milwaukee Wisconsin Journal Sentinel, *Milwaukee's business districts could get more cameras* (June 6, 2013), http://www.jsonline.com/news/milwaukee/milwaukees-business-districts-could-get-more-cameras-b9928179z1-210462761.html.

[30] ICO, CCTV, http://ico.org.uk/for_the_public/topic_specific_guides/cctv.

private sector cameras because the effects on privacy and civil liberties would be less. The main reason is that the information would be in private and not government hands. He cites the Boston Marathon bombing, where a business surveillance camera provided the most useful footage.[31] The point for present purposes is recognition that there is a respectable argument that a delegation of information collection – whether mandated or not – may be more protective of privacy rather than less protective. The details, of course, make all the difference.

The Milwaukee program illustrates how surveillance can result from joint activities that can easily cross the lines between private and public activities with no simple means to determine who is delegating responsibility. If there were applicable privacy laws in Milwaukee, the laws would have to be carefully parsed to determine which law applies to which data at which time.

E. Pawn Shops and Second-Hand Stores

In many jurisdictions around the world, pawnbrokers who provide loans against goods and dealers who purchase used goods from consumers have been required to maintain records about the goods that they purchase in order to discourage trades in stolen property and to assist in police investigations of stolen property. An Edmonton municipal bylaw that dates back to 1913 requires pawnshops and second-hand stores to record the personal information of individuals who pawn or sell items. The bylaw also requires pawnshops and second-hand stores to make this information available to a peace officer upon request.

This bylaw became the subject of a 2008 OIPC order[32] and subsequent court case.[33] The Commissioner found that the city did not have the authority to require second-hand stores and pawnshops to upload the personal information of the pawnshop's customer to a database operated by Business Watch International (BWI), a contractor to the Edmonton Police Service (EPS). The court quashed the OIPC order on a variety of grounds, but the circumstances under which the case arose and its analysis of information flows remain relevant here.

Of particular interest for present purposes is the collection of personal information about customers by a pawnshop subject to the bylaw. The bylaw imposes a type of KYC requirement and the pawnshop operates under PIPA. Both the City of Edmonton and EPS are subject to the FOIP Act. One of the issues in the case was how the differing authorities of the two laws affected the collection

---

[31] Julian Sanchez, The False Security of Surveillance Cameras (undated), http://www.cato.org/publications/commentary/false-security-surveillance-cameras.

[32] Office of the Information and Privacy Commissioner (Alberta), *The City of Edmonton, Edmonton Police Service, Emu Inc. (Carrying on Business as Cash Converters Mill Woods)* (2006), Orders F2007-001, F2007-2, P2007-001 http://www.oipc.ab.ca/downloads/documentloader.ashx?id=2183. A similar case arose in Ontario and was the subject of a complaint and order by the Information and Privacy Commissioner (Ontario), Order MO-2225 (2007), http://www.ipc.on.ca/images/Findings/up-mo_2225.pdf.

[33] *Business Watch International Inc. v. Alberta (Information and Privacy Commissioner)*, 2009 ABQB 10 (2009), http://www.albertacourts.ab.ca/jdb/2003-/qb/civil/2009/2009abqb0010.pdf.

and disclosure of information and which law applied at which time. The Commissioner and the court had different views on this point, and the court's ruling turned on this and other points of which details and resolution are not relevant to this analysis.

Nevertheless, the case remains noteworthy here not because of the differing views or the outcome but because of the careful analysis of the flow of information and the application of privacy laws to the parties to the data collection and use. BWI was the contractor for EPS. The data BWI held included information required to be disclosed under the bylaw as well as information that went beyond the requirements of the bylaw. The court pointed out that volunteered information fell under a different privacy standard than the information required to be disclosed by the bylaw. Another complication was the use of the database for other purposes by the pawnshops.

The specific holdings of the case are not important, but the detailed analysis of the relationship between the parties, the flow of personal information and the application of the two privacy laws is just the type of analysis that may be relevant to decisions about personal information collection. Even the complicating factor of the collection of volunteered as well as mandated information is noteworthy because it illustrates another layer of complexity. As government, contractors, and other third parties increasingly enter into multi-faceted relationships that involve the collection and transfer of personal information among multiple parties, any evaluation of an information collection decision calls for a careful and thorough review of the privacy consequences.

F. School Vaccinations

In the U.S., all 50 states require students entering schools to have vaccinations against certain diseases.[34] All states recognize exemptions for medical reasons, often because of the compromise of a child's immune status by a permanent or temporary condition, because the child has a serious allergic reaction to a vaccine component, or because of a prior serious adverse vaccination event. Most states also allow an exemption for religious reasons. Some state laws require that a family must belong to a religious group with bona fide objections to vaccinations. Others recognize religious exemptions based only on parental attestation based on a religious belief (but not a philosophical, scientific or personal belief). Other states accept a plain statement of religious objection. Some states allow personal belief exemptions.[35]

In Canada, three provinces require proof of immunization for school entrance – Ontario, New Brunswick and Manitoba – but they do not require the same vaccinations.[36] In all three provinces,

---

[34] See National Conference of State Legislators, *States with Religious and Philosophical Exemptions from School Immunization Requirements*(undated),

http://www.ncsl.org/research/health/school-immunization-exemption-state-laws.aspx.

[35] College of Physicians of Philadelphia, *A History of Vaccinations* (2014), http://www.historyofvaccines.org/content/articles/vaccination-exemptions.

[36] Alberta does not require vaccinations for students. However, the Public Health Act allows a medical officer of health to require a school to provide contact information about students in order for the health officer to

parents can object on medical or religious grounds and reasons of conscience. Compulsory vaccinations are not consistent with the Charter.[37]

While methods vary from jurisdiction to jurisdiction, schools with mandatory requirements generally enforce vaccine laws by denying admission to students without proof of vaccination or exemption. The process brings information into schools that school authorities do not collect otherwise. This is an example of a government program that effectively delegates an information collection function to a third organization.

It may appear that the privacy stakes here are low, and they may be so for students that receive vaccinations in ordinary course and provide the required evidence. Privacy issues may be greater for students who seek exemption. The reasons for exemption, whether religious, personal or medical, may reveal information about a student and their family that they would not otherwise share with the school in the ordinary course of operations. Information that might not have been maintained in any records held by a third party or that may have been subject to protection under a health record privacy regime will now appear in a school record subject to a different privacy regime. To illustrate the point, at least in part, a recent change in the American federal health privacy rule allows health care providers to disclose information about a student's vaccination to a school under procedures that are simpler than those otherwise applicable to disclosures.[38] The change supports school vaccination requirements. Other sharing of health information about students with schools remains subject to standard rules.

G. Highway Travel

Driving an automobile down a highway can result in the collection and maintenance of personal information by different entities using a variety of technologies. The privacy issues involve a complex interplay of the roles and obligations undertaken by government and assigned to government contractors and other players. The discussion here points out some of the privacy issues related to several current technologies, but there are more possibilities on the horizon. Surveillance of vehicles and drivers is likely to be a growth area for future personal information collection by government, the private sector and joint ventures, including surveillance and sharing by the vehicle itself. The examples discussed here are not comprehensive of all driver surveillance activities in use.

---

contact the parent or guardian about available health programs, including immunization. Public Health Act, Chapter P 37, § 18.1(2). http://www.qp.alberta.ca/1266.cfm?page=P37.cfm&leg_type=Acts&isbncln=9780779774685.

[37] Public Health Agency of Canada, Canadian *National Report on Immunization* (1996), http://www.collectionscanada.gc.ca/webarchives/20071212103611/http://www.phac-aspc.gc.ca/publicat/ccdr-rmtc/97vol23/23s4/23s4b_e.html. See also Vaccination Risk Awareness Network, http://vran.org/exemptions/legal-exemption-forms/.

[38] 45 C.F.R. § 164.512(b)(1)(vi) (2014), http://www.ecfr.gov/cgi-bin/text-idx?SID=0ddf45c05efb2e8daf54bc17ab06bdbe&node=45:1.0.1.3.78.5.27.8&rgn=div8.

Red light cameras enforce traffic laws by capturing an image of a vehicle that entered an intersection against a red traffic light. Cameras obtain license plate numbers and motor vehicle records identify vehicle owners. Government contractors sometimes operate red light cameras. For example, the City of Edmonton has a contract with American Traffic Solutions for photo enforcement.[39] The assignment of tasks under the contract and the exchange of information that supports those tasks affect privacy interests. A contractor and the government agency that hired the contractor could be subject to varying privacy obligations, but much would depend on the terms of the contract and, perhaps, the location of the contractor (e.g., in another Canadian jurisdiction or in another country).

While red light cameras generally only take pictures of violators, automatic license plate reader (ALPR) technology has great potential to affect privacy when used in other ways.[40] Whether used by government, contractors for the government or private actors, ALPRs create information on a vehicle's locations. Given enough cameras, ALPRs can track the location of a vehicle over time, resulting in a detailed profile of a driver's habits. The privacy sensitivity is high.[41] Choices about who operates ALPRs, what happens to the resulting information, who can use the information and how long the data may be kept affect privacy significantly so it is important to determine how privacy laws apply.

Highway electronic toll collection systems use radio-frequency identification (RFID) transponders on vehicles to communicate with reader equipment in toll collection lanes by reflecting back a unique radio signature. This is another technology that effectively records the location of a vehicle on the highway, with other personal data collected directly from motorists when they enroll in the program. Electronic toll collection raises some of the same issues as other highway vehicle location recording devices. Complexities arise when private companies rather than governments operate some roads or lease the roads from public agencies.[42] Privacy laws and contractual provisions

---

[39] American Traffic Solutions, Press Release, *The City of Edmonton, Alberta to be Canada's Largest Photo Enforcement Program; Selects American Traffic Solutions for 10-Year Contract to Provide Upgraded Digital Red-Light and Mobile Speed Camera* (4/3/09), http://www.atsol.com/the-city-of-edmonton-alberta-to-be-canadas-largest-photo-enforcement-program-selects-american-traffic-solutions-for-10-year-contract-to-provide-upgraded-digital-red-light-and-mobile-speed-cameras/.

[40] See, e.g., International Association of Chiefs of Police, *Privacy impact assessment report for the utilization of license plate reader* (2009), http://www.aamva.org/WorkArea/linkit.aspx?LinkIdentifier=id&ItemID=3450&libID=3436.

[41] Information and Privacy Commissioner (Ontario), *SURVEILLANCE, THEN AND NOW: Securing Privacy in Public Spaces* 26 (2013) ("[T]he use of enhanced ALPR systems to maintain a detailed accounting of every licensed vehicle that passes along a stretch of road, clears a check-point or enters into a park, town or city, 24 hours a day, seven days a week, would obviously have grave implications for privacy."), http://www.ipc.on.ca/images/Resources/pbd-surveillance.pdf.

[42] This is the case, for example, 407 Express Toll Route (ETR) in Ontario, http://www.407etr.com/index.html. See also Information and Privacy Commissioner (Ontario), *407 Express Toll Route: How You Can Travel the 407 Anonymously* (1998), http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=335.

determine the rules governing the collection, use, disclosure and other processing of the personal information.

Another issue common to these highway travel collection issues – and perhaps to many other personal information decisions – is outsourcing. Outsourcing is a practice in which a government or another entity hires a supplier under contract to manage activities on behalf of the government or entity. Many governments and others outsource personal information intensive activities for a variety of reasons, including lack of internal resources, efficiency and cost savings. Outsourcing can be mostly unremarkable, although for present purposes it raises important issues about which privacy law applies to data created by the outsourcing. The new element for present purposes – and one that has drawn considerable attention in Canada – is the outsourcing of personal information intensive activities to other countries.

As the discussion above shows, deciding who does the information collection necessarily raises questions about what privacy regime applies. When information processing occurs in another country, the determination of which privacy laws apply can be more complex and more consequential. Because U.S. companies commonly provide services for Canadian entities, the privacy situation in the U.S. is important. While the U.S. has some sectoral privacy legislation, many personal information processing activities by private sector entities are not subject to any federal or state privacy laws. The situation is different in a European Union (EU) country, where national privacy laws apply to most data controllers in the country. Even there, however, there may be differences between national laws in EU member states and laws in Alberta.

It is sufficient to highlight the issue here. A review of U.S. or other foreign privacy law is beyond the scope of this report. The OIPC and the Treasury Board of Canada Secretariat both issued reports on outsourcing in 2006 that remain relevant.[43] OIPC offered the view that "the most effective control and governance of outsourcing will require a mix of statutory provisions, enhanced diligence in the selection and monitoring of contractors, rigorous application of model contract formulations, and transparent testing and audit programs." This conclusion is fully compatible with the discussion and strategy in this report.[44]

H. Communications Data Retention

In 2006, the EU established a Data Retention Directive[45] (Directive) mandating each member state to enact a law requiring providers of electronic communications services and networks to keep traffic

[43] Office of the Information and Privacy Commissioner (Alberta), *Public-sector Outsourcing and Risks to Privacy* (2006), http://www.oipc.ab.ca/Content_Files/Files/Publications/Outsource_Feb_2006_corr.pdf; Treasury Board of Canada Secretariat, *Privacy Matters: The Federal Strategy to Address Concerns about the USA PATRIOT Act and Transborder Data Flows* (2006), http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_128/pm-prp/pm-prp01-eng.asp.

[44] OIPC at 30-31.

[45] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006, 2006 O.J. (L 105) 54-56, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

data related to phone calls and emails for a period of six months to two years. The Directive followed terrorist incidents in Madrid, London and elsewhere. The traffic data must include information necessary to identify the originator and the recipient of phone calls (including Internet telephony) and emails, and information on the time, date and duration of the phone calls and emails. The Directive allows disclosure of retained data only to the competent national authorities in specific cases and in accordance with national law. The Directive was highly controversial from the beginning and remains so today.[46]

Other jurisdictions have considered similar requirements. In 2012, the Canadian government proposed Bill C-30, the *Protecting Children from Internet Predators Act* [47], but variations on this bill date back much earlier. The bill sought to ensure that telecommunications service providers have the capability to enable national security and law enforcement agencies to exercise their authority to intercept communications and to require telecommunications service providers to provide subscriber and other information. Bill C-30 died as had its predecessors, but may have re-emerged in 2013 in the cyberbullying legislation, Bill C-13[48].

The U.S. has from time to time considered data retention proposals, but no legislation resulted. Recent disclosures about data collection activities of the National Security Agency may have changed the nature and focus of the debate about the retention of telecommunications metadata in the U.S. and elsewhere around the world. Some of the details of the EU Directive are relevant to a discussion of its privacy effects. The duties of communications providers include requirements that personal data retained must be subject to technical and organizational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorized or unlawful storage, processing, access or disclosure. The data must be subject to controls so that access is restricted to specially authorized personnel of the telecommunications provider. The effect is to prevent use of the data for commercial purposes. Retained data must be destroyed at the end of the period of retention. Police access is limited to specific cases, which prevents blanket requests for calling information and effectively requires some degree of particularized suspicion for access to the records. The Directive also called for the maintenance of statistics on use of retained records and for an evaluation of the Directive after a few years.[49]

---

[46] On April 8, 2014, the Court of Justice of the European Union ruled that the Data Retention Directive is invalid. The Court found, among other things, that by adopting the Data Retention Directive, the EU legislature exceeded the limits imposed by compliance with the principle of proportionality. http://curia.europa.eu/jcms/jcms/P_125951/.

[47] http://www.parl.gc.ca/HousePublications/Publication.aspx?Docid=5380965&File=32#1. Earlier versions of telecommunications interception and data retention legislation exist.

[48] An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act was tabled November 20, 2013 and is now in second reading http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=6311444.

[49] The Article 29 Working Party issued a report as part of this effort. *Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data*

IV. Advice for Assessing Information Collection Decisions

A. What Aspects Matter to Privacy?

The assignment of an information collection requirement to a non-governmental organization may be more or less consequential from a privacy perspective depending on the circumstances. The purpose of this section is to specify circumstances and elements to consider when evaluating an information collection decision. Below are some privacy-measurement standards that will help to categorize decisions that are potentially more consequential for privacy and decisions that are less consequential.

Although the standards are stated as either/or propositions, in reality, each is more likely to be applied along a sliding scale that is more nuanced than the standards suggest. Nevertheless, we doubt that the subject will allow for the establishment of a formal scale or assigning weights to the various factors. The element identified here may be most useful as a checklist or starting point for discussion and evaluation.

1. Personal information **would or would not be collected** in the absence of a requirement to maintain or report information. An organization may be required to maintain information that it would maintain anyway, even in the absence of the requirement. A physician maintains a health record about a patient's communicable disease whether or not the disease is reportable to public health authorities. On the other hand, a scrap metal dealer normally might not keep any information about a customer selling metal but for a legal requirement. Even those businesses that collect information about customers – banks, for example – may not keep as much information or keep it as long as required by KYC laws.

2. The organization collecting personal information **is or is not experienced in privacy protection**, such as with maintaining personal data, providing accountability measures and training staff. While all organizations subject to PIPA may face similar privacy obligations, those already familiar with privacy rules and that have been complying with the rules are likely to do a better job than an organization that has no familiarity. A bank is likely to do a better job on privacy when faced with a personal information collection obligation than a business that did not previously collect any personal information on its customers.

3. The organization collecting personal data **does or does not have the ability to use for secondary purposes** (e.g., marketing/profiling) the data collected. Other secondary uses may also result, including research and other activities associated with so-called "big

---

Retention Directive 2006/24/EC amending the e-Privacy Directive (WP172), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf.

data". Not all secondary uses may be harmful, and some have the potential to be beneficial. An understanding of the possibilities is essential to any privacy evaluation. A mandate to collect personal information can result in a new pool of consumer data that can be used for consumer marketing, profiling or in other ways that many might find unwelcome. For example, a liquor licensee required to verify the age of patrons and to maintain the information for later review ends up with a customer list that may include name, address and other information found on acceptable forms of identification. Maintenance of driver's license pictures may result in attractive individuals receiving unwanted attention. These consequences are more troublesome from a privacy perspective. However, if the licensee can only verify age but cannot maintain any information otherwise, no data becomes available for secondary use and the privacy concern disappears.

4. The organization collecting personal data **has or does not have existing capabilities/staff to provide necessary security**. Privacy law typically requires reasonable security measures. It is fair to assume that existing security obligations for financial institutions will be more extensive than the security obligations at a neighbourhood hardware store.

5. The collection of personal information **does or does not create new pools of data that increase the risk of identity theft** or that in other ways could adversely affect data subjects. The threat and incidence of security breaches appear to be increasing. The costs and consequences of breaches for both organizations and individuals also appear to be increasing. Even experienced merchants have become the target for identity thieves. A new collection of personal information by an organization creates new targets for criminals, especially if the information is maintained on and accessible through the Internet. Dangers may be greater where organizations inexperienced in security acquire new collections of consumer data.

6. The organization collecting personal information is or is not otherwise experienced in meeting data subject demands for **access or correction**. An individual's right to see and seek correction of personal information is a feature of nearly every privacy law. A merchant that only occasionally deals with consumers may find a KYC obligation challenging. For example, the sale of agricultural chemicals calls for the collection of identification information that may include consumers at times.[50] Sellers of chemicals are not likely to be familiar with or adept at meeting privacy obligations when they arise, and staff training will likely be an issue for them.

7. Government (or others) can **access the data with or without judicial process** or other formal procedures. In some cases, the purpose of collecting personal data is expressly for access and use by law enforcement. The terms under which law enforcement can obtain

[50] Explosives Regulations, 2013 (SOR/2013-211) §§ 473, 475, http://laws-lois.justice.gc.ca/eng/regulations/SOR-2013-211/page-138.html#docCont.

data is always an issue because the procedural protections that limit access to records protect the privacy interests of data subjects. Laws strike a balance between the competing interests. However, regardless of the applicable procedures, creation of new information resources often makes data more available to anyone in government who has the power to compel production of the data under existing authority. In addition, data pools may become available to private litigants who want the data and can meet the required standard. The data might be demanded in a lawsuit involving the organization maintaining the data or in a lawsuit involving the subject of the data. For example, in divorce or child custody cases, information might be useful to shed light on the parties to the litigation. When third parties hold personal data, individuals may have a harder time protecting their privacy interests.

8. The **data subject does or does not receive effective notice.** Notice is another feature common to privacy laws. Two types of notice are relevant here. The first type is notice about the personal data collection. Providing this type notice to consumers can be difficult and the rules can vary. Providing effective notice to consumers can be a particular challenge. Contrast consumer notification about telecommunications data retention rules and airline passenger screening rules. Passengers must provide some personal information when buying an airplane ticket, thus obtaining some notice about the data collection and its purpose. Those using the Internet or telephone system have no equivalent transaction or opportunity for notice, except for a formal written notice buried in a privacy policy. The second type of notice arises when an organization holding personal information discloses the data to the government or to any third party. The question is whether the data subject is entitled to notice before the disclosure so that there is an opportunity to object in a timely fashion.[51]

9. The **organization has or does not have a relationship with the data subject** so that data collection is not an unusual or unexpected event. A merchant with a video camera in a store collects personal information about all who enter the store. There may or may not be effective notice to shoppers of the surveillance, but it is likely the case that some shoppers will not be customers or may be cash customers whose identities are not known to the merchant. In contrast, a bank knows its customers and the customers know the bank. Both the bank and the customer will have an easier time of managing privacy matters as a result.

10. The personal data collected by a private sector entity **is or is not immediately reported to government**. Those merchants subject to FINTRAC requirements have a bundle of

[51] Several US laws provide limited rights to notice of impending disclosures. The Right to Financial Privacy Act provides a very limited right to notice when some federal government agencies seek an individual's bank records. 12 U.S.C. § 3401 *et seq*., http://www.law.cornell.edu/uscode/text/12/3401. The health privacy regulation under the Health Insurance Portability and Accountability Act provides an individual with a somewhat greater right to notice when someone seeks the individual's health record in a judicial or administrative proceeding. 45 C.F.R. § 512(e), http://www.ecfr.gov/cgi-bin/text-idx?SID=5d1baa3e161e00feb568a11d2ac5c007&node=45:1.0.1.3.78.5.27.8&rgn=div8.

obligations. They must promptly report suspicious transactions to a government authority, but they are only required to maintain identity information collected for KYC purposes for possible future use by a government authority. While the mere collection of personal information raises some privacy concern, the immediate reporting of personal information to any government or to any third party raises different concerns.

11. The personal information collected **is or is not routinely discarded in a defined period** unless selected for reporting or review under a clear standard. Privacy interests are typically better protected when personal information is erased when retention is no longer justified. A video surveillance camera that keeps footage for 24 hours and overwrites the footage if no reason exists to keep it is less troubling from a privacy perspective than a FINTRAC requirement to keep all customer data for five years after a customer closes an account.

12. **There is or is not a risk that the personal information collected will become outdated** in a fashion that may materially affect the data subject. Data quality standards generally provide that data should be relevant and up-to-date for the purposes for which the data will be used. Data kept beyond any need is more likely to grow inaccurate or irrelevant as time passes. A decision of the Supreme Court of Canada involving a woman who pleaded guilty to a shoplifting charge and received a pardon after five years illustrates the point. She applied for a job with the Montreal Police and the police rejected her because of the conviction. The result was a 13-year legal battle over whether and how information about a conviction that had been pardoned could be used in an employment context.[52] The result, which was something of a mixed decision, is not relevant here, but the basic facts are instructive.

13. The **data subject has or has not given consent** to the collection of personal data. A good example where consent diminishes privacy concerns is an electronic highway toll collection device. A motorist who acquires the device knows many of the consequences of using it. When an ALPR captures a license plate number, the motorist typically is unaware of the collection of personal information. Consent may not cure all privacy ills, but it certainly is a factor in assessing privacy consequences.

14. **Privacy oversight will be enhanced or degraded** by placing the collection of personal data outside of government. Legislation establishes the formal powers of privacy regulators and that is the starting point for answering the question here. Statutory authority is not necessarily the ending point, however. Many other factors go into determining the allocation of privacy resources and the degree of practical cooperation that privacy regulators can obtain from various organizations subject to its oversight. Further, other bodies, including the legislature, privacy advocacy organizations and the media, may contribute to privacy oversight. It is also worth observing that government

---

[52] *Montréal (City) v. Quebec (Commission des droits de la personne et des droits de la jeunesse)*, 2008 SCC 48, [2008] 2 SCR 698, http://www.canlii.org/en/ca/scc/doc/2008/2008scc48/2008scc48.html.

records for activities that collect personal information may be subject to public disclosure through a variety of mechanisms, including access to information policies. Records maintained by private entities are not available through access to information requests.

15. **There is or is not a benefit to the individual** in the new data collection. Women walking to their cars alone in a parking lot at night see a clear benefit in having video cameras, particularly if a live human monitors the cameras, whereas passersby filmed on a street corner may see no benefit, only intrusion.

B. Ideas for Evaluation of Personal Information Collection Choices

Part A of this section offered a list of elements that help to identify and assess the privacy consequences of asking a private sector entity to collect personal information rather than have a government agency collect the information. This part focuses more on processes and procedures for conducting an evaluation of a decision. The goal here is to suggest methods, approaches, and courses of action for privacy regulators or others to consider when evaluating choices about personal information collections. It is a checklist of ideas, although each idea may not be appropriate in every case. The assumption here is that the function under evaluation is a new one, but the ideas offered may also have value if an existing function comes under review.

1. **Identify the decision**. This may be half the battle. It is likely that many decisions to ask a private sector entity to collect personal information will be a small part of larger proposals seeking to accomplish a public purpose of which privacy issues may be a small or even inconsequential part. Those who sponsor a bill, draft a regulation or administer a program may not be aware of the privacy implications or realize that the proposal affects the application of privacy law. In some cases, however, changing the privacy rules may actually be one of the goals. Sometimes, the choice about who is to collect the information appears only after a proposal moves partway through the decision process. These can be the most difficult to find. Regardless, the first challenge is to find relevant proposals and to call for public attention, discussion and debate.

2. **Identify the reason**. The choice to assign a personal information collection activity to a non-governmental entity may be purposeful, accidental or unnecessary. In some of these cases, the sponsor may be willing to change or withdraw a proposal once informed of the consequences in order to avoid what they may perceive as an unnecessary fight over privacy. If the choice is purposeful, finding the stated reasons for it is a starting point for further analysis and discussion. It allows for an informed discussion of the relationship between the public policy objective and the entity collecting the personal information.

3. **Seek consultation with affected stakeholders**. Decisions about personal information collection affect those who are data subjects as well as those organizations tasked with the collection. All stakeholders should participate in the discussion and decision-making. In some cases, stakeholders themselves will identify the issue and bring it to the attention of the privacy regulator and the public. Maintaining and expanding communications with privacy stakeholders is obviously a worthwhile activity for privacy regulators in this and other respects.

4. **Provide privacy education to those who need it**. As proposals move along policy, legislative or administrative tracks, decision makers need to be informed when privacy concerns exist. In addition, those who are affected by an information collection – including those who may be tasked with collection responsibilities and those who may be data subjects – need to understand the privacy issues involved.

5. **Discuss the cost, risks and benefits**. This report acknowledged in the introduction that not all decisions to ask non-governmental entities to undertake personal information collection are unjustified. Certainly some may be justifiable on public policy grounds. Evaluating the costs, benefits and privacy risks will be part of nearly every debate, and these concerns belong on the table as early as possible.

6. **Evaluate the privacy consequences**. A standard tool for evaluating privacy is the privacy impact assessment (PIA). One major goal of a PIA in this context is to focus on the different consequences of private vs. public collection of personal information and on any related privacy consequences. Any evaluation must closely examine the collection of data, the use and disclosure of data, and other elements of data processing in order to describe fairly and completely how the different potentially applicable privacy laws would apply. In some cases, the difference might be inconsequential and, in other cases, the difference may be major. Detailed advice on the timing, conduct and content of PIAs is not within the scope of this report.

7. **Pay special attention to outsourcing**. Outsourcing has been controversial across Canada already, and concerns about foreign privacy laws, including, but not necessarily limited to, in the U.S., have expanded with recent revelations about national security activities and related data collection operations. Information transfers to another jurisdiction may be vulnerable both in transit and at the destination. The adequacy of current outsourcing control in any context is worth reviewing.

8. **Determine who will be responsible for breach notification consequences**. Breach notification laws are relatively recent. Experience shows that breaches can be costly both to a reputation and financially. For delegated or joint activities involving the collection and transfer of personal information, it may be essential to identify in advance who will take responsibility for fulfilling breach notification obligations, whether the obligations are mandated or merely appropriate. The more complex the relationship between parties to any information collection or transfer, the greater the importance of determining responsibility in advance. Any delays resulting from legal or contractual uncertainties could seriously undermine the interests and needs of the affected data subjects. It may be worth observing that breaches where government agencies are or are perceived to be responsible in whole or in part may present political risks to government officials.

9. **Seek agreement for the completion of a privacy evaluation before any decision is final**. A PIA or other evaluative tool will have no effect if decision makers proceed with a proposal before an evaluation of the privacy consequence is available. It is appropriate to ask to postpone decisions for a reasonable period to allow for a review of privacy and to ask for a public response to the evaluation as well.

10. **Offer alternatives**. As some of the examples above demonstrated, relationships between government agencies and private sector entities that involve the collection and sharing of personal information can take many forms. Personal information processing may be a function shared between multiple parties, rather than being completed by government or other organizations. Creative approaches achieve better privacy results without undermining program objectives.

11. **Propose a sunset for the information collection**. Personal information collection choices, even those made relying on appropriate decision tools, may lose their justification over time. Changes in technology, among other things, may undermine the premise or privacy consequences of a decision. Reasonable assumptions about the costs or benefits may turn out not to be correct. Unforeseen developments in other spheres may make a difference to the privacy consequences. One familiar way to force reassessment of a decision is to include in the initial authorization that the requirement end at a given time with the possibility of reauthorization. Another way is to mandate at the end of a fixed period a review of the requirement as a trigger for the opportunity for making changes. Some legislatures resist the imposition of mandatory parliamentary review, but there are other alternatives, such as mandating privacy regulators to conduct an audit and assessment, possibly in concert with other relevant legislative officers or oversight bodies.

V. Concluding Thoughts

We offer a few additional thoughts for the problem of personal information collection decisions.

When imposing an information collection requirement on a private entity, is the government doing indirectly what it cannot do directly? In the introduction, we briefly mentioned the work of Jon Michaels about privatization of government activities and his concept of "workarounds" where the government accomplishes through privatization what it cannot do on its own. This may be a real concern in some information collection decisions.

When imposing an information collection requirement on a private entity, is the government doing indirectly what it cannot do directly?

The increasing sophistication of surveillance technology extends the range of real world privacy-affecting possibilities in ways that only science fiction writers could envision a few years ago. The decreasing price of that technology is also a major factor. Privacy invasive activities limited in the past by cost, such as the tracking of individuals in public, may become commonplace in the near future. A government that hesitates to propose universal surveillance for fear of a public reaction might move toward that goal with a cooperative program that supports merchants willing to place cameras in and around their stores.

Could assignment of some personal information collection activities to the private sector be more privacy protective than having a government agency do the collection? Personal information in the hands of a government agency may find its way to other agencies with greater ease than information

held by a third party. External barriers, such as seeking court approval for access to personal information, may better protect privacy than internal barriers invisible to the public. The risks of secondary use by the government should be weighed against the risks of secondary use by the private sector. The point is that there should be no fixed bias on one side or the other.

The possibility that necessary information collection can be accomplished more efficiently by one actor or the other will be a factor in evaluating many decisions. It will not be the only factor, however. Many citizens may be unhappier if the police collect some types of personal information than if others do. In other words, efficiency matters, but it is not always determinative.

Is it possible that the population as a whole has complexity fatigue? How much energy does the average individual or family have to devote to privacy management? By this, we mean understanding the flow of personal information and the exercise of privacy rights and options. The importance of enforceable citizens' rights in these deputizing situations remains. However, the likelihood of anyone actually acting on those rights grows fainter because of the complexity of life in an information society. What will best provide for the enforcement of privacy rights?

In the end, the protection of privacy requires a careful review of the consequences of personal information collection choices. In an increasingly technological and complex environment, it is important to follow the trail of data, identify the actors and their legal obligations and ask the right questions in order to identify all the privacy risks and consequences. Only then can policymakers decide an important public policy issue in a reasoned and appropriate way.

Appendix: Alberta Privacy Law Comparison Chart

Currently, five laws address privacy issues in Alberta. The *Freedom of Information and Protection of Privacy Act*[53] (FOIP), the *Personal Information Protection Act*[54] (PIPA), the *Health Information Act*[55] (HIA), the *Personal Information Protection and Electronic Documents Act* (PIPEDA)[56] and the *Access to Motor Vehicle Registration Information Regulation*[57] (AMVIR). Upon review, we decided to omit the HIA, PIPEDA and AMVIR in the interest of space. Accordingly, the following chart illustrates some of the major differences between the law for the public sector (FOIP Act) and private sector (PIPA) only. The chart is not complete and summarizes only provisions of particular interest. Consult the FOIP Act and PIPA for the exact wording and interpretation of each Act.

	FOIP	PIPA
Applicability	Public bodies, which include all provincial departments, agencies, listed boards and commissions, school boards, charter schools, post-secondary institutions, health care bodies and local government bodies (e.g., municipalities, libraries, police services, irrigation and drainage, Métis settlements, and housing management and their agents).	All Alberta private sector organizations. An organization includes a corporation, a trade union, a partnership, or an individual acting in a commercial capacity an association that is not incorporated (e.g., a school council, an ad hoc group). It does not include a public body already covered by the FOIP Act, a federally-regulated organization that is already covered by PIPEDA, societies, agricultural societies and organizations registered under Part 9 of the *Companies Act* except when collecting, using or disclosing information in the course of a commercial activity.
Scope	All records of information in any form in the custody or under the control of a public body, including court administration records but not information in a court file or record of a	PIPA does not apply to specific types of personal information or when the information is collected, used or disclosed for certain purposes, including:

[53] http://canlii.ca/t/821t. Regulations at http://canlii.ca/t/831s.

[54] http://canlii.ca/t/81qp. Regulations at http://canlii.ca/t/83gh.

[55] http://canlii.ca/t/81pf.

[56] http://canlii.ca/t/7vwj

[57] http://canlii.ca/t/82xl.

	FOIP	PIPA
	judge. Specified records and types of information are exempted from the Act. The FOIP Act takes precedence if there is inconsistency or conflict with another Act, unless paramountcy has been created.	• Journalistic, artistic, literary, or personal or domestic purposes • Business contact information for the purpose of contacting an individual in relation to his or her business responsibilities • Health information covered by the *Health Information Act* • Personal information in court files.
Personal Information	All recorded information about an identifiable individual, including name, address, phone, race, national or ethnic origin, colour, religious or political beliefs or associations, age, sex, marital status, family status, identifying number, symbol or other particular assigned to the individual, fingerprints, blood type, biometrics, inheritable characteristics, information about health, health care history, educational, financial, employment or criminal history, opinions about the individual, and individual's personal views or opinions except if about someone else	Information about an identifiable individual.
Employee Information	No special provisions.	Employees are individuals and include apprentices, volunteers, participants, work experience or co-op students and contractors. An employer may collect, use and disclose personal employee information without consent if the individual is an employee and if reasonable for the purpose and limited to the work/volunteer relationship. Employees must receive notice about the purpose for collecting.
Privacy Impact Assessments	Privacy impact assessments (PIAs) are not required though the Office of the Information and Privacy Commissioner of Alberta (OIPC) recommends them. The Commissioner can review and comment on the privacy implications of a public body's program but does not	PIAs are not required though the OIPC recommends them. The Commissioner can review and comment on the privacy implications of an organization's program but does not "approve" the PIA, just "accepts" it.

	FOIP	PIPA
	"approve" the PIA, just "accepts" it.	
Collection	Public body may collect personal information only for purposes expressly authorized under an enactment, regulation or directive, for law enforcement purposes, or, when necessary, for and directly related to operating programs or activities. Information must be collected directly from the individual unless indirect collection is permitted by the Act or is authorized by the individual. When information is collected directly, the individual must be notified of the authority and purpose of the collection, unless notification would lead to inaccurate information.	Organizations may collect personal information only for reasonable purposes and only the amount and type reasonably needed to carry out the purposes for collecting it. Information must be collected with consent, unless expressly allowed without consent by the Act or is authorized by the individual. When information is collected directly, the individual must be notified before or at the time of collection of the purposes of the collection and the contact information of a person who is able to answer questions about the collection on behalf of the organization.
Use and Disclosure	Use and disclosure allowed only for purposes for which collected, for consistent purpose, for a law enforcement purpose, for another purpose with express consent or for purpose set out in the Act.	Use and disclose information allowed only for reasonable purposes and only for amount and type of information needed to carry out those purposes. Use and disclosure allowed without consent in specific circumstances usually when authorized by law or for a law enforcement purpose, but also when the use is clearly in the interests of the individual and consent cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent.
Outsourcing	No provision specifically addresses outsourcing, but a contractor may be considered an employee of a public body in some cases.	Notification to individuals at time of collection or transfer that specifies use of service provider outside Canada, where to get info on policies/practices about the organization's use of service providers, and who to contact with questions.
Safeguards	Must make reasonable security arrangements for information under custody or control.	Must make reasonable security arrangements for information under custody or control. Duties of accuracy and breach notification.

	FOIP	PIPA
Access	Any person may make a written request for access with sufficient detail to identify record and pay fee. Public bodies must make every reasonable effort to assist and respond.	Individuals may ask for access to their personal information, to know how it is or has been used, and to whom and under what situations it is or has been disclosed. Organizations may charge a reasonable fee for access, other than for employee information. Organizations must make every reasonable effort to assist and respond.
Refuse Access if Invasion of Privacy	Section 17(2) sets out situations where disclosure would not be an invasion, and Section 17(4) sets out situations presumed to be an invasion of privacy, which then requires consideration of relevant factors.	In some circumstances, organizations can or must refuse access, such as when disclosure would harm someone, an investigation, or legal proceeding or when access would disclose the personal information of someone else or of confidential business information.
Correction	Yes. Where correction refused, head of public body to annotate record. Notice of correction/annotation to other public bodies and third parties who have had access within one-year when corrected unless information not material and individual agrees it is not necessary.	Yes. Notification of other organizations that received the information before correction. Where correction requested but refused, notation as to that fact to be added to file.
Penalty	Fine of not more than $10,000 for an individual, and fine of not more than $500,000 for a person other than an individual.	Fine of not more than $10,000 for an individual, and fine of not more than $100,000 for a person other than an individual.
Judicial Review	Yes.	Yes.

Authors' Biographies

Robert Gellman

Mr. Gellman worked for 17 years on the staff of the Subcommittee on Government Information of the U.S. House Committee on Government Operations. During that time, he was responsible for all information policy activities including privacy, the *Privacy Act of 1974,* health privacy, the collection and dissemination of electronic data, the *Freedom of Information Act* and other matters. From 1996 to 2000, Bob was a member of the National Committee on Vital and Health Statistics, an advisory committee of the U.S. Health and Human Services Department. He chaired its Subcommittee on Privacy and Confidentiality from 1996 to 1998.

Since 1995, Mr. Gellman has also worked as a privacy and information policy consultant with clients that included large and small companies, trade associations, government agencies (U.S. and others), NGOs and privacy advocacy organizations. He has been a member of the Editorial Board of Government Information Quarterly since 1996, and in 2012, he was named Senior Fellow at the Center on Law and Information Policy, at the Fordham University School of Law.

He holds a BA from the University of Pennsylvania and a JD from the Yale Law School.

Stephanie Perrin

Since 1984, Ms. Perrin has devoted most of her career to information and privacy issues, having started as one of the first federal Access to Information and Privacy Coordinators at the then-Department of Communications. For ten years, she worked as a policy analyst for the Department of Communications and Industry Canada, developing the Canadian Standard for the Protection of Personal Information and incorporating it in law as the *Personal Information Protection and Electronic Documents Act* (PIPEDA) for the private sector. She also represented Canada at the Organisation for Economic Co-operation and Development on the committee dealing with privacy and security issues, and worked in the private sector as Chief Privacy Officer for Zero Knowledge Systems. She has held the positions of Director of Policy and Research at the Office of the Privacy Commissioner and Director of Risk Management Policy for Service Canada. Most recently, she has re-launched Digital Discretion Inc. which she initially started in 2003.

Ms. Perrin graduated from Carleton University with an MA, and is now a doctoral candidate at the Faculty of Information at the University of Toronto, where she is researching issues influencing online privacy protection. .

Dr. Jennifer Barrigar

Dr. Barrigar is a legal scholar and writer on privacy and reputation. For several years she served as Legal Counsel at the Office of the Privacy Commissioner of Canada where she participated in the initial application and interpretation of Canada's private sector law, as well as working with international standards for privacy and data protection. She has also taught law courses at the University of Ottawa and Carleton University.

Dr. Barrigar holds LL.D and LL.M. degrees from the University of Ottawa, working with the Centre for Law, Technology and Society. She also holds an LL.B. from Dalhousie University and a BA (Honours) from Carleton University.