Deloitte.

Report on the Collection and Use of Canadians' Personal Information by Wireless Service Providers and Third Party Entities

January 6, 2017
ISBN: BC92-92/2017E-PDF
978-0-660-07479-5

Contents

1. Executive Summary

1.1 Purpose and objectives

The Canadian Radio-television and Telecommunications Commission ("CRTC") is committed to ensuring the effectiveness of the Wireless Code and is undertaking a review of the Wireless Code in 2016 and 2017 in order measure the effectiveness of the Code's objectives, which includes ensuring wireless customers are equipped with a better understanding of their service and are able to make informed decisions about wireless services.

The overall objective of this report is to provide an overview of the collection and use of Canadians' Personal Information (PI) by Wireless Service Providers (WSP) and third party entities. The report aims to:

- Contribute to the CRTC's overall understanding of current and emerging privacy issues in the wireless market, in support of furthering the goals of the Telecommunications Act; and
- Assist the CRTC with its 2016-2017 review of the Wireless Code, a mandatory code imposed as a condition of service on WSPs pursuant to section 24 of the Telecommunications Act, by providing insights as to how the Wireless Code is meeting its objectives with respect to its privacy provisions.

1.2 Summary of findings

The research is this report is based on primary research conducted by interviewing the Privacy Officers of fifteen (15) Canadian WSPs, and on secondary research articles. The following section provides a summary of the main findings of this research.

The Collection and Use of Customer PI by WSPs Considers WSP Business Needs as well as Customer Privacy

While the Wireless Code has created consistency in the wireless industry for customers, all WSP Privacy Officers view Personal Information Protection of Electronic Documents Act (PIPEDA) as the central privacy regulation and standard by which privacy is governed in the wireless industry. WSPs collect PI in accordance with their obligations under PIPEDA and appropriately outline the purposes of this collection in their privacy policies. WSPs report that they use customer PI in order to support their operational activities.

WSPs Do Not Sell Customer PI to Third Parties

WSPs report that they do not sell customer PI to third parties under any circumstances. However, WSPs do share customer PI with various third parties in order to receive a service which supports their business operations (e.g. printing and mailing bills to customers).

WSPs Have Established Privacy Roles and Responsibilities

WSPs of all sizes have a privacy accountability model in place to embed the protection of customer privacy into their organization. This model is typically dependent on the size of the organization (i.e. major, flanker, or small), which is consistent with varying structures across other industries.

The Majority of WSPs Have a Formally Documented Privacy Breach Procedure

The majority of WSPs have a formal and documented privacy breach policy or procedure in place; the breadth and formality of the policy is generally proportional to the size of the WSP.

WSPs Use Contractual Restriction as their Main Tool for Restricting Third Party Collection and Use of Customer PI

The evidence suggests that the main tool WSPs use to restrict the collection and use of customer PI by third parties is via contractual obligation, as well as other methods which vary across WSPs (e.g. audit).

Using Customer PI for Secondary Purposes is a Rarity in the Wireless Industry Today

WSPs do not regularly use customer PI for new uses beyond what is originally contemplated, but if/when they do, they all require the appropriate level of consent. WSP Privacy Officers are mindful of customer preferences for various features and work to ensure that consent is properly obtained when contemplating new uses/disclosures of PI.

Most WSPs Contemplate Providing Consumers with Service Offerings that Incorporate Emerging Technologies

The results of the interviews with respect to emerging technologies highlight the rapid pace at which Canada's wireless market and consumer offerings are changing. At the time of the interviews, most Canadian WSPs were contemplating providing service offerings that use emerging technologies (e.g. Internet of Things, augmented reality) to individual wireless customers, but indicated that they had not contemplated the extent to which these technologies will be implemented or established implementation timelines, and as such, had not fully considered the privacy requirements for such technologies.

However, WSPs have already begun to venture into the realm of emerging technologies, although at varying degrees and sometimes in only ancillary ways. For example, several WSPs currently offer Internet of Things solutions, but the vast majority of these services target large business customers, not individuals. Some WSPs offer wearables, such as smart watches, as mobile device accessories. The major WSPs offer virtual reality headsets as mobile device accessories that customers can pair with a smartphone. Most WSPs sell smartphones that customers can use to download third-party augmented reality apps, like Pokémon Go. Although these are accessed using the WSP's network, WSPs do not have contractual agreements directly with third-party applications; rather, the customer consents to the application's privacy agreement.

Notice and Consent, Human Error, and the Internet of Things Identified as Greatest Privacy Challenges in the Wireless Market Today

WSPs identified the following issues as the greatest current challenges in protecting the privacy of customers' information in today's wireless market: notice and consent, human error, the Internet of Things, legal complexities, transparency, external threats, malicious intent, and big data. Privacy Officers face challenges to providing meaningful notice to customers and obtaining meaningful consent from customers as the result of the growing complexity of services, technologies, the wireless market and today's market more broadly. Privacy Officers also expressed concern regarding unintentional mistakes made by employees that could cause a privacy incident or breach. Privacy Officers also see the Internet of Things as a unique challenge: they cannot control how individuals share their PI across various applications and devices, but a risk to their customers' privacy may still exist.

Privacy Challenges in the Wireless Market Today are Not Unlike Privacy Challenges in Other Industries

The results of the interviews demonstrate that the greatest privacy challenges in today's wireless market are similar to those privacy challenges in other industry areas, including obtaining meaningful consent and providing meaningful notice to customers in an increasingly-complex environment, as well as protecting consumer privacy in an age of emerging technologies.

Wireless Customers May not Always Fully Understand WSP Disclosures of Personal Information

While participating-WSP privacy policies do provide lists of the disclosures of customer PI they may make, some of these may constitute disclosures beyond what a customer may typically consider as a disclosure of PI. For example, disclosures of PI for product development, marketing, research, and third-party agent services may not typically be contemplated by a wireless customer and terms such as "marketing" and "research" may be too broad for customers to fully understand their meaning and context.

Further Consumer Education about Privacy would Benefit Consumers

WSPs indicated that further education across Canada on privacy and information-sharing technologies (e.g. social media) would greatly benefit consumers in better understanding how to protect their information, with companies in turn responding to consumer demands.

WSPs Indicated Compliance with Most Wireless Code Privacy Rules

The results of the interviews indicate that most WSPs consider that they are generally complying with the most of the Wireless Code's privacy rules. For example, each participating WSP has a privacy policy publicly available on their website and indicated that they provide customers with 30 days' notice prior to changing their privacy policy.

However, it is of interest that the Wireless Code requires WSPs to provide a customer with a paper copy of the privacy policy when the customers signs their contract, unless the customer knowingly and expressly accepts an electronic copy. The Wireless Code policy also requires that privacy policies be provided in an accessible manner, which includes alternative formats for people with disabilities, upon request and at no charge[1]. Based on the interviews, only one major WSP and its flanker-brand WSP provide a hard copy of their privacy policy to the customer when they sign their service agreement, and most - but not all - WSPs provide their privacy policies in an alternative format for people with disabilities.

Strategic Implications

The results of the interviews provide evidence that WSP Privacy Officers view the privacy issues in their industry as being similar to those in other industries. To this end, it is important for the CRTC to work with the OPC to ensure that the wireless industry is regulated on a similar basis to other industries.

The results of the interviews also provide evidence that while the Wireless Code has helped ensure consumers better understand their privacy rights and wireless service options, all WSP Privacy Officers view PIPEDA as the central pillar by which privacy is governed in the wireless industry. As such, any changes to the Wireless Code with respect to privacy should be mindful of the strong privacy protections outlined in PIPEDA and should be made in consultation with the OPC.

The results of the interviews indicate that the WSPs consider that they are generally complying with Wireless Code's privacy rules; however, the CRTC may wish to explore this issue further during the Wireless Code policy review – in particular with respect to paper copies and accessible copies for people with disabilities.

[1] See paragraph 310 http://crtc.gc.ca/eng/archive/2013/2013-271.pdf

2. Introduction

2.1 Background

In 2013, the CRTC established the Wireless Code, a mandatory code of conduct for providers of retails mobile wireless voice and data services (i.e. WSPs). The Wireless Code was created to help consumers better understand their consumer rights and obligations found within customer contracts with WSPs. The Wireless Code's main objectives are to ensure that the wireless market operates in a consumer-friendly manner as well as to empower customers with the information they need to better understand their wireless service options. The CRTC is conducting a review of the Wireless Code in 2016 and 2017 as part of its Three-Year Plan 2016-2019 to "ensure its effectiveness in fulfilling its objectives". In addition to this three year review, the CRTC has also conducted annual public opinion surveys on customer mobile plans since launching of the Wireless Code.

The privacy-specific provisions of the Wireless Code require that WSPs carry out the following activities:

- Ensure wireless contracts and other related documents (e.g. privacy policy) are written in a way that is clear and easy for customers to read and understand;
- Give the customer a permanent copy of the contract and privacy policy at no charge immediately at the point of sale, or send a permanent copy of the privacy policy to the customer within 15 days, if agreed to over the phone or online;
- Provide the customer with a paper copy of the privacy policy, unless the customer expressly decides that an electronic copy is acceptable;
- Provide an easy to read explanation of the privacy policy within the contract; and
- Provide customers with at least 30 calendar days' notice before making changes to their privacy policy, clearly explaining the changes and when they will occur.

2.2 Scope

The scope of the report covers an in-depth analysis of the following topics:

- The type, sensitivity and amount of personal information collected by WSPs;

- How WSPs use customer data, including the disclosure, monetization or sale of data to third parties;
- Built-in privacy protections;
- How WSPs handle privacy breaches;
- How WSPs give customers control over how their personal information is handled;
- Restrictions WSPs place on the collection and use of personal information by third parties; and
- The greatest challenges to protecting the privacy of wireless customers in today's market.

The detailed findings analysis (See **Section 3**) incorporates the following primary and secondary research:

- The results of interviews conducted with nine (9) privacy officers representing fifteen (15) WSPs;
- Insights based on the secondary and publicly available research on data collection and privacy in the wireless industry;
- References to the publicly available privacy policies of the fifteen (15) participating WSPs; and
- The results of an interview conducted with a privacy specialist at the Office of the Privacy Commissioner of Canada (OPC).

2.3 Methodology

This report considers the results of nine (9) interviews conducted with Privacy Officers representing fifteen (15) WSPs. The participating WSPs fall into one of the following categories:

- **Major Canadian WSPs:** Major WSPs are the three (3) largest Canadian providers in today's wireless market in terms of both their customer base as well as the number of employees they have.
- **Flanker-brand WSPs:** Flanker-brand WSPs refer to a WSP that acts as an extension of an existing major WSP, but with different branding and service offerings. These WSPs are generally smaller in the number of wireless customers and employees they have relative to major WSPs.
- **Small WSPs**: These WSPs operate independent of major WSPs and are of a smaller size, with fewer employees and customers than major Canadian WSPs.

The names of the participating WSPs may be found **in Appendix A – Participating WSPs**. Please note that for confidentiality purposes, the identities of

the Privacy Officers have not been revealed and specific comments have not been attributed to the WSPs in this report.

The Privacy Officer interviews covered the following topics, at a minimum (see **Appendix B – Sample Interview Questionnaire**):

- the type, sensitivity, and amount of personal information collected and used by the WSP;
- whether the WSP shares or sells customer information it collects to third parties and how it ensures privacy in those cases;
- what types of restrictions the WSP impose on third parties to protect the privacy of their customers;
- how their particular WSP protects the privacy of their customers;
- how the WSP gives customers control over how their personal information is handled (including obtaining consent when personal information is used by the WSP for a purpose other than the original use);
- how the WSP notifies customers of changes to their privacy policies;
- how and when the WSP notifies customers of a privacy breach and how it mitigates the impacts of such breaches; and
- what, from the Privacy Officer's personal perspective, are the greatest challenges in protecting the privacy of wireless customers in today's market.

This report also considers the insights of a privacy expert at the OPC, who was interviewed with regards to issues that fall under the mandate of the OPC. The results of the interviews are reflected within **Section 3 – Detailed Findings and Analysis**. Insights based on the primary and publicly available research on data collection and privacy in the wireless industry may also be found in **Section 3 – Detailed Findings and Analysis**.

This report focuses on **mobile services** as defined within a WSP service contract or for which a customer subscribes to (i.e., mobile wireless voice, text, and/or data services). While smartphones are most often the device used by such subscribers, the report also considers emerging privacy issues relating to other devices requiring a contract with a WSP for voice and data services, such as tablets, smartwatches, and connected cars. These **emerging privacy issues** involve various technologies as are defined below:

- **Metadata:** Metadata is defined as data generated by technology that provides information about other data. In the context of communications, metadata provides details regarding the creation, transmission and distribution of a message (e.g. the location from which a phone call is made).[2]
- **Internet of Things (IoT):** IoT refers to the growing network of objects (e.g. watches, cars) that feature an IP address for internet connectivity, and the

[2] Office of the Privacy Commissioner of Canada, Metadata and Privacy: A Technical and Legal Overview, October 2014. https://www.priv.gc.ca/media/1786/md_201410_e.pdf

communication that occurs between these objects and other wireless devices and systems. For example, a WSP may sell connected car services to a manufacturer as well as a telematics device to consumers. It has been noted that IoT will offer numerous benefits to consumers, particularly in the field of healthcare where patients may be able to monitor their own vital signs without a hospital stay.[3]

- **Big data:** Big data refers to extremely large sets of data that may be computationally analyzed to reveal patterns, trends, and associations, especially relating to human behaviors and interactions.
- **Augmented reality:** Augmented reality is "a class or family of technologies that tend to have certain common and distinguishing features". These features include sense properties about the real world, process in real time, output of information to the user, contextual information, recognition and tracking of real-world objects and are either mobile or wearable.[4]
- **Cloud storage**: Cloud storage refers to the remote maintenance, management and back up of information made available to its users over a network, which is most often the Internet. The University of Toronto recently published a report which explains that the actual definition of the 'Cloud' has come to take on several meanings and misinterpretations. These false definitions may encourage the public to think of the Cloud in a non-physical world, independent of jurisdictions in which telecommunications equipment (e.g. servers) powering the Cloud run.[5]
- **Internet exchange point (IXP)**: An IXP refers to a physical infrastructure through which major network providers are able to connect their networks and exchange Internet traffic. For example, WSPs may use IXPs to exchange information about which of their customers are roaming and where, in order to properly invoice roaming charges.

---

[3] Federal Trade Commission Staff Report. Internet of Things: Privacy & Security in a Connected World. January 2015. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[4] Tech Policy Lab, University of Washington, Augmented Reality: A Technology and Policy Primer, September 2015. http://techpolicylab.org/wp-content/uploads/2015/10/Augmented_Reality_Primer.pdf

[5] University of Toronto. Seeing Through the Cloud: National Jurisdiction and Location of Data, Servers, and Networks Still Matter in a Digitally Interconnected World. 2015. http://ecommoutsourcing.ischool.utoronto.ca/wp-content/uploads/BohakerAustinClementPerrin_SeeingThroughTheCloud-PublicReport-15Sept2015.pdf.

3. Detailed findings and analysis

This section documents the findings from interviews with WSP Privacy Officers and a privacy specialist from the OPC, publicly available privacy documentation from WSPs, and publicly available publications on data collection and privacy in the wireless industry. This section will contribute the CRTC's understanding of the type, sensitivity, and amount of personal data being collected and used by WSPs, how they share or sell that information to third parties, and what steps Canadian WSPs have taken to protect customer privacy. Furthermore, this section will help inform the CRTC's overall understanding of privacy issues in the wireless service market in anticipation of its upcoming review of the Wireless Code.

3.1 The type, sensitivity and amount of personal information collected by WSPs

According to PIPEDA – the federal privacy legislation to which all WSPs are subject – "personal information" is defined as "information about an identifiable individual".[6] This includes information in any form, such as age, name, ID numbers, income, ethnic origin, or blood type; opinions, evaluations, comments, social status, or disciplinary actions; and employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant or intentions (e.g. to acquire goods or services). Organizations subject to PIPEDA, including WSPs, may only collect personal information that is necessary for the identified purposes. This collection must be limited to what is reasonable in the circumstances and must consider the balancing of customer needs against privacy rights.

As outlined by the Privacy Officers during the interviews and in the participating WSPs' online privacy policies, all participating WSPs collect similar types of personal information (PI) in order to conduct day-to-day business functions. The following personal information is collected directly from customers: name, phone number, email address, billing address, date of birth (DOB), government-issued identification (ID), social insurance number (SIN) (for credit check purposes only), payment history, usage history and location data (for billing purposes only). A

[6] Office of the Privacy Commissioner of Canada. A Guide for Businesses and Organizations: Privacy Toolkit – Canada's Personal Information Protection and Electronic Documents Act, December 2015. P. 3. https://www.priv.gc.ca/media/2038/guide_org_e.pdf.

majority of the participating WSPs collect cookies on their websites. Less than half collect call recordings (e.g. from customer service centres), preferred language of the customer, other authorized account user information, information on customer preferences and movie history (e.g. if the customer is also a television subscriber). See **Table 1** below for a detailed listing of types of personal information collected by WSPs directly from customers.

Table 1: Types of personal information collected by WSPs directly from customers

	WSP 1	WSP 2	WSP 3	WSP 4	WSP 5	WSP 6	WSP 7	WSP 8	WSP 9	WSP 10	WSP 11	WSP 12	WSP 13	WSP 14	WSP 15
Name	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Phone number	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Email address	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Billing address	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DOB	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Government-issued ID	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SIN	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Call recordings		✓	✓	✓	✓	✓						✓	✓		
Payment history	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Usage history	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Location data	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Preferred language							✓	✓	✓			✓	✓		

	WSP 1	WSP 2	WSP 3	WSP 4	WSP 5	WSP 6	WSP 7	WSP 8	WSP 9	WSP 10	WSP 11	WSP 12	WSP 13	WSP 14	WSP 15
Other authorized account user information							✓	✓	✓			✓	✓		
Information on customer preferences[7]							✓	✓	✓			✓	✓		
Movie history[8]							✓	✓	✓						

WSPs may also collect personal information about customers via a third party. For example, all of the major WSPs use a system of dealer networks to conduct business with customers 'on-the-ground' (e.g. a kiosk in a shopping mall). These dealer networks collect the same personal information that WSPs collect from customers who sign up with the WSP directly (e.g. name, phone number, email address, DOB, government-issued ID, SIN). Some WSPs also collect personal information indirectly from third party credit check companies (e.g. Equifax) that provide WSPs with the results of a customer's credit check. However, it was found that most of the small WSPs do not rely upon indirect collection of customer PI and instead collect directly from the customer.

Table 2: Types of PI collected by WSPs via third parties

	WSP 1	WSP 2	WSP 3	WSP 4	WSP 5	WSP 6	WSP 7	WSP 8	WSP 9	WSP 10	WSP 11	WSP 12	WSP 13	WSP 14	WSP 15
Name		✓	✓	✓	✓	✓	✓	✓	✓			✓	✓		
Phone number		✓	✓	✓	✓	✓	✓	✓	✓			✓	✓		
Email address		✓	✓	✓	✓	✓	✓	✓	✓			✓	✓		
DOB		✓	✓	✓	✓	✓	✓	✓	✓			✓	✓		

[7] This is collected via surveys or while a customer service representative is assisting a customer.
[8] This is collected from a WSP-provided TV service.

	WSP 1	WSP 2	WSP 3	WSP 4	WSP 5	WSP 6	WSP 7	WSP 8	WSP 9	WSP 10	WSP 11	WSP 12	WSP 13	WSP 14	WSP 15
Government-issued ID		✓	✓	✓	✓	✓	✓	✓	✓			✓	✓		
SIN		✓	✓	✓	✓	✓	✓	✓	✓			✓	✓		
Credit check results		✓	✓	✓	✓	✓	✓	✓	✓			✓	✓		
Usage history							✓	✓	✓			✓	✓		
Location data							✓	✓	✓			✓	✓		
Preferred language							✓	✓	✓			✓	✓		
Other authorized account user information							✓	✓	✓			✓	✓		
Information on customer preferences[9]							✓	✓	✓						

Based on the interviews, six (6) WSPs have a formal sensitivity classification system (e.g. high, medium, low) for collecting customer PI. For these WSPs, financial information (e.g. credit check results, credit card information) ranks as the highest level of sensitivity. Eight (8) WSPs currently have an informal (e.g. undocumented) PI sensitivity classification, while one WSP does not have any method of classifying the sensitivity of customer PI. Several WSPs also consider non-privacy related legal requirements when determining the sensitivity of personal information. For example, many WSPs also collect personal information in order to ensure compliance with the Payment Card Industry Data Security Standard.

Most of the participating WSPs collect metadata which is used for operational purposes only (e.g. length of a phone call for billing purposes), while two small WSPs do not collect any metadata given their infrastructure.

[9] This information is collected via surveys or while a customer service representative is assisting a customer on the phone.

Based on the interview results and privacy policy review, it appears that WSPs collect PI in accordance with their obligations under PIPEDA and appropriately outline the purposes of this collection in their privacy policies.

3.2 How WSPs use customer data, including the disclosure, monetization or sale of data to third parties

The OPC provides guidance to organizations on the appropriate use, disclosure, and retention of customer PI for business operations. This includes:

- Use or disclose PI only for the purposes for which it was collected, unless the individual consents;
- Keep PI only for as long as necessary to satisfy its purposes;
- Keep PI used to make a decision about an individual for a reasonable amount of time, so that the individual may obtain the information after a decision has been made; and
- Destroy or anonymize PI that is no longer needed for an identified purpose or legal requirement.[10]

According to interviews and review of WSP privacy policies, WSPs use customer PI in order to support their operational activities, including but not limited to the activities outlined below:

- Mailing communications to customers;
- Mailing bills to customers;
- Creating marketing materials (internally);
- Validating customer identities;
- Processing customer payments;
- Providing customer service assistance;
- Understanding customer needs and preferences;
- Understanding customer eligibility for products and services;
- Developing and enhancing products and services offerings;
- Managing business operations, including employment matters; and
- Meeting legal and regulatory requirements.

All Privacy Officers definitively stated that the WSPs do not sell customer PI to third parties. Based on the privacy policies of the participating WSPs, customer PI is disclosed to third parties for the purposes of providing operational support to the

[10] Office of the Privacy Commissioner of Canada. A Guide for Businesses and Organizations: Privacy Toolkit – Canada's Personal Information Protection and Electronic Documents Act, December 2015. P. 19. https://www.priv.gc.ca/media/2038/guide_org_e.pdf.

WSP (e.g. billing and mailing). See **Table 3** below for a list of common purposes for which customer PI is disclosed to third parties.

Table 3: Common purposes for which customer PI is disclosed to third parties

	WSP 1	WSP 2	WSP 3	WSP 4	WSP 5	WSP 6	WSP 7	WSP 8	WSP 9	WSP 10	WSP 11	WSP 12	WSP 13	WSP 14	WSP 15
Mailing	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Billing	✓	✓	✓	✓	✓		✓	✓	✓		✓	✓	✓		✓
Product development		✓	✓	✓	✓						✓	✓	✓	✓	
Marketing		✓	✓	✓	✓						✓	✓	✓	✓	
Credit checks		✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	
Disclosures required by law or emergency	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Providing information to an authorized agent of the customer		✓	✓	✓	✓		✓	✓	✓			✓	✓	✓	
Research or data processing		✓	✓	✓	✓		✓	✓	✓			✓	✓		
WSP third-party agent services (e.g. sales)		✓	✓	✓	✓		✓	✓	✓			✓	✓		✓
Long distance billing	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Although WSP privacy policies indicate the above disclosures of customer PI, some of these may constitute disclosures beyond what a customer may typically consider as a disclosure of PI. For example, disclosures of PI for product development,

marketing, research, and third-party agent services may not typically be contemplated by a wireless customer. Further, terms such as “marketing” and “research” are quite broad, and customers may not fully understand these disclosures without requesting further information from the WSP, a practice that does not commonly occur in the wireless industry. This suggests that WSPs should consider means of clarifying to customers the ways in which PI is disclosed beyond what may be reasonably expected. [11]

3.3 Built-in privacy protections

PIPEDA is based on the ten (10) privacy principles of the Canadian Standards Association Model Code for the Protection of Personal Information (“CSA Model Code”), which became recognized as a national standard for privacy protection in 1996. The CSA Model Code is used across Canada and the world as the basis for privacy legislation, policies and procedures. CSA Model Code is made up of the following ten principles:

1. Accountability
2. Identifying Purposes
3. Consent
4. Limiting Collection
5. Limiting Use, Disclosure and Retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual Access
10. Challenging Compliance

According to the OPC, businesses should be aware that in addition to the principles set out in PIPEDA, they have an overriding duty that any collection, use or disclosure of PI must only be used for purposes that a reasonable person would consider appropriate in the given situation.[12] This is an essential part of maintaining customer trust.

Throughout the interviews, the Privacy Officers discussed a number of privacy protections in place to protect customer PI, including:

[11] Office of the Privacy Commissioner of Canada. A Guide for Businesses and Organizations: Privacy Toolkit – Canada’s Personal Information Protection and Electronic Documents Act, December 2015. https://www.priv.gc.ca/media/2038/guide_org_e.pdf.
[12] Office of the Privacy Commissioner of Canada. A Guide for Businesses and Organizations: Privacy Toolkit – Canada’s Personal Information Protection and Electronic Documents Act, December 2015. https://www.priv.gc.ca/media/2038/guide_org_e.pdf.

De-identification

WSPs use de-identified aggregate data to make informed choices about which services to offer to customers and/or where to build their networks (e.g. physical towers).

Anonymization of PI

WSPs anonymize customer data once the individual is no longer a customer (e.g. two (2) years after a contract has expired/terminated). This enables the WSP to continue to use the anonymized data to drive business insights.

Privacy Accountability Frameworks

A privacy accountability framework refers to a model of accountability and responsibility for privacy that is embedded in an organization through its various privacy roles (e.g. Privacy Officer, Privacy Lead). All of the participating WSPs have an accountability framework for privacy, but with varying structures. In general, the Chief Privacy Officer (CPO) or equivalent has ultimate accountability for the protection and safeguarding of customer PI. In some instances, the CPO is assisted by an Associate Chief Privacy Officer, or equivalent role. Major WSPs are more likely to have a dispersed model in which each department contains an appointed 'Privacy Champion' who acts as the privacy liaison within their department and provides a valuable business view to privacy leaders within their organization. Major WSPs also assign various aspects of their privacy governance structure to a privacy ombudsman office, cyber security team, data loss prevention team, legal team and/or corporate security team. Flanker brand WSPs tend to leverage the privacy protections already in place at the major WSP with which they are affiliated. Small WSPs have smaller privacy accountability structures, usually consisting of a general manager with privacy accountability who may have one or two additional employee resources assisting with customer privacy complaints. These varying accountability structures are consistent in other industries, where the maturity of privacy governance is often proportional to the organization's size and resources.

Privacy oriented customer service

As stated in the Wireless Code, WSP contracts and related documents (e.g. privacy policy) must state how a customer can make a complaint about wireless services.[13] All of the participating WSPs describe on their websites and in their privacy policies how a customer may file a complaint (e.g. call centre phone number, complain email address). In dealing with privacy and/or service complaints, WSPs employ a variety of channels to provide similar complaint resolution services. All participating WSPs have a privacy mail box on their website, an email address customers can send complaints to and/or a call centre with customer service representatives

[13] Canadian Radio-television and Telecommunications Commission. The Wireless Code. June 2013. http://crtc.gc.ca/eng/archive/2013/2013-271.pdf.

equipped to deal with privacy inquiries and complaints. Some of the major WSPs also have an investigative group which handles larger privacy issues.

Security

Accountability for ensuring appropriate security measures are taken to protect customer PI tends to fall in different areas according to the different WSP. For many WSPs, the Chief Security Officer (or equivalent) maintains ultimate accountability for appropriate security measures, and is generally supported by a security team which may include a data loss prevention team. Other Privacy Officers expressed that accountability in this area is shared between both the Chief Privacy Officer and the Chief Security Officer and their respective supporting teams.

Overall, WSPs of all sizes tend to have a privacy accountability model in place to embed the protection of customer privacy into their organization. What type of privacy accountability model is typically dependent on the size of the organization (i.e. major, flanker, or small), which is consistent with varying structures across other industries. For example, a relatively small WSP might have a General Manager with ultimate accountability for privacy and an Assistant with privacy responsibilities, while a major WSP may have an intricate team of privacy stakeholders (e.g. Privacy Officer, a Privacy Team, Privacy Champions or Leads within the various departments).

3.4 How WSPs handle privacy breaches

New amendments to PIPEDA are making privacy breach notification clauses and logging of security incidents mandatory under the recently enacted Digital Privacy Act (DPA)[14]. Once enacted, the breach notification provisions of the DPA will amend PIPEDA to require organizations to notify not only affected individuals but also the OPC in the event of a breach, and other relevant stakeholders. Under the breach notification provisions, private organizations – including WSPs – that become aware that they have experienced a breach of security safeguards must conduct a situational analysis to determine whether or not the breach poses a "real risk of significant harm" to an individual whose personal information was involved in the breach. If this risk exists, organizations must report the breach to the OPC, as well as to individuals impacted by the breach in a form and manner prescribed by the DPA. Further, the DPA requires record keeping of all breaches, regardless of the risk of significant harm.

Consistent with the purpose of the PIPEDA amendments, it was noted from the interviews that twelve (12) of the WSPs have a formal breach policy or procedure in

[14] The Government of Canada. The Digital Privacy Act. June, 2015. http://laws-lois.justice.gc.ca/PDF/2015_32.pdf.

place to help manage privacy breaches. The Privacy Officers from twelve (12) of the participating WSPs follow the privacy breach guidelines provided by the OPC[15]. These twelve WSPs have a formal privacy breach policy or procedure in place and a designated team of individuals who are responsible for identifying a breach and responding to it with support from other teams within the organization. The major WSPs also have comprehensive privacy breach response playbooks. The three remaining WSPs are small in size, have not experienced a privacy breach, and do no currently have a documented privacy breach policy or procedure in place.

In the interviews, the Privacy Officers of all WSPs stated that notification of a privacy breach to the customer occurs on a case-by-case basis. For example, a minor privacy incident might warrant a notification sent through mail on a customer's next bill, while a large privacy breach with severe privacy implications for the customer (e.g. identity theft) may merit a call or email shortly after the scope of the breach is confirmed. All participating WSPs have a 'customer first' focus which implies that if potential harm may come to the customer as a result of the breach, they will notify the customer. However, the WSP determines the timing and manner in which they notify the customer based on the scale and severity of the privacy breach or incident.

For those WSPs with a documented privacy breach policy, notifying customers of a privacy breach involving a third party would be treated in the same manner as a breach at the WSP, with the exception of heightened involvement from their legal and procurement teams. For example, the Privacy Officer at one major WSP noted that when it recently learned of a breach at a third party smartphone provider, the WSP reached out to its customers to notify them of the breach as part of its 'customer first' perspective.

The interview findings demonstrated that the large WSPs are prepared for the PIPEDA amendments while the smaller WSPs still have work to do to ensure compliance with the upcoming changes.

3.5 How WSPs give customers control over how their personal information is handled

As outlined by the OPC in its toolkit[16] and confirmed by a privacy specialist at the OPC, the purpose of PIPEDA is to balance a business' needs against an individual's

[15] The Office of the Privacy Commissioner of Canada. Key Steps for Organizations in Responding to Privacy Breaches. August, 2007. https://www.priv.gc.ca/media/2086/gl_070801_02_e.pdf.

[16] Office of the Privacy Commissioner of Canada. A Guide for Businesses and Organizations: Privacy Toolkit – Canada's Personal Information Protection and Electronic Documents Act, December 2015. https://www.priv.gc.ca/media/2038/guide_org_e.pdf.

privacy rights. Part of this balance is ensuring that customers have control over how their personal information is handled. In an effort to provide wireless customers with the tools they need to control how their PI is managed, the Wireless Code outlines the following items WSPs should have in place:

- A privacy policy that is easy for customers to read and comprehend;
- A practice of providing customers with a permanent hard-copy of the contract and privacy policy at no charge immediately at the point of sale (or send a permanent hard-copy of the privacy policy to the customer within 15 days, if agreed to over the phone or online);
- A brief explanation of the privacy policy within the contract; and
- A practice of providing a minimum of thirty (30) calendar days' notice before making changes to their privacy policy, clearly explaining what the changes are and when they will come into effect.[17]

The following observations were made in regards to how the participating WSPs make their privacy policies readily available to consumers:

- Each participating WSP has a privacy policy publicly available on their website that outlines what information they collect, how they use that information and how they then protect their customers' privacy.
- Based on the interviews conducted, only one major WSP and its flanker-brand WSP provide a hard copy of their privacy policy to the customer when they sign their service agreement.
- All participating Privacy Officers maintain that customers may request a copy of their privacy policy, hard copy or electronic, at any time by calling, emailing (via a privacy email address or privacy mail box on their website) or inquiring at a store location.
- A majority of the WSPs will provide their privacy policy in alternative formats (e.g. braille, large font), upon request.
- A majority of the participating WSPs have a simplified summary of the privacy policy included in their service contracts.
- According to the interviews, customer requests for hard copies of their respective privacy policy are rare amongst WSPs of all sizes.

The following observations were made in regards to how the participating WSPs communicate changes to their privacy policies to their customers:

- According to interviews with the Privacy Officers of WSPs, changes to their respective privacy policies do not occur regularly.
- When changes do occur, all of the WSPs explain that part of their communication to their customers involves notifying them on the company website with a minimum of 30 days' notice.

[17] Canadian Radio-television and Telecommunications Commission. The Wireless Code. June 2013. http://crtc.gc.ca/eng/archive/2013/2013-271.pdf.

- Some of the major WSPs also provide Frequently Asked Questions (FAQs) on their website to accompany the new policy.
- In addition to using their website to alert customers of privacy policy changes, some WSPs also send bill inserts to customers, SMS text messages and/or emails notifying them of the change.
- WSPs with a large amount of customers using month-to-month payment plans are more likely to send out an SMS text notification to customers.

In the OPC's submission to the CRTC's 2012 public proceeding that established the Wireless Code, the OPC summarizes the criticality of WSPs having customer-friendly privacy policies that provide enough information around how PI is used as well as instructions for how to make a complaint[18]. In general, the findings in the Privacy Officer interviews are consistent with the submission by the OPC on the public record of the Wireless Code proceeding.

Customers may also control how their PI is handled through opting in or out of various additional features. For example, one of the major WSP and its flanker-brand utilize an online behavioural marketing program which creates customized ads for customers. For this program, express consent was collected from customers and the major WSP also worked with the OPC to ensure it was protecting privacy throughout the program lifecycle. Other WSPs do not use additional features and those that are considering doing so acknowledge that they would obtain express consent from their customers. None of the participating WSPs, based on interviews conducted, use customer PI for secondary purposes without expressed consent.

Twelve (12) of the participating WSPs rely on express and implied consent, while three (3) small WSPs rely solely on implied consent and do not use customer PI for purposes other than what was originally intended.[19] For example, when a customer signs up for a phone plan with a WSP they expect that their PI (e.g. name, mailing address) will be used by the WSP in order to provide the service. WSPs tend to rely on implied consent when the activity is a part of the WSP's service and is a general expectation. For credit checks, express consent is obtained across all participating WSPs. WSPs do not often use customer PI for new uses beyond what is originally contemplated, but if/when they do, they all require consent based upon the information sensitivity level.

---

[18] The Office of the Privacy Commissioner of Canada. Proceeding to establish a mandatory code for mobile wireless services: Submission of the Office of the Privacy Commissioner of Canada to the Canadian Radio-television and Telecommunication Commission (CRTC). December 2012. https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_crtc_121204/.

[19] Express consent is given explicitly in writing, orally or through an online action (e.g. clicking "I agree"), while implied consent is derived from situations in which consent may be reasonably inferred from the action of the individual. From: Office of the Privacy Commissioner of Canada, *Privacy Toolkit: A Guide for Businesses and Organizations*, December 2015. https://www.priv.gc.ca/media/2038/guide_org_e.pdf.

These findings suggest that WSPs are mindful of customer preferences for various features and ensure that consent is properly obtained when contemplating new uses/disclosures of PI.

3.6 Restrictions WSPs place on the collection and use of personal information by third parties

In this report, the term "third parties" refers to external providers of advertising or marketing services, partner WSPs and/or any vendors providing WSPs with an operational service (e.g. bill printing). According to the OPC,[20] organizations should consider the following key tips when transferring PI to third parties:

- Name a person to handle all privacy aspects of the contract;
- Limit use of the personal information to the purposes specified to fulfil the contract;
- Limit disclosure of the information to what is authorized by your organization or required by law;
- Refer any people looking for access to their personal information to your organization;
- Return or dispose of the transferred information upon completion of the contract;
- Use appropriate security measures to protect the personal information; and
- Allow your organization to audit the third party's compliance with the contract as necessary.

According to the interviews, all participating WSPs follow some or all of the OPC's advice above regarding transferring PI to third parties. All WSPs use contractual agreements to restrict the collection and use of PI by third parties. Additionally, all of the Privacy Officers expressed that it is the WSP's preference not to disclose PI to third parties if the business purpose for which a third party is retained may be adequately performed without such information. A majority of the participating WSPs restrict third parties collection and use of customer PI by putting various access controls in place (e.g. view-only access). Many WSPs have their own mechanisms for restricting third parties that are unique to their organization. For example, a WSP's legal counsel may advise the procurement team on what information a third party should have access to and what information is not necessary for the third parties' business purposes and then the information the third party has access to will be limited accordingly.

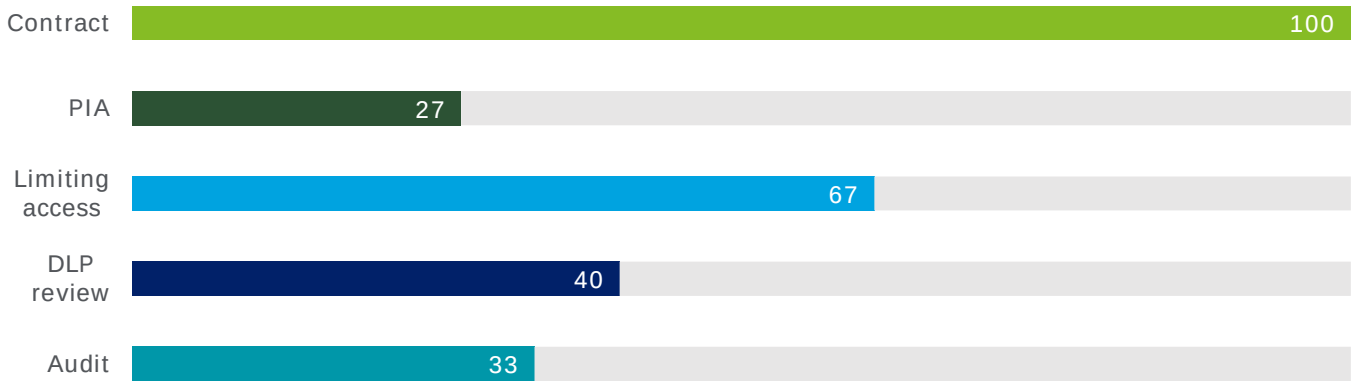
[20] Office of the Privacy Commissioner of Canada. A Guide for Businesses and Organizations: Privacy Toolkit – Canada's Personal Information Protection and Electronic Documents Act, December 2015. https://www.priv.gc.ca/media/2038/guide_org_e.pdf.

The major WSPs were more likely to have a Privacy Impact Assessment (PIA), audit or Data Loss Prevention (DLP) review process in place for the purpose of vetting third parties. Having third party vetting mechanisms in place contributes to an organization's overall risk management practices and validates the strength of privacy controls already in place to safeguard customer PI.

Fourteen (14) of the fifteen (15) participating WSPs have a process in place for ensuring the return or disposal of customer PI previously shared with a third party for their relevant business purposes. For example, upon the completion of a WSP initiative a third party must either return or destroy (with a receipt of destruction) the WSP-collected customer PI. Whether or not the information is returned or destroyed is dependent upon the WSP's own discretion. Only the smallest participating WSPs do not have this practice in place, again due to their limited interaction with third parties.

Flanker-brand WSPs tend to leverage third parties procured by their major WSP while smaller WSPs, due to their limited interaction with third parties, do not have formally documented practices for restricting third party collection and use of customer PI. These tools to limit disclosure of information to third parties are documented in **Chart 1** below.

Chart 1: Tools WSPs use to limit disclosure of information to third parties



*Numbers reflect % of participating WSPs

3.7 Wireless Service Providers and emerging technologies

3.7.1 Location-based features

Location-based services refers to services offered through a mobile phone that use the device's geographical location. All of the interviewed Privacy Officers explained that the WSPs use location-based tracking for instances in which an emergency is occurring (e.g. a 911 phone call). Some of the major WSPs also utilizes location information for the purposes of targeted marketing, using both prior notice to the customer as well as expressed consent (e.g. opt-in). Overall, the smaller WSPs tend to not use location-based features, with the exception of emergency situations.

The Public Interest Advocacy Centre (PIAC), in their report on location-based technologies and the law[21], argue that as Canadians continue to increasingly use smart phones and other mobile devices, PIPEDA may not adequately protect Canadians from having their locational information over-collected or even misused by third parties. The PIAC also explains that Canadian telecommunications providers may currently have the most direct access to mobile-device user information and as a result should consider customer privacy a top priority. While WSP Privacy Officers stated that location data is collected from customers, it is collected for indicated purposes only (as described above) and is not directly used by the WSP beyond operational purposes or without opt-in consent.

3.7.2 The Internet of Things (IoT) and augmented reality

None of the participating Privacy Officers identified their respective WSP as currently offering IoT solutions or augmented reality to their individual customers. However, WSPs of all sizes express interest in using augmented reality technologies in the future or at least better understanding applications of augmented reality in their business. WSPs have, however, started venturing into the realm of emerging technologies, although at varying degrees and sometimes in only ancillary ways. For example, several WSPs currently offer Internet of Things solutions, but the vast majority of these services target large business customers, not individuals.

3.7.3 Cloud storage, Internet Exchange points (IXPs) and jurisdiction

During the Privacy Officer interviews, it was found that a majority of WSPs use cloud storage, with a few of those using cloud services having already conducted PIAs on their third party vendor. Of the participating WSPs using the cloud, some ensure no PI goes into the cloud while others do store PI in the cloud but have strict jurisdictional rules[22] around doing so. The majority of cloud-using WSPs only store

[21] The Public Interest Advocacy Centre (PIAC). Off the Grid: Pinpointing Location-based technologies and the Law. June 2015. http://www.piac.ca/wp-content/uploads/2015/09/OCA-2014-15-Off-the-Grid-Location-based-technologies-and-the-law-Final-Report.pdf.

[22] These rules refer to the authority given by law to a court to rule on legal matters within a particular geographic region.

non-sensitive information in the cloud and are conscientious about addressing customer concerns and keeping servers local. Small WSPs are more likely to not use cloud storage services due to their smaller information holdings and more limited resources, but are considering using these services in the future. One participating WSP stores a subset of its wireless billing information in the cloud. WSPs are increasingly aware of the risks of storing wireless billing information in the cloud given recent concerns surrounding wireless billing payment models. These concerns include: the potential misuse of additional customer information they learn (e.g. detailed purchase history and merchants involved); and the increased possibility of "phone bill cramming" (e.g. charges under ambiguous or misleading headings such as "service charge" or "other fees").[23]

The interview findings were consistent with a recent University of Toronto report that recommends that Canadian organizations avoid outsourcing electronic communications services beyond Canadian borders.[24] The report states that Canadian public IXPs can help keep communications traffic local. If these services are outsourced, then organizations should conduct a PIA and TRA on the third party service provider as well as revisit past decisions to outsource.

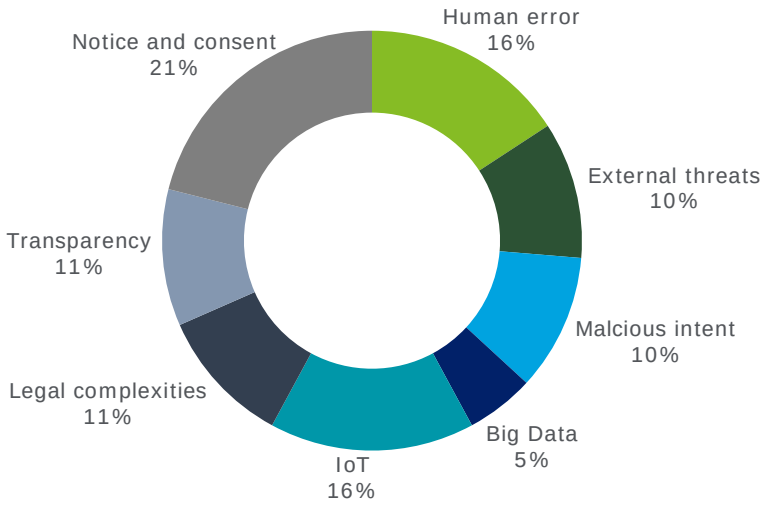
When asked about IXPs, the Privacy Officers of major and flanker-brand WSPs stated that their organizations have the capability to use both Canadian and non-Canadian IXPs for billing purposes only (e.g. roaming charges). A few of the small WSPs are only able to utilize Canadian IXPs based on their infrastructure. All of the Privacy Officers expressed that their WSPs do not respond to international requests from law enforcement – a court order will always need to be endorsed by a Canadian court before a Canadian WSP responds.

3.8 The greatest challenges to protecting the privacy of wireless customers in today's market

WSP Privacy Officers identified the following as the greatest challenges to protecting customer privacy in today's market (See **Chart 2** below).

Chart 2: The greatest challenges to protecting wireless customer privacy in today's market

[23] Carlisle Adams. Have Money, Will Travel: A Brief Survey of the Mobile Payments Landscape. June 2013. https://www.priv.gc.ca/media/1771/mp_201306_e.pdf.
[24] University of Toronto. Seeing Through the Cloud: National Jurisdiction and Location of Data, Servers, and Networks Still Matter in a Digitally Interconnected World. 2015. http://ecommoutsourcing.ischool.utoronto.ca/wp-content/uploads/BohakerAustinClementPerrin_SeeingThroughTheCloud-PublicReport-15Sept2015.pdf.



Notice and consent: Privacy Officers face challenges to providing meaningful notice to customers and obtaining meaningful consent from customers. The participating Privacy Officers see this as the result of the growing complexity of services, technologies, the wireless market and today's market more broadly.

Human error: Privacy Officers express concern regarding human errors, or unintentional mistakes made by employees that could cause a privacy incident or breach. Many of the Privacy Officers see challenges with providing employee training and awareness on an ongoing basis as a potential cause for these human errors.

The Internet of Things (IoT): Privacy Officers and the OPC see the IoT as an emerging challenge to protecting wireless customer privacy. Privacy Officers see IoT as a unique challenge and understand that they cannot control how individuals share their PI across various applications and devices, but that a risk to their customers' privacy may still exist. A recent OPC research paper on IoT contends that IoT may benefit consumers in the retail market and home environments as it provides a method of generating detailed customer behaviour analytics, allowing for increasingly tailored and consistent marketing across devices (e.g. phones, tablets)[25]. Conversely, the security and privacy risks of IoT include, for example, as technology improves there is a possibility that de-identified data could be re-identified. [26]

[25] The Office of the Privacy Commissioner of Canada. The Internet of Things: An introduction to privacy issues with a focus on the retail and home environments. February, 2016. https://www.priv.gc.ca/media/1808/iot_201602_e.pdf
[26] Federal Trade Commission Staff Report. Internet of Things: Privacy & Security in a Connected World.

Legal complexities: Privacy Officers express facing challenges due to multi-jurisdictional privacy laws. Complying with several legislations across Canada requires these WSPs to spend more time and resources on compliance.

Transparency: Privacy Officers view providing a reasonable amount of transparency to customers as a challenge. To exemplify, some WSPs receive 'blanket requests' for information about a customer's account that may take days to access and provide to the customer, taking away from the WSPs time and privacy resources. These WSPs want to be transparent, but within reason. The OPC also identified this as an important emerging issue.

External threats: Privacy Officers see external threats (e.g. denial of service attacks) as one of the greatest challenges to protecting the privacy of wireless customers.

Malicious intent: Privacy Officers view malicious intent or internal threats (e.g. a rogue employee stealing customer credit card information) as one of the major challenges impacting the protection of wireless customer PI.

Big data: Privacy Officers wonder what kinds of privacy risks the rise of big data analytics may bring (e.g. issues with anonymizing large sums of data, accuracy of the data).

Other challenges identified by the OPC

In an interview with a privacy specialist from the OPC, the following other privacy issues facing WSPs were identified, including:

- Challenges for smaller WSPs that do not have the privacy resources major WSPs have;
- Some WSPs may face challenges adapting to the new breach notification amendment to PIPEDA stemming from the breach notification amendment of PIPEDA; and
- Employee snooping (e.g. a family member looking at their relatives wireless account information without consent).

4. Conclusion and summary of insights

The results of the interviews provide evidence demonstrate that the wireless industry is not necessarily unique from other industries when it comes to protecting the personal information of individuals. Most Privacy Officers did not see the challenges described in the detailed analysis section above as unique to the wireless industry. Rather, these challenges were seen as endemic across all industries due to recent and constant changes in technology (e.g. big data, IoT).

While most WSPs were contemplating providing emerging technologies, such as augmented reality, to wireless customers, they stated that they did not currently offer these types of services to their individual wireless customers and as such are not currently building in privacy protections to regulate these technologies.

WSPs have, however, started venturing into the realm of emerging technologies, although at varying degrees and sometimes in only ancillary ways. For example, several WSPs currently offer Internet of Things solutions, but the vast majority of these services target large business customers, not individuals.

While participating-WSP privacy policies provide an overview of the disclosures of customer PI they may make, some of these may constitute disclosures beyond what a customer may typically consider as a disclosure of PI. For example, disclosures of PI for product development, marketing, research, and third-party agent services may not typically be contemplated by a wireless customer. Further, terms such as "marketing" and "research" are quite broad, and customers may not fully understand these disclosures without requesting further information from the WSP, a practice that does not commonly occur in the wireless industry. This suggests that WSPs should consider means of clarifying to customers the ways in which PI is disclosed beyond what may be reasonably expected. [27]

The report findings also demonstrated that similar to other industries, larger organizations have more resources in place to have documented practices and policies and therefore a more robust, mature framework for privacy. In the wireless industry, the "flanker" brands tend to leverage the models established by their larger brand. This leaves the smaller WSPs, some of which do have established privacy practices but others which have immature privacy frameworks.

[27] Office of the Privacy Commissioner of Canada. A Guide for Businesses and Organizations: Privacy Toolkit – Canada's Personal Information Protection and Electronic Documents Act, December 2015. https://www.priv.gc.ca/media/2038/guide_org_e.pdf.

Many Privacy Officers expressed that in today's market, the development of industry-specific laws may discourage innovation within the wireless market and create competitive imbalances in the broader market. While the Wireless Code has created consistency in the wireless industry for customers, all WSP Privacy Officers view PIPEDA as the central privacy regulation and standard by which privacy is governed in the wireless industry. In turn, WSP Privacy Officers have a deep understanding of PIPEDA and implement privacy measures within their respective organizations to ensure compliance. As such, any changes to the Wireless Code with respect to privacy should be mindful of the strong privacy protections outlined in PIPEDA and should be made in consultation with the OPC.

Regardless of the industry, an important part of maintaining customer trust is ensuring that customer needs are balanced against a customer's privacy rights. This may be done by providing customers with ways to control their personal information in a meaningful way. Another way that privacy rights may be maintained – and that was expressed by the WSP Privacy Officers – is through education not only at the business level but at the school level as well. Education across Canada on privacy and information-sharing technologies (e.g. social media) would greatly benefit consumers in better understanding how to protect their information, with companies in turn responding to consumer demands.

Appendix A – Participating WSPs

- Bell Mobility
- Rogers
- TELUS
- Virgin Mobile
- Fido
- Chatr
- Koodo
- Public Mobile
- Brooke Telecom
- Cityphone
- Eastlink
- Execulink
- Hay Communications
- SaskTel
- WIND Mobile (Shaw)

Appendix B – Sample Interview Questionnaire

Deloitte LLP has been retained to write a report on behalf of the Canadian Radio-television and Telecommunications Commission (CRTC) on the Collection and Use of Canadians' Personal Information by Wireless Service Providers (WSPs) and Third Party Entities. The purpose of this report is to assist the CRTC with its upcoming review of its Wireless Code and to contribute to the CRTC's overall understanding of the current and emerging privacy issues in Canada's rapidly evolving retail mobile wireless service industry. In order to prepare the report, the CRTC has requested that we conduct interviews with Privacy Officers at twelve (12) Canadian WSPs. Please note that the identities of the Privacy Officers interviewed will remain confidential and none of your responses will be associated with your company's name. However, the report will include a list of WSPs that participated in the interviews.

The following questionnaire will help inform the discussion during our scheduled interview time. Please review this questionnaire prior to our scheduled interview time, and come prepared to answer these questions. Some responses may contain similar information to that provided in previous responses.

If you serve as the Privacy Officer for more than one WSP, please be prepared to answer each question separately for each provider.

Question	Answer
Section 1: Accountability	
1. Who is the individual who handles all privacy aspects of the customer contract?	
2. To whom should complaints about privacy matters be referred?	
3. Who is accountable for ensuring the appropriate security measures to protect the personal information (PI)?	

Question	Answer
Section 2: Privacy Policies	
4. How can customers access your privacy policy (other than online)? In which formats? What steps do customers have to take to get a paper copy or an alternate form of a privacy policy?	
5. How do you communicate updates to your privacy policy to consumers? Within what time frame do you communicate these updates before they take effect?	
Section 3: Personal Information Collection, Use, Disclosure, and Destruction	
6. What types of personal information does your organization collect directly from its customers? Examples may include payment history, location data, tracking information.	
7. What types of personal information does your organization collect from its customers via a third party? Examples may include PI from smartphone operating system providers or third party application providers and advertisers; metadata.	
8. Does your organization classify the levels of sensitivity of the personal information it collects? If so, how?	
9. How does your organization obtain consent from individuals? Specifically, how does your organization obtain consent when personal information is used for a purpose other than the original use? (provide some examples)	
10. Do you have a means of evaluating whether handling of PI remains consistent with the purposes identified in the privacy policy (for which consent was initially provided)? If so, what is that process? Who is accountable for managing the process?	

Question	Answer
11. Are additional features (e.g. customizing profiles, advertisements, and location-based features) offered on an opt-in or opt-out basis? What does this look like?	
12. How do you limit disclosure of the information to third parties to that which is authorized by your organization or required by law? Who oversees this (who is accountable)? How do you communicate this to consumers?	
13. What are your procedures for returning or disposing of the transferred information upon completion of the contract? Upon the completion or end of a particular initiative (e.g. an online behavioural marketing program that has come to an end)?	
Section 4: Third Parties	
14. Does your organization share or sell the customer personal information it collects to third parties? Please provide some general examples (e.g. marketers, app providers).	
15. In cases where customer personal information is shared or sold to third parties, how does your organization ensure customer privacy is protected? For example, are customers required to opt in to participate? Are they provided notice?	
16. What kinds of special features does your company use – e.g. customizing profiles, advertisements, location-based features), and which types of third parties do you use for these special features? Do they have access to customer information?	
17. How do you ensure that any third parties with access to customer information use equivalent privacy and security safeguards? Do you impose	

Question	Answer
any restrictions on third parties to protect the privacy of their customers?	
18. Does your organization audit the third party's compliance with the contract? If so, please describe the process and frequency.	
19. What is the procedure for notifying customers of new uses of their data, which may involve third parties? Is consent obtained using opt-in or opt-out measures? If it depends on the initiative, what are the relevant criteria for deciding?	
Section 5: Emerging Issues	
20. **Tracking:** Do you use location-based or tracking related features? If so, which kinds of features are employed and how is consent obtained from customers for these features?	
21. **Cloud:** Do you use cloud storage for any of your data? Does this data contain PI? What kinds of PI? Which providers? Have you expressed any preferences around the storage of your data, like location, and if so, what have the cloud providers responded with?	
22. **Jurisdiction:** What kinds of Internet Exchange Points (IXPs) do you use (e.g. local/Canadian)? Does identifiable data ever pass through another jurisdiction? Is it encrypted? How do you respond to information requests from other jurisdictions' law enforcement? How is this process explained to customers?	
23. **Internet of Things/Augmented Reality:** Which kinds of IoT/AR technologies do you support with wireless network services? How do these contracts differ from mobile contracts? Where do you refer customers who have privacy questions – to the manufacturer's privacy policy	

Question	Answer
and team, or to your own privacy policy and team?	
24. **Metadata:** How do you collect, use, store, and dispose of metadata? How do you classify metadata – is it protected like personal information or sensitive information? Do you share or sell metadata to third parties? How do you mitigate for risks of re-identification?	
Section 6: Breaches	
25. How and when does your organization notify customers of a privacy breach?	
26. Does the organization notify customers of privacy breaches involving third parties?	
27. If a privacy breach does occur, what steps does your company take to mitigate the impacts of such breaches?	
Section 7: Concluding Thoughts	
28. What, from your perspective, are the greatest challenges in protecting the privacy of wireless customers in today's market?	

Appendix C – Bibliography

1. Adams, C., University of Ottawa, *Have Money, Will Travel: A Brief Survey of the Mobile Payments Landscape*, June 2013. https://www.priv.gc.ca/media/1771/mp_201306_e.pdf

2. Bohaker, H. et al., University of Toronto, *Seeing Through the Cloud: National Jurisdiction and Location of Data, Servers, and Networks Still Matter in a Digitally Interconnected World*, 2015. http://ecommoutsourcing.ischool.utoronto.ca/wp-content/uploads/BohakerAustinClementPerrin_SeeingThroughTheCloud-PublicReport-15Sept2015.pdf

3. British Columbia Freedom of Information and Privacy Association, *The Connected Car: Who's in the Driver's Seat? A Study on Privacy and On Board Vehicle Telematics Technology*, March 2015. https://fipa.bc.ca/connected-car/

4. Federal Trade Commission, *Internet of Things: Privacy & Security in a Connected World*, January 2015. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

5. Office of the Privacy Commissioner of Canada, "Proceeding to establish a mandatory code for mobile wireless services: Submission of the Office of the Privacy Commissioner of Canada to the Canadian Radio-television and Telecommunication Commission (CRTC)", December 4, 2012. https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_crtc_121204/

6. Office of the Privacy Commissioner of Canada, *Metadata and Privacy: A Technical and Legal Overview*, October 2014. https://www.priv.gc.ca/media/1786/md_201410_e.pdf

7. Office of the Privacy Commissioner of Canada, *Privacy Toolkit: A Guide for Businesses and Organizations*, December 2015. https://www.priv.gc.ca/media/2038/guide_org_e.pdf

8. Office of the Privacy Commissioner of Canada, *The Internet of Things: An introduction to privacy issues with a focus on the retail and home environments*, February 2016. https://www.priv.gc.ca/media/1808/iot_201602_e.pdf

9. Tech Policy Lab, University of Washington, *Augmented Reality: A Technology and Policy Primer*, September 2015.

http://techpolicylab.org/wp-content/uploads/2015/10/Augmented_Reality_Primer.pdf

10. White, G., Public Interest Advocacy Centre, *Off the Grid: Pinpointing Location-based Technologies and the Law*, June 2015. http://www.piac.ca/wp-content/uploads/2015/09/OCA-2014-15-Off-the-Grid-Location-based-technologies-and-the-law-Final-Report.pdf

www.deloitte.ca

Deloitte, one of Canada's leading professional services firms, provides audit, tax, consulting, and financial advisory services. Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited.