The Conference Board of Canada | Le Conference Board du Canada

Exploring Canada's Top Privacy Challenges.

Summary Report of the Canadian Privacy Summit 2016

REPORT AUGUST 2016

Exploring Canada's Top Privacy Challenges: Summary Report of the Canadian Privacy Summit 2016

Alison Howard and Mark Robbins

Preface

This report provides information and insights on stakeholder positions concerning the legislative environment for privacy and data, and other emerging privacy issues, as expressed at the Canadian Privacy Summit 2016. Canada's collective privacy challenge is to determine how best to protect the personal privacy of individuals while encouraging organizations to use data to prosper and grow. Private and public sector summit participants agreed on the need to identify or create a meaningful, consent-based model of privacy for the digital age.

To cite this report: The Conference Board of Canada. *Exploring Canada's Top Privacy Challenges: Summary Report of the Canadian Privacy Summit 2016*. Ottawa: The Conference Board of Canada, 2016.

CONTENTS

Acknowledgements

This report was prepared by The Conference Board of Canada under the direction of Dr. Michael Bloom, Vice-President, Industry and Business Strategy. The report was researched and written by Alison Howard, Associate Director, and Mark Robbins, Research Associate. It was reviewed internally by Andrew Pender, Associate Director, Organizational Excellence, and externally by Kim Norton, Director, Compliance and Privacy, Ontario Pension Board, Caroline Dignard, Vice President, Legal Affairs and Chief Privacy Officer, Cogeco Connexion, and John Liut, Director, Corporate Compliance and Chief Privacy Officer, Home Trust Company. This report was prepared with financial support from Innovation, Science, and Economic Development Canada. The findings and conclusions of this report are entirely those of The Conference Board of Canada. Any errors and omissions in fact or interpretation remain the sole responsibility of The Conference Board of Canada.

EXECUTIVE SUMMARY

Exploring Canada's Top Privacy Challenges: Summary Report of the Canadian Privacy Summit 2016

At a Glance

- This report provides information and insights on stakeholder positions concerning the legislative environment for privacy and data, and other emerging privacy issues, as expressed at the Canadian Privacy Summit 2016.
- Canada's collective privacy challenge is to determine how best to protect the personal privacy of individuals while encouraging organizations to use data to prosper and grow.
- Private and public sector summit participants agreed on the need to identify or create a meaningful, consent-based model of privacy for the digital age.

The Conference Board of Canada and the Office of the Information and Privacy Commissioner of British Columbia co-hosted the inaugural Canadian Privacy Summit on April 13–14, 2016, in Vancouver, British Columbia. It brought together many of Canada's foremost privacy experts from the public and private sectors in a wide-ranging conversation about the nature of privacy in Canada.

This event was designed to help establish common ground between attendees, promote deeper understanding on privacy issues in Canada, and ultimately foster the basis for solutions. The purpose of this report is to provide information and insights on stakeholder positions, as expressed at the summit, concerning the legislative environment for privacy and data, including the ***Personal Information Protection and Electronic Documents Act*** (PIPEDA), the ***Privacy Act***, and emerging privacy issues.

The expert community of summit participants holds a wide range of divergent opinions and interpretations of the state of privacy and privacy legislation in Canada. While those from the regulatory community tended to be more aware of the legal penumbra and legislative failings, those in the private sector were more conscious of regulatory burdens and practical barriers to implementation. As envisioned, the summit helped these disparate groups make significant progress toward understanding how their needs and actions affect one another.

Areas of Consensus and Concern

The privacy community at the summit achieved breakthroughs in finding common ground in several areas. First, participants agreed that consent was, and continues to be, an important mechanism for protecting privacy. However, most participants recognized the declining utility of

Advertising is one of the most hotly contested areas in the privacy community.

this principle as it was originally envisaged in the body of law. There was a general sense of urgency around the need to identify or create a meaningful, consent-based model of privacy for the digital age.

Second, participants agreed that providing more education to the private sector and the public would have a significant impact on compliance, perhaps more so than additional regulations and enforcement efforts. Nonetheless, participants appreciated that some regulations—particularly in the area of competitive advantage—can be constructive for industry. In such areas, the absence of targeted regulations can be harmful to industry and the privacy environment in general.

The summit made significant headway in identifying privacy objections in the digital age. Participants concluded that traditional legal means do not always provide clear limits on the use of data. With the new opportunities that technology offers, many privacy concerns stem less from the collection of data than from its inappropriate use.

Advertising is one of the most hotly contested areas in the privacy community. Inappropriately customized advertisements highlight some of the most egregious violations of privacy. Similarly, the persistence and frequency of tailored online advertisements is one of the greatest nuisances to Internet users. Yet, the ability to advertise to customers is one of the key functions of business and, when done properly, it can be advantageous to consumers as well. People seldom object to advertisements that accurately align with the purchases they intend to make.

Law enforcement and the security establishment are both struggling to understand and cope with the challenges surrounding digital privacy. Law and security efforts must contend with privacy issues for warrants, licence plate scans, counter-terrorism measures and, of course, maintaining public trust.

There is a global element to privacy, especially since so many new functions of the privacy sphere associated with technology are not constrained by geography. Participants agreed that Canada's privacy environment is more permissive than Europe's while still holding a higher standard of data protection than the United States.

To live and work in the modern world is to accept being part of a super-connected, global community.

Future Directions

Participants generally feel that Canada's core privacy legislation and regulations are sound, but could be improved with some modifications. Opportunities for improvement include:

- **Optimize scarce resources to improve the privacy environment.** Recognize that effective privacy is a joint construction of regulators and industry. By optimizing the resources of both sides, privacy policies and practices would improve more rapidly and with greater cohesion.
- **Provide guidance and tools.** Leverage industry best practices in formulating guidelines and educational materials and tools, and offer assistance to those seeking to improve their compliance and internal privacy standards.
- **Continue enforcement efforts.** Enforcement efforts are, more than ever, necessary to stem the tide of the minimally compliant and conspicuously non-compliant entities that are undermining efforts to renew the social contract between industry and the public.
- **Identify and respect "no-go zones."** The privacy community should establish some firm limitations on the use and collection of data. For example, higher standards should be afforded to vulnerable groups, including children.

Conclusion

To live and work in the modern world is to accept being part of a super-connected, global community. As in other jurisdictions, Canada faces the challenge of updating or renewing its privacy-related legislation. Our collective privacy challenge is to determine how best to protect the personal privacy of individuals while encouraging organizations to use data to prosper and grow. While Canada's privacy sphere is strong, there are several ways stakeholders can bolster the privacy environment.

CHAPTER 1

Introduction

Chapter Summary

- Canada needs to strike a balance between ensuring personal privacy and enabling organizations to sell and access personalized products and services.
- The Canadian Privacy Summit 2016 was convened to further our collective national understanding of key and emerging privacy issues in Canada.
- The sessions of the two-day summit encompassed two overarching themes: the economics of personal information, and emerging technologies/the Internet of Things (IoT).

Data privacy touches the economy, society, and individuals. There is increasing anxiety around privacy: super-connected systems demand continuous access to citizens and their activities, thus creating continuous privacy challenges.

The emergence of new information and communications technologies (ICTs), such as the IoT, social media services, and big data analytics, have put pressure on privacy frameworks in jurisdictions around the world. Canada needs to strike a balance between ensuring personal privacy and enabling organizations to sell and access personalized products and services. At the same time, we need to be mindful of both present and future threats in a world of rapid change.

To further our collective national understanding of key and emerging privacy issues in Canada, The Conference Board of Canada and the Office of the Information and Privacy Commissioner of British Columbia co-hosted the *Canadian Privacy Summit 2016: Finding Solutions for Canada's Top Privacy Challenges*. The event took place on April 13–14, 2016, in Vancouver, British Columbia. This report summarizes and analyzes the discussions and debates of the participating experts and practitioners at the summit. (The program is included in Appendix B.) Where appropriate, the report supplements the summit findings with relevant examples and research analyses from a review of literature on privacy issues.

This report provides information and insights into stakeholder views on the legislative environment for privacy and data, including the *Personal Information Protection and Electronic Documents Act* (PIPEDA), the *Privacy Act*, and emerging privacy issues. Three key areas of policy research—consent-based privacy protection, protecting anonymity, and transparency—are discussed throughout. The findings will be used to augment previous policy research and potential approaches

The purpose of the summit was to identify the key and emerging privacy issues in Canada.

already under consideration. For example, the Office of the Privacy Commissioner (OPC) of Canada is contemplating the following options[1] to strengthen privacy protection:

- enhancing informed consent through improved ways of explaining information management practices to individuals;
- alternative solutions that limit permissible uses or establish "no-go zones";
- stronger accountability mechanisms for organizations to demonstrate compliance;
- new accountability mechanisms to assess fairness and ethics in the proposed uses of individuals' personal information;
- strengthened regulatory oversight to ensure that solutions are effective.

Other proposed solutions are considered below and presented in the final recommendations.

Purpose, Audience, and Topics

The purpose of the summit was to identify the key and emerging privacy issues in Canada through engaged, open dialogue. In some sessions, participants also debated potential solutions. The event served as a neutral forum for privacy officers in organizations and regulators at the federal and provincial/territorial levels from across Canada to meet and discuss these issues.

An invitation-only event, this two-day summit brought together top experts and key stakeholders from diverse sectors in the Canadian privacy communities to discuss the latest developments and tackle the tough privacy issues facing Canada. Participants shared their experiences and best practices, offering fresh perspectives and innovative solutions to these challenges. Participants included chief

1 Office of the Privacy Commissioner of Canada (OPC), *Consent and Privacy*, 10–11.

privacy officers, chief marketing officers, chief data officers, public sector privacy leaders, Canadian privacy regulators and leaders, and privacy leaders wishing to shape thought leadership.

Summit participants attended the summit to:

- gain a better understanding of privacy policies and their impact;
- learn more about the privacy issues facing organizations across Canada;
- discover strategic approaches and leading-edge thinking around key privacy issues, ultimately helping critical decision-making and reducing risk for the organization;
- gain insight and valuable perspectives from Canadian experts and regulators.

The summit sessions encompassed two overarching themes: the economics of personal information, and emerging technologies/the IoT. Session presentations and discussions covered several topics, including:

- transparency and meaningful consent;
- global trends in accountability;
- online behavioural tracking;
- privacy and surveillance;
- big and smart data analytics for marketing;
- cross-border data flows, accountability, and breach reporting;
- emerging technologies and privacy regulations;
- data-driven innovation, digital disruption, and privacy.

Summit Opening and Stage Setting

The summit opened with a thought-provoking presentation by noted competitive and strategic intelligence expert Estelle Métayer. She shared several key messages that set the stage for subsequent summit discussions, including:[2]

2 Métayer, "The Privacy Conundrum."

Some car insurance companies are tracking customer relationship status on Facebook because the odds of getting in an accident increase after a separation.

- Around the world, customers and the public are giving up privacy for various reasons, such as an exchange for personalized services or products, and simpler interfaces. Accordingly, we must examine our beliefs and opportunities to develop or deny the exponential growth in business models based on advancing technologies. It is prudent, therefore, to examine how private sector and government stakeholders in other countries have tackled the issue and where they are heading to identify best practice models and global trends in privacy and data security.
- Businesses are shifting their models in search of ways to simultaneously capitalize on big data analyses while protecting their own data. The inevitable clash of priorities means that companies, governments, and organizations in all sectors are exploring the economics of personal information (e.g., how to unlock and monetize data; how far the boundaries of privacy can be stretched).
- Regulation of privacy data varies from country to country. Sub-national pieces of legislation offer differing degrees of protection and present diverse approaches (e.g., regarding breach reporting). These differences create challenges for multinational companies seeking to comply with legislation.
- There is a great appetite for trading privacy for convenience in Canada, although there is evidence to suggest that the public has double standards for government and private sector data collection.

Big data is here and companies are already actively leveraging it. Examples of current big data usage in the private sector include:

- Some car insurance companies are tracking customer relationship status on Facebook because the odds of getting in an accident increase after a separation. These insurance companies will then want to charge those customers an added premium.
- Companies are connecting data points through loyalty cards. Your loyalty card knows what you buy and then sells that information to another company, which then gears advertisements accordingly.

- Software that tracks the location of employees is being used to determine who talks with whom, how employees share information within an organization, and which individuals are nodes for activity and knowledge.

Potential Privacy Scenarios for Canada in 2030

Several potential future privacy scenarios for Canada were presented to illustrate the results of different approaches to privacy.[3] The likelihood of a particular scenario becoming dominant is determined by whether consumers will tend to be concerned or complacent and by the role of regulators. Descriptions of the four potential scenarios follow.

Data Lockdown

This potential scenario would be characterized by the following changes and roles:

- The public will be very concerned by multiple breaches, and massive protest demonstrations are likely.
- Governments and regulatory bodies will be setting up certification standards and linking them to the marginal tax rate; creating "SWAT" teams with access to corporate servers to test and validate data usage; and creating a new Minister of Data (or Privacy) in the federal Cabinet, as well as a national ombudsperson for reporting data breaches. They will also play a role in penalizing corporations with heavy fines for data breaches, establishing a digital identity for all citizens and residents, and ensuring that policies are strict and backed by significant budgets for tracking and prosecuting activities.
- Corporations will invest heavily in data encryption technologies. Massive awareness and training programs will emerge, along with new business models that allow consumers to put a price on their privacy. "Comply or explain" will be the norm.

3 Métayer, "The Privacy Conundrum."

The public could take control through violent demonstrations and clashes.

Centurions

This potential scenario would be characterized by the following changes and roles:

- The public will be interested in new technologies, but will look to government to provide guidelines for safeguarding their privacy. Private data safes will be created and blockchain technologies will emerge to store private and citizenship-related data (e.g., health).
- Governments and regulatory bodies will be required to develop effective policies to support the development and implementation of blockchain-like technologies to safeguard private data. Radical transparency will be called for, including the use of e-residency and e-identity cards nationwide. Privacy will be incorporated into the curricula taught in elementary and secondary schools.
- Corporations will have full capacity to monetize data. Institutional shareholders will demand data audit committees in major organizations, and new compliance programs will be developed. The onus will be on corporations to comply and explain how they use data.

Data Chaos

This potential scenario would be characterized by the following changes and roles:

- The public will be very concerned and will take control through violent demonstrations and clashes; citizen-led guerillas; “data neighbourhood” watches; and consumer-driven public, crowdsourced databases that score companies on a trust index.
- Governments and regulatory bodies will fail to protect, be subject to regular hacking/breaches, and will not coordinate efforts. Many different organizations will attempt to assess and develop data compliance programs, but will develop multiple standards in the process.
- Corporations will create new business models where consumers are charged for privacy. A rift will emerge among publicly traded companies due to pressure from shareholders for rapid returns and an increased rate of data monetization. Corporations will locate their data centres in

Private policing firms could emerge to police data and privacy.

other countries. Private policing firms will emerge to police data and privacy (e.g., the "big four" accounting firms[4] will develop a large service portfolio in this area).

Wild West

This potential scenario would be characterized by the following changes and roles:

- Consumers/citizens will trade privacy for convenience, ease of use, and favourable pricing. Generations will clash as millennials and Generation C enter the world of work and become key decision-makers for purchases. Consumers will market their personal data at a price of 50 cents per day.
- Governments and regulatory bodies will provide guidelines, and several commissions will issue reports. They will require corporations to publish corporate data responsibility (CDR) reports, which will have limited success. There will be no enforcement of national rules as geo-barriers fall.
- Four companies will dominate and control the data market: Amazon, Google, Facebook, and Uber. Corporations will consolidate as these "big four" acquire all technology companies related to data management in Canada. Business models will rely on the monetization of data, and data will flow freely between geographic areas. Data hacking cases will increase, and corporations will include the related costs as a single line in their annual reports. Algorithms to predict future behaviour will be hidden from public view.

Report Organization

The remainder of the summit program took the form of panel discussions. Participants' views demonstrated a shared desire to balance the rights of individuals to control their own information with the needs of Canadian companies to innovate and compete. Chapters 2 to 6 summarize the major topics covered at the summit: transparency and

4 Deloitte, PricewaterhouseCoopers, Ernst & Young, and KPMG.

consent; global trends in accountability; online tracking and behavioural advertising; privacy and surveillance/law enforcement, and customer privacy; and perspectives of privacy regulation in Canada. Chapter 7 summarizes the challenges and opportunities of improving policies in three key areas: consent-based privacy protection, protecting anonymity, and transparency.

CHAPTER 2

Transparency and Consent

Chapter Summary

- Computing power and big data analytics pose challenges to traditional modes of establishing individual consent and data uses.
- Both PIPEDA and the *Privacy Act* maintain consent at the core of their conceptions of privacy and privacy protection.
- Private sector data users call for greater guidance and advice on codes of practice for transparency and consent that would help them to comply successfully with regulations.

The Plenary Session 2 panel explored whether the current Canadian legislative model can meet the challenges presented by the data-driven world of today and tomorrow. Panellists discussed the application of concepts such as individual control, consent, transparency, and harm to identify strengths and pain points.

Through the discussion, participants began to outline a way forward that would enable Canadians and Canadian companies to reap the economic and societal benefits related to data use while achieving meaningful privacy. This chapter summarizes the primary discussion of transparency and consent from this session, and discussions from other summit sessions that touched on these issues.

Canada's Privacy Legislation in the Paper Age

Summit attendees questioned the continuing relevance of the current privacy legislation in a world that now operates according to the principles of big data collection and analysis. Participants expressed concern about whether legislation has kept pace with these paradigm shifting technologies. The bulwark of privacy legislation in Canada is the *Privacy Act*, enacted in 1983 to limit the collection and disclosure of personal information by federal departments. This Act and its mission are steeped in the principles of the Canadian Charter of Rights and Freedoms.[1] The Charter is central to modern Canadian values and legal tradition, and is often seen as capstone legislation for the Canadian constitution. The close connection between the *Privacy Act* and the Charter demonstrates that this legislation embodies values that are important to Canada and Canadians.[2]

1 *Privacy Act*.

2 The *Privacy Act* has equivalent legislation in each province.

Information from the public realm that is collected or publicly shared now often falls into a global, universally accessible domain.

Summit participants praised the embodiment of contemporary Canadian values in the *Privacy Act*, and also agreed that these values are widely accepted as relevant today. However, there is widely held concern about the continuing meaningfulness and relevance of technical aspects of the Act in the digital age. Many tenets of the *Privacy Act* were designed for a world in which data collection and dissemination were principally conducted through the medium of paper. Just as paper once defined the rules and practices of data collection, storage, and transmission, silicon chips are now redefining these same rules in the digital age.[3]

The emergence of a new and dominant data medium has a significant impact on privacy. For one, the frequency of information circulation has increased exponentially in ways never anticipated in the paper era when the *Privacy Act* came into force. Information from the public realm that is collected or publicly shared now often falls into a global, universally accessible domain where there are typically few or no practical limits on how long this information can be stored. The radical interconnectivity of the digital age makes it difficult to anticipate where this information will be circulated, among whom, and to what end.

Canada's Privacy Legislation in the Digital Age

The digital age has important implications for consent since the concept of individual consent—for both data collection and personal data use—has been systematically challenged by the exponential increase in data and conceivable uses. Similarly, standardized modes of individual consent and data uses may have been appropriate for the computing power and Internet penetration rates of the paper age, but big data analytics pose a challenge to these standards. For example, raw computing power and immense data sets make it possible for data scientists to infer personal information that was not shared by consent. Increases in technologically enabled options—such as the ability to

3 Basbanes, *On Paper.*

PIPEDA and the *Privacy Act* maintain consent at the core of their conceptions of privacy and privacy protection.

reconstitute pieces of data—and the ability to share data had many attendees questioning the continued relevance of existing legislation and whether it will continue to pass the test of time.

The introduction of PIPEDA in 2000 updated Canada's foundational body of privacy legislation.[4] The newer legislation, with a mandate covering the private sector, sought to modernize the body of law with increased consideration for digital and electronic documentation.[5] Although PIPEDA considers the implications of technological developments up to that point, there continues to be exponential growth in both the complexity and sophistication of technology. Industry and government representatives observe that regulators are struggling to keep up and the current legislation is far from comprehensive. Both PIPEDA and the *Privacy Act* maintain consent at the core of their conceptions of privacy and privacy protection, making discussions about consent central to the Canadian Privacy Summit 2016.

Some summit participants see an over-use and over-reliance on the concept of consent, while others view it as fundamental to the legal tradition and enforcement. It was noted that 4 to 16 per cent of privacy-related complaints received by the OPC identify consent as the main issue. The OPC and other privacy actors recognize the need to closely examine consent, and to make determinations about what this term actually signifies today. Some suggest that informed consent—that can be understood to be meaningful to the user—may be eroding in significance under the barrage of data and consent forms that are characteristic of the information age.

(Re)Constituting Meaningful Consent

One presenter suggested that the Internet exposes the average user to roughly 1,500 privacy policies each year. Without regard for comprehension, it takes an estimated average of 10 minutes to simply

4 *Personal Information Protection and Electronic Documents Act*.

5 PIPEDA also has provincial equivalents in several provinces.

read each agreement. This would require more than 35 working days per person each year, which is unrealistic. The summit attendees do not expect this is happening and concurred that most people give privacy agreements only a cursory overview, at best.

Given the sheer volume of privacy agreements, it is worth asking whether consent achieved through today's standard processes can really be meaningful. If most people are not actually reading these agreements, then what are the chances that consent obtained in this manner will withstand close legal scrutiny? This poses a problem for individual users, but also for companies collecting data—they may find that their legal precautions do not protect them from liability. This could significantly impede prospects for data-based innovation and personal privacy more generally. As a preliminary step, these consent forms could be consolidated so that there is a realistic probability people will read them. Otherwise, expectations must be adjusted surrounding the term "consent" and the legal guarantees it affords.

Several attendees suggested some measure of consolidating similar consent agreements into categories or classes. This would enable users to understand the degree of privacy afforded by a given consent form without having to read every consent form encountered on the Internet. This streamlined system would be more intelligible and meaningful for all users, perhaps restoring the consent model to a certain extent. Before browsing the Internet, people could be asked to indicate the degree of consent they give data collectors, and could also be asked to give further consent as necessary based on the website they visit. This is only one solution, but it demonstrates the degree of reconceptualization that will be necessary to reconstitute consent to something more recognizable to the lens of current legislation.

In Germany, financial institutions consider Facebook profiles when offering credit.

Public Forums, Social Media, and Data Collection Consent

There is an important dichotomy surrounding the willingness to share data and the willingness for that shared data to be used elsewhere. In one noteworthy example, attendees remarked that third parties often use "relationship status" on social media to determine what services to offer. For example, car insurance companies have found that people who have divorced or separated recently are more likely to have a vehicle accident. Using publicly available data collected through social media, these companies have adjusted the rates and coverage policies they offer consumers accordingly.

These practices have wide-reaching and often contested legal implications. On the one hand, it is unlikely that social media users are updating their "relationship status" with an understanding that this information will be used to inform their automotive insurance rates. In this sense, there is a consent deficit because the individual has not consented to the use of their personal information in this manner. This concern was championed by some representatives of regulatory institutions and by activists within the privacy community. On the other hand, since this "relationship status" is being shared willingly, and in a publicly available forum, the argument can be made that consent already exists and is a product of the information being knowingly shared in public. Someone who shouts their relationship status aloud in a park is afforded privacy protection on the same basis; they too are making information publicly available. Participants were ultimately unable completely to resolve this issue or reconcile these two standpoints. This is an important area to create greater unity of opinion with significant implications as governments and private organizations increase their use of data posted to publicly available forums, including social media.

There are ever expanding frontiers for the possible use of publicly available data. Some of these are already being employed in other jurisdictions. In Germany, financial institutions consider Facebook profiles when offering credit, since they have found that those with good social

The respect for individual privacy is based on deep-seated respect for personal autonomy.

standing also tend to pay creditors in a timely fashion. Similarly, the government of China has adopted a method for judging people's "social credit score." This score can then be used to inform employer and social institution recruitment scores, and to direct government investigations. These developments obviously have significant implications for equity, social justice, human rights, and privacy.

Situating Consent

There are many questions about who is ultimately in control of data, which has significant implications for consent. Underpinning the individual consent model is the principle that individuals retain decision-making power over the circulation of their personal data. In law, and in many everyday scenarios, this individualized model of consent continues to remain central and highly relevant. Yet the "possibilities" frontier is quickly expanding and, as a result, new technologies and the power of big data analytics threaten to bypass the individualized consent model.

The Internet has created such high daily volumes of individual data consent requirements that official consent has become almost meaningless in its current form. There are some innovative proposals to restore the significance of the individual consent model, but it is unclear whether they could keep pace with the rate of technological change. This is especially unlikely given the rising penetration of data into everyday affairs through the IoT. It is staggering to consider the volume and complexity of consent agreements that would be required in a world where most home appliances are instantaneously connected to one another and are collecting data in perpetuity.

However impractical an individualized consent model may become, this system remains rooted in important social values and stems from cultural choices about what is important to Canadians. The respect for individual privacy is based on deep-seated respect for personal autonomy, which is itself part of the foundation for liberalism and democracy. This relationship is emphasized in the 1967 book *Privacy and Freedom*—the

seminal work of Dr. Alan Westin and a highly influential text in the privacy community.[6] Thus, a challenge to individualized consent is not to be taken lightly.

Although the demand for individualized consent may be technically difficult to accommodate given trends in data development, there is understandably little room to compromise on the matter of individualized consent because of its significant implications for matters of individual liberty and human rights. The rare suggestions to the contrary raised a great deal of concern among attendees, especially among the more activist members of the privacy community. The importance of the individual was a common starting point in many discussions of how to more specifically interpret policy and enforcement.

Perspectives were difficult to reconcile when it came to the matter of obtaining individual consent for data collection versus the inherent responsibility of data users for their data-sharing practices. For example, some felt that the major burden of responsibility for information posted on social media lies with the individual posters, while others felt that the major responsibility rested with those collecting this data. This was one of the few areas where the attendees made little progress toward a group consensus. It was clear to all involved that there is some degree of shared responsibility in these situations, but it remained unclear to what degree the public posting of data constituted implied consent.

Consent in Data Collection and Use

There was debate among summit participants about whether the best point to obtain consent is in the process of data collection or in the process of data interpretation and use. Again, the consensus was that there is a duty to have some measure of consent in place during both of these processes, but the topic of discussion focused principally on where the major and minor responsibility should rest. For example, people may be willing to share personal information casually with their hairdresser

6 Westin, *Privacy and Freedom*.

(e.g., about family or spending habits) unless or until the hairdresser uses this information for corporate marketing purposes. In this case, consent exists for data collection and for some forms of data use, but with a clear (albeit unspoken) limitation. Were the hairdresser to use information collected from casual conversation for corporate marketing purposes, the most likely outcome would be some form of disapproval of the data's use. This example illustrates that there are social norms and expectations that oppose the idea of implied consent for unlimited uses of data. This forms part of the basis for encoding into law, or some form of jurisprudence, the requirement that consent for data collection alone is insufficient, and consent must also be attained for the data's use.

While this stipulation is important as a matter of principle, there are significant limitations for how this might be interpreted in practice. A commonly raised counterpoint pertains to publicly available data collected by the federal government, such as postal codes and demographic data. It is hard to imagine that individuals have consented to every conceivable use of this data, or that many individuals are even aware of the full range of information collected. To place these kinds of limits on data users without ample nuances, caveats, and exceptions would not only reverse a great deal of precedence but would also not be practical or feasible.

There was ultimately a successful synthesis of these opposing standpoints. Participants generally accepted that extreme interpretations of either position are not meaningful because they reflect neither reality, nor aspiration. They agreed that it is necessary to have some kind of consent for data collection practices, as well as end-use, to interpret whether there has been respect for privacy. Regulatory hard-liners softened their positions, and data users in the private sector began to demand greater guidance and advice on codes of practice that would help them to successfully comply with the spirit of the law within legal grey areas and uncharted waters.

Some surveys indicate that people become more willing to trade their personal data when they know what they can receive in exchange.

Attitudes Toward Privacy

Recent survey data indicate a growing appetite in Canada to trade privacy for convenience. Canada ranks among the top 20 countries with the greatest willingness to compromise on personal privacy by sharing information for the sake of convenience.[7] There is little doubt that consumers desire more access to personalized products and services. That raises the question: To what extent are they willing to trade one for the other? Interestingly, these recent surveys also indicate that significant numbers of Canadians are willing to share personal data, but not for the sake of trade or other forms of direct compensation.

There are some concerns that taking these survey trends at face value, without further qualifications, may impede a balanced interpretation. For one, surveys of this type do not benchmark respondents' awareness of the amount or type of data that is being collected. There is ample evidence to suggest that the average individual has only a rudimentary understanding of the data being collected about them, and does not conceive of the full implications of this data collection. Were survey participants fully informed about the full range of privacy implications of their data sharing, they might be less willing to share data than the survey results indicate.

Some of these surveys also indicate that people become more willing to trade their personal data when they know what they can receive in exchange. The fact that Canadians appear to be relatively reluctant—when compared to those in other peer countries[8]—to trade personal data might suggest that there are significant knowledge deficits among the Canadian public. The implication of this is that surveys that indicate increasing public support for the sharing of personal data may have methodological weaknesses, as suggested by some summit participants.

7 Métayer, "Data."

8 Ibid.

A strong case can also be made that the popularity of data collection practices or privacy measures themselves are inherently insufficient to form law. Further, the values expressed in public opinion surveys are not necessarily going to determine a regulatory outcome. Laws and norms are based on long-term processes that consider a range of opinions and standpoints, not just the majority opinion in the immediate term. Regulations and standards must consider popular views, but without being unduly influenced by them—regulations are about finding a reasonable compromise for all parties.

Privacy Protections for Youth

It is important to note that there are strong generational differences in attitudes toward data privacy. Perhaps unsurprisingly, millennials are significantly less concerned with privacy than are older generations. Millennials have greater expectations that their personal data are being used by others—including the government, data companies, and even their own employers—and are also more likely to trade privacy and personal information for customization of services. This is bound to have a long-term impact on the nature of data and privacy legislation as younger generations age and have a greater impact on political and commercial norms.

Some summit participants suggested that young people are also much less likely to fully appreciate the effect of unqualified data sharing on their long-term future, which may be contributing to their comparative enthusiasm for the practice. This is similar in nature to assertions that survey data present false support for data collection since enthusiasm for data sharing may be underpinned by a relative unawareness of its importance. While this is difficult to confirm, younger generations do risk greater exposure to the negative consequence of data sharing because of their relative inexperience with the world at large and the enduring impacts of data-use violations.

Employers are increasingly using data collection and analytics to improve their business practices, with potentially troubling implications for privacy.

This raised the issue regarding whether these conditions, taken in full, represent a sufficient hazard to merit additional protections for young people. The consensus appeared to be that the relative innocence of youth was sufficient to override the difference in generational values, at least for minors and in accordance with existing standards of protection for minors. Many also felt that this should represent a "no-go zone" although the group was far from reaching a full consensus on this issue. The term "no-go zone," refers to a topic or population that is barred to marketers.

Employee Analytics and Monitoring

Employers are increasingly using data collection and analytics to improve their business practices, with potentially troubling implications for privacy. The most common form of data collection about employees is through publicly available data posted to social media. This occurs often regardless of whether the employees have consented to the practice, or if they are even aware that their personal data are being used to inform management decisions. At a bare minimum, this should be rectified by implementing internal policies that inform employees about the data that are being collected about them, and establishing clear limits on what collection is permitted.

For many companies, coming into compliance with privacy standards will require revision of their existing privacy policies, an increase in transparency that includes notifying staff of the privacy policies, and the disposal of data that were previously collected without clear consent. These should be the first steps toward regaining the trust of employees, many of whom are—perhaps rightly—skeptical of how employers use their personal data.

Beyond compliance, there are concerns about effectiveness and equity stemming from the employment of big data analytics in the workplace. For example, big data analytics have shown a correlation between effective management and travel expenses, with those spending more on travel tending to receive more frequent promotions. Although data

science may prove this relationship, accepting this as fact is unlikely to foster better decision-making. Many of these rules of thumb developed from data science are difficult to verify and are borne of a process that is itself suspect. It is also worth noting that a process that uses existing trends to definitively chart future directions is likely to stifle innovation and progress.

Conclusion

The changes to the privacy environment instigated by the digital age pose a challenge to business as usual, and to the legislation governing privacy. Adapting to the technological possibilities frontier will require careful attention to issues such as consent, social media, collection and use of data, and minimum privacy protections, all within the kaleidoscopic shifting of public attitudes toward privacy. Balancing successful compromise among stakeholders comes with many technocratic difficulties, but as the summit has demonstrated, there is a great deal of common ground to work from and these challenges are far from insurmountable.

CHAPTER 3

Trends in Accountability

Chapter Summary

- What it means to be an accountable organization and how to achieve accountability are evolving concepts.
- Most companies do "baseline" accountability in order to meet their minimum legal obligations.
- Strong principles are not enough—we also need appropriate mechanisms and technocratic prescriptions to ensure meaningful transparency.

The Plenary Session 3 panel explored accountability frameworks, codes of conduct, and cross-border data flows. The concept of "accountability" is not new. Attendees and panel members discussed recent developments in this area, and the potential influence on Canadian law and practices. They also explored how accountability schemes can play a critical role under circumstances in which individual control may not be fully effective.

The intent of this panel was to spark new ideas on how to leverage accountability schemes to achieve both privacy-protective outcomes and data-driven innovation. This chapter summarizes the primary discussion of global and domestic trends in accountability from this session, and discussions from other summit sessions that also touched on these issues.

Legal/Regulatory Compliance

Summit attendees agreed that the definition of accountability has many parts, including the need for compliance. The discussion included mention of the fact that there are more than 100 requirements related to accountability in the British Columbia system alone. These requirements translate to a high volume of detail that needs to be clearly explained in terms of what it means for, and requires of, companies. For many small businesses, the time involved in reading and understanding all required privacy materials is prohibitive and ineffectual. There are very few privacy officers at this level, and many people have never heard of privacy legislation, let alone understand its actual provision or implications.

Attendees also agreed that companies must be prepared to report to regulators on different aspects of their data collection and use practices, even if these were not otherwise tracked for business reasons. Participants felt that companies perform baseline accountability

Some participants expressed a desire for fewer legislative changes in favour of more non-binding guidance for organizations.

to meet their minimum legal obligations (i.e., check marks), but not necessarily to make fundamental improvements. A summit participant estimated that there are perhaps 50 companies in Canada[1] that currently excel in the privacy realm—a miniscule portion of the 1.1 million Canadian businesses.[2]

Some participants expressed a desire for fewer legislative changes in favour of more non-binding guidance for organizations. There is no one series of standards that will act as an ultimate, generally accepted standard. Therefore, the educational value of accountability guidance is high for companies and represents an opportunity for positive change. Improved privacy guidelines and standards will help organizations in a way that new regulatory burdens could not. Further, some attendees cautioned against opening up statutes that have existed for a long time and that were the product of carefully constructed social contracts. They lauded the approach of the current system of guidelines based on a few statutes as this system permits individual firms to create their own pathways for compliance.

One of our strengths in Canada with regard to privacy is that we have a good, responsive system. However, as the power of organizations grows, it becomes increasingly apparent that strong principles are not enough: we also need appropriate mechanisms and technocratic prescriptions. Some delegates suggested that legislative amendments could be used to address the need for mechanisms. Other countries are also considering how to address this need. For example, the European Data Protection Supervisor recently published *Towards a New Digital Ethics*, an opinion paper that explores codes of conduct as well as audits and discusses them as specific mechanisms.[3]

1 The estimate reflected the sense that the best companies in the privacy sphere were all very large corporations. Small- and medium-sized businesses, it was felt, are not of a sufficient size to permit them to scale privacy initiatives to the level of "excellence."

2 Innovation, Science and Economic Development Canada, *SME Research and Statistics*.

3 European Data Protection Supervisor, *Towards a New Digital Ethics*.

We cannot collectively expect, or afford, governments to pour massive amounts of funding into ensuring organizations are accountable.

Breach Reporting

The requirement to report data breaches is an important regulatory tool that helps to establish measures that can be acted upon; it also puts pressure on companies to disclose when breaches have occurred. There was a call among summit participants for organizations to clearly define what constitutes a "data breach." One attendee explained that, by their organization's working definition, they averaged more than 10,000 breaches each year—an example of an uncommon definition of "breach." Reporting is also valuable for understanding how each individual breach happened. In turn, the reporting function and subsequent systematic analysis then helps other companies learn to avoid a similar problem in future (e.g., an issue due to human error, or a system error).

Internal Accountability

Attendees stressed that it is important for organizations to be accountable to the law, rather than merely compliant with their own internal business processes. Some argued to push accountability more into the compliance and legal functions of an organization, while others countered that this approach would effectively turn into an internal baseline standard. Organizations would then be content to do the bare minimum. This field is moving so quickly that locking industry into today's minimum legal standards is a poor choice for long-term success and robust data protection.

We cannot collectively expect, or afford, governments to pour massive amounts of funding into ensuring organizations are accountable. Organizations must therefore consider their options to ensure internal and legal accountability. One suggestion was to use a distributed model of accountability (i.e., champions within different operational areas of an organization). Overall, we should approach privacy protection as an ecosystem that includes all stakeholders, including the board, CEO, managers, staff, and others.

There are considerable entry and exit barriers for customers to switch companies if they do not accept some of the activities regarding data.

Accountability to the board of governors was considered very important but difficult to fully achieve. A time of crisis is not the time to engage board members in discussions about their role versus the role of management in privacy governance. There needs to be a built-in, regular reporting process, which is already in place for many, and clarity concerning roles as well. Management needs to ensure that such a framework is in place and accompanied by readily usable tools. The board, in turn, needs to ensure that it is asking management the right questions to ensure sufficient compliance with appropriate compliance standards.

Incentives

Summit participants were keen to encourage a holistic view of privacy compliance. Taking an aspirational view will lead to ongoing discussions of incentives. Companies need strong incentives, but market imperatives differ greatly across sectors. Incentives should include a higher level, widely relevant motivation for compliance. A good policy program and internal standards incorporate their own incentives. Building trust and reassurance in data subjects, such as survey participants, is one example.

There are incentives for companies to comply or improve their privacy. There are considerable entry and exit barriers for customers to switch companies if they do not accept some of the activities regarding data. The individual cost to change service providers may be much more significant than the consequences of data use. This is not reflected in the legislation, which assumes no real opportunity cost for consumer action.

Microsoft and other leading-edge computer companies have adopted many self-regulating instruments and policies to protect data in the "cloud" and other virtual spaces. Compliance with these standards may be expensive for companies, but it probably costs less than non-compliance (breach risk) or moving to a hard regulatory system.

Conclusion

An examination of our collective privacy goals in Canada, and how we measure up, leads to the realization that we need to increase transparency. The answer to increased accountability is improved transparency and mechanisms for ensuring that this transparency is meaningful.

CHAPTER 4

Online Tracking and Behavioural Advertising

Chapter Summary

- As advertising harnesses the power of big data analytics and "consumer targeting" to increase effectiveness, it is increasingly at risk of violating the individual right to privacy.
- Tailored advertisements—which use big data analytics for determining trends and consumption patterns to predict consumer preferences and future purchases—offer a significant advantage to the firms that employ them.
- Outreach that does not respect the consumer's sense of privacy is considered bad for business.

Online tracking and behavioural advertising are not new concepts. Yet, while there have been established guidelines and industry frameworks for some time, there remains a high degree of variability in how they are applied. Online activities and capabilities are increasingly affecting both individuals and organizations; at the same time, the lines between online and offline activities are not as clear as they once were. Moreover, the Internet continues to facilitate the creation of new markets where products and services are sold in ways that are not always readily understood.

The Plenary Session 4 panel and dialogue explored advertising related practices, their objectives, risks, consumer expectations, and other contextual factors within the current legal framework as well as relevant recent legal cases. This chapter summarizes the discussion of online tracking and behavioural advertising from this session and others that also touched on these issues.

Advertising and Privacy

Advertising is geared to match products to market and individual demands. In theory, advertising helps consumers make informed choices and companies find markets for their products. It should therefore be of mutual benefit to companies and consumers alike, but this idea faces obstacles when it moves from theory into practice. As advertising harnesses the power of big data analytics and "consumer targeting" to increase effectiveness, it is increasingly at risk of violating individuals' right to privacy.

Internet users try to avoid computer hackers and other online criminals with roughly the same intensity as they try to avoid advertisers.

There is significant evidence that people value advertisements that are tailored to their needs and preferences. Although many people view advertisements as a nuisance, well-targeted ads can be helpful to a consumer looking to make a purchase, and do not necessarily evoke a negative reaction. As one attendee said: "A car advertisement that reaches me when I am looking to buy a car is not a problem. The problem occurs six months after I've made my purchase and I am still receiving car advertisements." Some suggested that the underlying problem has little to do with targeted advertising but with ineffective advertising.

There is invariably some truth to this, but few agreed that the challenges facing the advertising industry are limited to ineffectively targeted ads. The irritation of repetitive and redundant advertisements may fall under this description, but the advertising industry's issues go well beyond being a minor annoyance to some users. One study indicated that Internet users try to avoid computer hackers and other online criminals with roughly the same intensity as they try to avoid advertisers.[1] Similarly, most attendees feel that the greatest hazards in the privacy realm are related to data-driven and targeted advertisements.

Tailored Advertising

At first glance, online advertising should not present any undue ethical dilemmas, nor should it generate significant disapproval from consumers. However, big data analytics has profoundly disrupted the advertising industry. By tracking, collecting, and analyzing information about spending and browsing habits, it is possible to infer other personal information that was not explicitly collected, and for which the individual did not provide consent. Tailored advertisements that use big data analytics for determining trends and consumption patterns to predict current consumer preferences and future purchases offer a significant advantage to the firms that employ them.

1 Métayer, "Data."

A prominent example of the ick factor in online and data-driven advertising is the "Target pregnancy scandal."

The individual who owns the personal information that stems from these analyses did not consent to its collection and use, which opens up the potential for privacy violations. The result is shock, and even disgust, as individuals learn about advertisements that are geared to details of their personal lives that they have not shared or consented to share. Attendees referred to this as the "ick factor." It is not surprising, then, that with the advent of big data and data-driven targeted advertising, privacy infringements related to advertising have become one of the most commonly cited privacy concerns.

A prominent example of the ick factor in online and data-driven advertising is the "Target pregnancy scandal." Like most major retailers, Target uses data analytics to tailor coupons and other forms of advertising to customers based on their purchase history. In this example, Target mailed coupons for maternity wear and baby clothes to a high school student. The student's father, outraged that Target was sending advertisements to his daughter that might encourage her to get pregnant at such a young age, complained to Target. Soon after, the daughter informed her father that she was, in fact, already pregnant.[2]

In one sense, these tailored advertisements from Target were successful because they identified an expectant mother and sought to inform her consumer preferences at exactly the right time. However, they constituted a clear violation of privacy by violating the daughter's ability to share news of her pregnancy as she saw fit. Target's ability to know about something as intimate as a pregnancy before immediate family members caused widespread outrage, forcing the company to scale back its tailored advertising program. Target had clearly crossed a line in this case. However, it may not be as clear in future cases where to draw the line between successful advertising and invasion of privacy.

Greater restraint on the part of industry was proposed as part of the solution for reducing the ick factor. One example mentioned involved a clothing tailor who, based on intimate personal knowledge of his clientele, could make clothing recommendations as new fashions or

2 Hill, "How Target Figured Out."

supplies became available. There was little argument that such expert knowledge of client preferences was deeply personal, but it was tolerated in this case because the relationship between the client and the tailor was also personal. Through this lens, new technologies have enabled companies to have personal knowledge in the absence of a personal relationship. From this perspective, the lack of a personal relationship, then, could be the basis for objections, rather than the personal knowledge itself.

One attendee pointed out that regulations and standards of conduct tend to lag behind new inventions. Thus, drinking alcohol while driving was legal immediately after the invention of the automobile, and few people used safety equipment when home power tools first became available. It could be reasonable to expect that the business norms surrounding how to treat the power of targeted advertising are similarly lagging behind the capacity to target and tailor advertisements. This would suggest that the major privacy challenges from targeted advertising lie principally outside the realm of collection and even use—the most important factor for targeted advertising could conceivably be context.

Customer Tracking

Most websites use some form of user/customer tracking methods, either through data collection while customers are browsing the website, or through data collection that continues before and after users visit a particular site. Attendees are of the view that the collection of browsing data is fairly well-known and well-understood by the public, although they also noted that greater awareness of tracking tends to correspond with greater concern about privacy issues. Indeed, a 2016 survey noted that 57 per cent of global citizens and 47 per cent of Canadian citizens are more concerned about online privacy compared with a year ago.[3] These results point to a lack of trust in the customer-tracking practices that industry uses.

3 CIGI-Centre for International Governance Innovation, *2016 CIGI-Ipsos Global Survey*.

Another idea is to modernize consent by creating a streamlined and effective opt-out process to protect consumer privacy better.

In an age of increasingly sophisticated technology, the ability to track potential customers will inevitably increase. One example raised was the development of personalized "bots" on Facebook that follow users as they browse to act as a pseudo-personalized customer service agent. In addition to some likely incidents of the ick factor, this type of tracking and universal personalization of browsing results raises significant red flags. For example, what are the implications for a world where individuals are only exposed to opinions that confirm their pre-existing ideas? How will it be possible to support a robust democracy, or individuality itself, when algorithmic intelligence determines the world as people view it? Questions of these kinds were raised but not resolved.

There were suggestions that consent could be reintroduced for the collection of online browser data. While attendees acknowledged this approach has been used in Europe, they were uncertain whether such a scheme would be an improvement. For example, France has a "cookie policy" that states websites must ask permission to use cookies. The permission granted is then valid for 13 months of browsing. Some of the "fine print" of the European legislation seemed arbitrary to attendees (i.e., Why not 14 months or 7 months?) and there were concerns it would just encourage web service providers to "shop" for new jurisdictions that suit their operational needs. Some thought it might also undermine consumer trust by seeming duplicitous, since many of these policies involve retroactively asking permission to continue an existing practice.

Opting Out

Another idea is to modernize consent by creating a streamlined and effective opt-out process to protect consumer privacy better. With this approach, data would still be collected and analyzed as it is today, but companies would explicitly raise awareness of what data they are collecting and how it is used. At the same time, the process for users to withdraw permission would be simplified. This type of mechanism would more accurately reflect the current reality of industry practice (i.e., data is often collected without meaningful consent), and would improve the privacy environment for consumers.

As a real-world example of a successful opt-out mechanism, attendees discussed a program developed by the industry—"AdChoices." The program causes an icon to appear to customers of businesses registered with AdChoices, which indicates that their data is being collected. It then offers an accessible opt-out mechanism. The program aims to improve awareness of data collection practices, restore trust, and make it easy for those with objections to disengage from the data collection. Such an initiative would also help to streamline the data collection efforts of websites since it can adopt a wider interpretation of consent.

There was some concern among attendees that programs such as AdChoices might represent a de facto recognition of implied consent. Attendees were particularly troubled by the thought that any acceptance of one common measure of implied consent would be a slippery slope to ultimately do away with meaningful data privacy altogether. Industry representatives countered that this was an effective solution, a reasonable compromise, and that existing regulations are already placing an unmanageable burden on industry as it is.

Industry Self-Regulation

Industry representatives commented that some elements of the regulatory environment are awkward and burdensome to the business community, yet they were cautious about proposing any major rollback of regulations. Industry representatives noted that a "Wild West" scenario of data regulation—marked by unbridled competition and the near absence of government intervention—would present obstacles to their business models as well. Continuing relationships with customers depend on trust and the stature of a business brand, both of which can be significantly eroded by advertising that offends customer sensibilities. Attendees situated privacy violations within this context: not just as a human rights concern. In this sense, outreach that does not respect consumer's sense of privacy is considered bad for business.

A healthy respect for privacy can be an effective risk mitigation strategy.

A healthy respect for privacy can be an effective risk mitigation strategy. Just as industry self-regulation plays a role in protecting the public interest, the advertising and data industries understand that they have a stake in curbing the worst excesses of data analytics and privacy violation. In the words of one presenter, "A solution that works for everyone is the best business case." The AdChoices program is a good example of a self-regulating strategy that mitigates risk. Businesses opt-in to AdChoices to be associated with a reliable brand known for respectful use, collection, and analysis of data. Some attendees felt that this is a useful demonstration of industry proposing an effective solution to privacy issues.

Most summit participants felt that, overall, industry had yet to demonstrate the capacity or responsibility to merit the government's trust to fully self-regulate. Both regulators and private sector representatives shared this viewpoint. Some felt there is room for self-regulation, but only when directed by overarching government codes of practice and guidelines. Others suggested that the data and advertising industries would like to raise the standards of behaviour but face a collective action problem that can only be resolved by government involvement. Very few suggested that outright or heavy-handed regulation of the sector would result in the desired improvements.

Selling Your Own Data

Throughout the summit, attendees discussed the exchange of user data for some form of remuneration, thereby facilitating a two-way trade rather than simply data collection. Most often, this trade was discussed as a means to customize goods and services. This can make sense as data analytics inform the development of new products and services that are attuned to consumer preferences better. However, the customization of advertising is one of the larger challenges facing the data and privacy communities, and some attendees understand this to be the result of industry doing a poor job of expressing the benefits it provides to users in exchange for data. As one attendee explained, it is more convenient to search for a piece of information online rather than drive to a library

to look it up. This also represents a huge cost savings for consumers. People are not used to thinking of the benefits of the Internet in relation to the alternative, or viewing data in relation to the cost of free online services.

In some sense, people expect to browse the Internet at no cost even though there was a cost to develop it, and it was largely developed with a business case in mind. That business case depends in large part on the collection of data, and many attendees felt that if users were given the choice to pay for Internet services at cost or share their personal data, they would choose to share their the personal data. Others contested the equivalence in value of data and services, suggesting that the value of the data collected via the Internet are many times greater than the services offered to those who use the Internet.

There is some difference in privacy and data treatment, segmented by income. Higher income users tend to have better data protection, more limited collection of data, and more guarantees that the data will not be used inappropriately. This is mostly because high-income customers are scarce and losing them as customers comes at a high cost for businesses. This represents a troubling reality where, in many cases, the poor are afforded less privacy protection than the rich.

Use of Data by Third Parties

Summit participants expressed concern about the trade of information among third parties. To some, this is a certain next step or even the reality of existing industry practices. Attendees noted that many practices for using and trading data among third parties are already standardized. For example, data analysis (e.g., click-through results) for e-mail marketing campaigns are regularly shared with third parties in an effort to improve future marketing initiatives. In this case, although recipients have not agreed to share their data with third parties—and likely have not agreed to data collection at all—few would suggest that it raises red flags for privacy.

Medical records are one of the priority areas for establishing effective comprehension and guidelines.

The risk to privacy is if an organization takes the idea of consent to third-party sharing to extremes. Although the above example may be a type of violation of privacy law, the major concerns arise with regard to egregious violations. Medical records are one of the priority areas for establishing effective comprehension and guidelines. These records often contain extremely sensitive data with significant implications for privacy, and yet they are used by third parties as part of regular practices for research and treatment. Although standard practices are used to make the data anonymous, this process can often be undone through big data inference. There was a sense that the medical community represents a significant opportunity for improving compliance and developing better standards.

One subject of particular interest to participants was how to treat the collection of data about children. The initial reaction of many was to suggest an outright ban on collecting this type of data, and that underage people should be considered a "no-go zone." Yet, as someone pointed out, demographic data indicating the number of family members, including children, are readily available to marketers and, in fact, necessary to some business practices. It would be difficult, for example, for toy makers to conduct effective advertising if they could not determine who has children and who does not. There is room for nuance and interpretation in this area, and attendees agreed that the issue of third-party use and collection requires greater attention from the policy community.

Conclusion

The advertising industry has inherited a wealth of new capacities and capabilities from the technological revolution. Yet, so far, capability has far outpaced industry norms, consumer values, and government regulation. Many segments of the business community are falling behind, which could negatively affect their competitive standing and customer relationships. There will always be a minority that ignores accepted standards and norms. However, the majority seek to comply. They are struggling to do so with a partially completed regulatory system, in

addition to new data capacities for which the full implications are poorly understood. These factors make guidelines, education, and compliance assistance the best tools for improving industry standards and privacy in Canada.

CHAPTER 5

Privacy and Surveillance

Chapter Summary

- The threat environment today is fast-paced, global, and well-connected.
- While most surveillance work is now conducted online, regulations have yet to fully catch up with this reality.
- Corporations and government organizations must act as good custodians of the information that they collect, regardless of the purpose of the data collection.

Law enforcement of data privacy and national security access to customer information continue to play starring roles in news stories. Following a recent high-profile case in Ontario that suggests businesses have an obligation to stand up for their customers' privacy in the face of government demands, businesses can expect to face pressure from both sides on these important issues. The issues become further complicated when there are multiple jurisdictions and legal imperatives involved.

The Plenary Session 5 panel discussed the ongoing tension between privacy and the public interest associated with law enforcement and national security investigations. This chapter summarizes the primary discussion of privacy and surveillance from this session, as well as discussions from other summit sessions that also touched on these issues.

Law Enforcement Data Responsibilities

In the information age, more and more information about individuals' "data trail" has been made available to law enforcement. However, the privacy sector and the law enforcement field do not always treat privacy issues in a similar way. For example, law enforcement officers may trivialize the importance of privacy considerations for personal information they collect if the information is metadata. In fact, metadata may actually be of greater consequence to an investigation than a recorded conversation, which requires a warrant to obtain. We need to understand the context and perspective of each side in order to make meaningful progress on these issues.

Law enforcement has an obligation to protect citizens and, therefore, a duty to obtain information that can inform criminal prosecutions. However, delegates feel that we need to investigate and define what

Law enforcement often uses licence plate recognition software to help identify stolen cars. However, law enforcement also collects an enormous amount of personal data based on all licence plates.

"minimal intrusion" means. Secondly, there was a call for improvement in how we determine the minimum amount of information required. For example, law enforcement often uses licence plate recognition software to help identify stolen cars. However, law enforcement also collects an enormous amount of personal data based on all licence plates. Unintended consequences can result, such as an individual being denied the ability to cross a border because of a prior mental health concern. Events such as these begin to brush up against the protections afforded by human rights.

Attendees posed a key question: Should there be some restraint or control on the requests from police, especially concerning the collection of data on individuals not concerned in an investigation? If so, how should those limits be set? For example, when should data be destroyed? In one case known as the "tower dump" case, the judge "set out guidelines in his ruling for how police and courts should handle requests for such orders to minimize the intrusion on personal privacy."[1] Attendees highlighted aspects of the guidelines such as the need to justify the reason, the length of time for which data is requested, why the records are relevant, and what efforts are being made to minimize the amount of data requested. Such detailed guidance emphasizes the fact that both the public and private sectors must act responsibly as custodians of information (e.g., health, education, or employment details).

There are information imbalances for stakeholders in the security community that must also be taken into account. This may be especially significant for judicial system stakeholders, who often have only a minimal awareness of both security and/or privacy concerns when they are asked to issue warrants and other legal decisions. This can cause significant slowdowns during time-sensitive investigations, thereby reducing the effectiveness of police and security forces. It can also have a negative impact on privacy when these decisions do not reflect

1 Dobby, "Ontario Court Rules."

a full appreciation of their potential implications. This area presents a significant and immediate opportunity for engagement and education from the privacy community.

The threat environment has never been as accelerated and complicated as it is today.

Protection and Security

The threat environment has never been as accelerated and complicated as it is today. Not only is it fast-paced, it is also global and well-connected. Technology and capability, and even societal norms, are evolving much faster than policy and regulations. The 9/11-related mantra in law enforcement, particularly in the United States, is "never again, never again." As a result, in recent years there has been a significant increase in the techno-prowess of law enforcement. Most surveillance work, for example, is now conducted online. Regulations have yet to fully catch up with this reality.

During the RCMP investigation known as Project Clemenza, it became apparent that the RCMP had access to a large volume of encrypted e-mails via access to BlackBerry's global encryption key. This case raised questions about how to regulate encryption. Information threats are now much more advanced. Attendees stressed the need to find a proper balance between protecting individual privacy and protecting the public by preventing terrorist acts and other traumatic events. Law enforcement agencies are closely focused on the task at hand. Attendees pointed out that law enforcement officers will take privacy protection as close to the line as possible in order to do their job (i.e., protect).

There are now privacy inconsistencies: whereas law enforcement officers can research a licence plate number very quickly, they need a judge's approval to obtain an IP address. The public's expectation is that law enforcement will stop all external or internal threats to public safety while maintaining full privacy. It is possible to avoid legal questions and offending individual's sensibilities, but it may have life-threatening consequences.

Many companies now require a court order before they agree to share any customer information.

Organizational Reactions to Data Requests

Government requests for data can create a privacy dilemma for organizations. In response to the millions of data requests that telecommunications companies receive from government departments each year, many have started to publish transparency reports as a proactive way to address privacy concerns. Delegates highlighted some federal government reporting guidelines that offer ways to unify the standards of such transparency reports, but felt more discussion was necessary to verify whether the guidelines were effective and ideal.

Companies develop their own transparency reports to bolster customer trust. Such reports also enable companies to inform the public about the high volume of requests for information that they receive from government and law enforcement. Transparency reports are a means of communicating to customers and shareholders that the company has heard and acted on the demand for greater sensitivity and transparency.

In extreme cases, organizations that do not comply with data requests end up in court. One key reason for non-compliance is the organization's obligation to protect the privacy of its customers. An example is the recent "tower dump" case in which Rogers Communications Inc. and Telus Corp. refused to comply with police orders to provide the personal information of about 40,000 cellphone users.[2] The court subsequently deemed the order to be a breach of the Canadian Charter of Rights and Freedoms.[3] This case demonstrates that organizations have discretion when making disclosure decisions, even to police requests.

Many companies now require a court order before they agree to share any customer information. In this way, they are acting as custodians of information since their customers normally have no sense that their information is being requested or how often. At the same time, they try to establish good working relationships with law enforcement

2 Ibid.

3 Ibid.

agencies to balance the flow of information. Due to increasing corporate requirements for a warrant, law enforcement requests are becoming more defined and narrow in scope.

Conclusion

Privacy and surveillance issues go beyond questions of private sector disclosure. Both corporations and government organizations must act as good custodians of the information they collect. From an operational standpoint, new guidelines for discretionary cooperation with law enforcement would help organizations have a better understanding of their options and provide more structure for the processes involved in responding to data requests.

CHAPTER 6

Perspectives on Privacy Regulation in Canada

Chapter Summary

- Privacy regulation tends to be fairly strong in developed countries and comparatively weak in developing countries.
- High-quality cooperation between industry and government, and good governance are more significant than the law itself.
- Some of the greatest successes of regulators and regulatory offices have been in education, awareness, and assisting with voluntary compliance.

The Plenary Session 6 panel was an animated discussion that looked at privacy regulation in Canada through various lenses. This session took place near the end of the summit, enabling participants to candidly discuss how privacy regulations measured up, as well as what they should look like in the future for a better Canada.

This chapter summarizes the primary discussion of privacy regulation from this session, as well as discussions from other sessions that touched on related issues.

Global Comparisons

Participants noted that privacy regulation tends to be fairly strong in developed countries and comparatively weak in developing countries. Canadian regulatory standards are at about the mid-point between Europe and the United States. Attendees felt that Canadian regulations are not as heavy-handed as in Europe, nor as lax and pro-business as regulations in the United States.

There was ample speculation about the direction of U.S. and European legislation. One area of broad consensus is that the full pursuit of either extreme of legislative philosophy in the Canadian context would be a mistake. There were concerns about the long-term impacts of European legislation, and whether it might stifle both the data industry and the downstream benefits that come with it. In terms of market capitalization, Europe represents only 2 per cent of the digital industry, while the United States represents 83 per cent.[1] In the immediate term, summit participants suggested that European data companies might leave jurisdictions that have punitively harsh regulations.

1 Derder, *Le Prochain Google*.

The status of Canada's framework and body of privacy law, relative to its peers, was one of the most hotly contested issues of the privacy summit.

The extreme monetization of data in the United States and data considerations also have implications of concern. With the present direction, it is possible to see a world where data privacy comes with a user surcharge, and there is a gradual and substantial erosion of the personal space that democratic systems afford. There are already concerns about the emergence of a multi-tiered system of privacy protection, where high-end customers are afforded better protections than others.

Canada does not yet fall into either extreme. Immediately following the keynote address, there was a vigorous discussion about where privacy regulations in Canada fit compared with peer countries. There was no consensus, with equal numbers of attendees portraying the regulatory environment as either a "Wild West" that permits everything regardless of its social utility or a "lock down" environment that permits nothing at the expense of progress. The status of Canada's framework and body of privacy law, relative to its peers, was one of the most hotly contested issues of the privacy summit, with little progress made toward a common understanding.

Another issue that drew frequent attention is the age of Canadian legislation and the continued relevance of regulations developed for a world in which paper was the principle medium of record. A relevant comparison could be the *Access to Information Act,*[2] which was adopted the same year as the *Privacy Act* and formed part of the same legislative thrust. International comparisons rank the quality of access to information legislation based on how well it is attuned to present-day digital realities. Canada fares poorly in international comparisons, currently ranking only 44th globally.[3] A key reason identified for Canada's poor ranking is its out-of-touch legislation. These results also support the case for regulatory renewal in Canada.[4]

2 *Access to Information Act*.

3 Centre for Law and Democracy, Global Right to Information Rating.

4 Centre for Law and Democracy, *Canada*.

There was considerable debate about whether Canadian privacy legislation needs to be updated. Most attendees expressed a desire to see an enhanced privacy regime in one way or another. However, there was little agreement regarding whether the legislation needs to be updated, repealed, or supplemented, or whether it is sufficient but open to different interpretations. In fact, much of the discussion focused on enforcement and jurisprudence of existing regulations, rather than a complete legislative overhaul. Canada's low rankings for access to information stem largely from the emphasis of rankings on the text of the legislation, rather than on the body of precedence or the ability of this legislation to be enforced. In this sense, international comparators disregard the fact that the legislation itself is only one part of the regulatory regime.

Too Much Regulation or Too Little?

Attendees look to standards from other countries to inform Canada's relative success or failure. Regulators tend to view the body of law in Europe, and the general thrust toward higher regulatory standards, as worthy of emulation in the Canadian system. The idea of privacy as a human right is at the root of a lot of European legislation, which places the burden of compliance on businesses. In other words, the expectation is that businesses must rise to the occasion and demonstrate compliance with regulations to be able to use and collect data. By contrast, industry representatives tend to support a more American model, which provides citizens with a baseline of privacy protections and the ability to contest data collection and use practices that negatively affect them.

Both systems have their advantages and disadvantages, and there was a general recognition that there is no ideal type or perfect example. Some felt that the Canadian privacy environment has struck a good balance between the European and American models, with one speaker claiming the Canadian body of law pertaining to privacy is "the best in the world." This perspective is rooted in the idea that regulators, legislators, and privacy officers can only be expected to "work with the hand they have

Regulators have the tendency to view additional regulations as a solution.

been dealt." In other words, high quality cooperation between industry and government and good governance in the privacy realm overall are much more significant than the letter of the law itself.

This idea runs up against the suggestion that regulators need more power and more regulations to govern the privacy realm effectively. Regulators have the tendency to view additional regulations as a solution, overlooking the successes that have been achieved in the space that exists between law and the free licence to act. In fact, some of the greatest successes of regulators and regulatory offices have been in education, awareness, and assisting with voluntary compliance. Many attendees from industry expressed very positive views about the value of these efforts and think there should be more outreach of this kind.

Regulators had mixed reactions to this message. On the one hand, there was welcome praise for the execution of their mandate to promote awareness, education, and compliance assistance. However, these activities tend to have limited staff and resources, which sometimes forces trade-offs concerning what elements of their mandate they are able to execute effectively and with full capacity. In the absence of renewed regulations, privacy commissioners and their offices spend much of their time pursuing legal activism through the judicial system, which is time-consuming. Although this is effective at improving the body of law, it often takes away from their ability to conduct outreach, education, and compliance assistance, thereby making the issue of privacy less accessible to the average Canadian.

Privacy and the Data Industry

In the search for effective policies to govern the data industry, there was some discussion of what might constitute a comparable industry to serve as an effective starting point for policy development. One suggestion was that since data is "mined" and somewhat comparable to a natural resource, we should treat data companies with the same standards as mining companies. Of course, unlike industries such as mining, data analytics are highly globalized operations with little dependence on

Data analytics are highly globalized operations with little dependence on geography.

geography. In addition, data mining and analytics companies have very little capital, almost none of which is fixed. The fixed assets that do exist, such as servers, are less and less likely to be located in the same place as the company's operations and staff since it is easy to shop for an ideal location to house servers elsewhere.

All these factors combine to impose strong limitations on policy options. If Canada were, for example, to clamp down heavily on privacy violations in a way that was especially burdensome to industry, then the affected companies could move their operations elsewhere with relative ease. This is particularly relevant to Canada since its neighbouring jurisdiction, the United States, already holds to a lower standard of data protection than Canada, making this move a very real risk. This exerts a downward pressure on regulatory standards since any radical departure from current norms could cause a flight of the industry. The point is far from academic. The 2001 adoption of the *PATRIOT Act* [5] in the United States led many data industries to relocate to Canada; there is little to suggest that a comparable shock to Canada's regulatory framework would yield a different result.

5 *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001*.

CHAPTER 7

Opportunities for the Future of Privacy in Canada

Chapter Summary

- The governance foundations for privacy in Canada are resilient and a point of strength for policy-making and for the legislative development process.
- Consent-based privacy protection, protecting anonymity, and transparency are each essential to the foundation of privacy laws, regulations, and practices.
- Advances in technology and data science are increasingly threatening our security and personal privacy.
- Summit discussions offered a number of opportunities to develop practical approaches to potential privacy reforms.

While Canada's privacy sphere is strong, there are a variety of future pathways that could be taken to bolster our privacy environment. Participants at the inaugural Canadian Privacy Summit generally felt that our country's core privacy legislation and regulations are sound, but could be improved with some modifications. Overall, they reached a consensus that reforms in both the public and private sectors are necessary to address the growing concerns associated with technological advances and global sharing capabilities.

The dialogue at the summit was promising and demonstrated that the governance mechanisms of the privacy community are vibrant and improving. Discussions were respectful, constructive, and made meaningful progress toward an invigorated privacy regimen. Agreement about specific legislative reform proposals was more limited. The governance foundations for privacy in Canada are resilient and a point of strength for policy-making and the legislative development process.

In terms of legislative proposals, opinions varied on whether legislative changes would produce the intended results. There was a wide consensus that existing legislation on privacy is out of date. However, there was also agreement that the privacy community itself was doing something right, and there was hesitancy to "throw the baby out with the bathwater." Some attendees were concerned that revisiting the legislation might jeopardize hard-won principles of privacy law, such as provisions that protect privacy as a human right, and consent as a mechanism for protection.

From another perspective, summit participants were concerned that opening up the body of legislation to revisions might yield improvements but could also lead to over-regulation. Aside from the regulators themselves, few attendees viewed a greater regulatory burden as a

While the consent model is leaning against the wind of technological capabilities, it may also be acting as a defence against the erosion of liberalism.

means to improvement. This stems partly from their sense of the added uncertainty that would come with opening up this conversation and from a recognition that there are some major successes with the governance regime that is operating in the legal penumbra.

Appetite for regulatory change stems from an understanding of the clear inadequacies of the body of privacy law. Any changes to the body of law itself must be careful to respect the norms, conventions, and practices of the privacy community in Canada so that future regulatory changes do not disrupt the delicate harmony that exists. That includes diligent consideration for values enshrined in law, as well as respect for the existing state of affairs and vision for the future of privacy and data in Canada.

Consent-Based Privacy Protection

Consent to the use and collection of personal data remains central to privacy legislation in Canada, and is a core principle of privacy more generally. Yet, advances in technology and data science have created technical possibilities that are pushing up against this concept and threaten to circumvent its relevance. The existing body of law does not adequately reflect this fact, nor do the laws themselves embody an appreciation for the current state of data science and technology, much less future possibilities.

Although the consent model reflects an age when the transmission of information occurred mainly by paper, it also demonstrates core democratic and liberal values that are central to Canada's political community. While the consent model is leaning against the wind of technological capabilities, there is widespread awareness that it may also be acting as a defence against the erosion of liberalism. From this perspective, any effort to move past the consent model is potentially an invitation to moral catastrophe. In some ways, this situation recalls attempts to reform the *Indian Act*. Many of those advocating against reform nonetheless found the dated provisions in the Act in great need of

change. In spite of this, they staunchly opposed reform out of a concern that particular protections may be gone forever by opening the Act up for discussion.

Any attempt at legislative reform needs to be conscious of this perspective on consent and that values are at the heart of the privacy community. Although many support legislative modernization, there are increasing concerns that technical considerations may trump the philosophical imperatives behind the privacy movement. However impractical individual consent for data collection may be, the individualism at the core of this model cannot be disputed and is something that many highly value.

Some innovative solutions have the potential to resolve this deadlock and improve privacy protections while upholding the principle of individual consent. These include bundling consent forms to streamline browsing, heightened notifications of data collection practices, greater ease of opt-out, and more mature industry norms on data collection and use. Although none of these solutions may be perfect from a hardline perspective, they could be leveraged to improve the status quo, where meaningful individual consent is rare and full compliance is often ceremonial.

In this sense, moving forward on privacy will require making a compromise on principle for the sake of improving practice. In a world where dozens of consent forms may be required during a single day of Internet browsing, consent has to be reconceptualized if it is to remain meaningful. This may not satisfy all involved, but a compromise is necessary if the principle of consent is to remain relevant in law and respected by users.

Protecting Anonymity

Anonymity has proven a difficult concept to justify since it is often associated in the public consciousness with crime and terrorism rather than independence and the right to privacy. Indeed, most anonymous browsing is, perhaps accurately, associated with the “Dark Net.” (The

Big data has made it easy to deconstruct the measures of online privacy that are afforded to the average user.

"Dark Net" is part of the "Deep Web" of content that is not accessible through search engines, and where users can browse and connect in full anonymity. It is often associated with criminal and illegal uses of the Internet.) Widespread acceptance of anonymity requires a rebranding and a public awareness push if it is to remain relevant to the average citizen. This is due in part to a lack of general awareness about how truly anonymous casual Internet browsing is, and how much can be deciphered about a person through their online presence.

From a capacity standpoint, big data has made it easy to deconstruct the measures of online privacy that are afforded to the average user. It has become easy to infer personal information through the collection of information that was voluntarily shared. This presents a difficult dilemma: How can the full capacity of data analytics be used without crossing moral or legal lines? A balance must be struck that guarantees individual privacy and anonymity without being overly restrictive to industry or detrimental to human progress.

Several potential solutions emerged from the summit discussions, all of which have come from industry practice. These approaches seek to minimize organizational exposure to risk and avoid legislative enforcement. One proposal was to silo data so as to limit the ability of organizations to infer private information from unrelated data sets. This approach would still permit the use of the data for purposes for which consent exists. A more radical suggestion from the open source community (e.g., Wikipedia) is not to collect or store any data of those who browse particular websites. In fact, this too is a risk-aversion strategy.

In most cases, there is no need for measures as extreme as that employed by Wikipedia, but its example highlights an important point—companies should not collect data for its own sake. There need to be limits on how long data can be stored, and how it may be circulated among third parties. This will go a long way to deter the over-collection of data, which in turn can help to stem privacy violations by way of

inference. Although some industry leaders have championed these solutions, there seems to be little to suggest that these standards will be widely adopted organically.

A 2014 decision by the Court of Justice of the European Union—commonly called the *Right to Be Forgotten*—established a precedent for the legal right to request that personal data be destroyed by search engines. This was a landmark limitation on data use and collection. Although there are many limitations to this "right," this case represents a legal precedent that has not gone unnoticed by the privacy community. While the body of law is far from granting a universal right to have the personal data that third parties collect destroyed upon request (as it is sometimes popularly interpreted), this nonetheless represents an interesting development for data collection and aggregation.[1]

It is also important to recall that the governance space is responsible for the development of many solutions related to anonymity, and industry can be willingly consulted for solutions and feedback. From the same imperative for risk aversion and continuous improvement, many within industry are enthusiastic to meet and exceed the voluntary best practices championed by regulators. Many think it is good business practice, and not merely a way to limit liability. It is a proven method to improve customer relationships and safeguard their brand.

Transparency

The issue of transparency splits into two issues: private sector transparency and public sector transparency. Many participants feel it is inappropriate to lump the two sectors together because they have significant differences in mandate. The private sector uses data to inform products and services, while public sector uses include security, law enforcement, and counter-terrorism. At the same time, both sectors aim to improve public trust, albeit to different ends.

1 European Commission, *Factsheet on the "Right to Be Forgotten" Ruling*.

In the post-9/11 security environment, data collection and analyses by the security services has increased dramatically.

An overarching concern among attendees was there may be too much reliance on transparency as a policy measure and as a panacea for other problems—an issue that was raised about the use of transparency as a policy tool more generally.[2] It is certainly important for actors in the privacy sphere to be transparent with their stakeholders and provide as much useful information as possible to interested parties. However, information sharing is not a substitute for good data practices, and excessive transparency can even undermine efforts to cultivate greater public trust.

This important qualification limits the effectiveness of transparency as a tool for enforcing legislation in the private sector, at least in a prescriptive and highly technical manner. To be sure, private organizations should be encouraged to be transparent. However, the diversity of business models undermines the effectiveness of a one-size-fits-all model mandated by legislation. The guidelines in circulation have proven helpful to that end, with many of the larger organizations using these guidelines as a springboard to even higher standards of transparency than those demanded by the regulatory community.

The state possesses a special prerogative when it comes to data collection and use. The question of public sector transparency tends to revolve around data collection and retention by the security apparatus. In the post-9/11 security environment, data collection and analyses by the security services has increased dramatically, which merits increased transparency on the part of the state. However, data use by law enforcement is covered by a legal patchwork, and many of the existing legal requirements that pre-date the world of big data are not suited to present-day realities. Similar observations can be made about transparency requirements that could use a reboot to become more reflective of current practices.

2 Best, *The Limits of Transparency*.

Opportunities

Optimize Scarce Resources to Improve the Privacy Environment

The summit raised the issue of how to treat those caught in violation of privacy norms and laws, in addition to simple punitive measures and direct prescriptions from law. As a case in point, Bell's attempt at personalized advertising—its Relevant Advertising Program[3]—was often cited as an example of what not to do. However, in the fallout of privacy violation, Bell has raised the bar and made every effort to become a leader in the privacy realm. At some point, the privacy community must recognize Bell and companies such as Bell for their present successes, rather than their past failures. This is part of a larger imperative to look beyond the letter of the law and to see effective privacy as a joint construction of regulators and industry. By optimizing the resources of both sides, privacy policies and practices will improve more rapidly and with greater cohesion.

Provide Guidance and Tools

A one-size-fits-all model imposed in a top-down fashion is not a very effective way to improve the privacy environment and optimize existing expertise. While industry needs—and in some cases demands—regulations in specific subject areas, the creative energies of industry should be enlisted in efforts to build a better privacy system. This involves using industry best practices to formulate guidelines and educational materials, such as tools, as well as offering assistance to those seeking to improve their compliance and internal privacy standards. In many cases, private actors want to comply with standards and norms but have difficulty achieving this, or even knowing when they are compliant. An ounce of prevention is worth a pound of cure,

3 Office of the Privacy Commissioner of Canada, *Results of Commissioner Initiated Investigation*.

More than ever, continued enforcement efforts are necessary to stem those who cross the line.

and members of the regulatory community should ensure that they act as resources for those seeking compliance, in addition to their role as guardians of the law.

Continue Enforcement Efforts

Industry members feel that many of the worst offenders are damaging the brand of reputable companies and eroding trust in the industry as a whole. There are pressures for those in the data industry, especially in advertising, to meet and exceed rising standards in order to improve and gain consumer trust. Yet, the few companies with regular business practices that violate industry norms and standards can undermine this groundswell. The challenge centres on the minimally compliant or conspicuously non-compliant firms that are undermining efforts to renew the social contract between industry and the public. These firms cause harm to the privacy community, erode the public trust in industry and government alike, and undercut the compliance efforts of legitimate businesses. More than ever, continued enforcement efforts are necessary to stem those who cross the line.

Identify and Respect "No Go" Zones

As with other efforts at regulation, the privacy community should establish firm limitations on the use and collection of data. Where these lines should be drawn was a matter of some disagreement at the summit, but there was agreement that limitations should be placed on the data that can be collected about children. Of course, a total limitation on data collection about children would present a problem to those companies looking to develop products and advertisements for parents. But the point remains that some higher standard should be afforded to vulnerable groups, including children.

Conclusion

To live and work in the modern world is to accept being part of a super-connected, global community. Our collective privacy challenge is to determine how best to protect individuals' personal privacy while encouraging organizations to use data to prosper and grow. As in other jurisdictions, Canada faces the challenge of updating or renewing its privacy-related legislation.

This paper has summarized the discussions of privacy experts, including regulators and private sector privacy officers, from the inaugural Canadian Privacy Summit 2016. It presents the various perspectives of participants to provide information on key and emerging privacy issues in Canada. Consent-based privacy protection, protecting anonymity, and transparency are each, in their own way, essential to the foundation of privacy laws, regulations, and practices. The opportunities presented above address these critical elements and offer practical approaches to potential privacy reforms that will balance private and public interest to safeguard individuals' privacy. They will also facilitate public trust in government and enable business to use data for commercial purposes: factors that are so important to Canadians' quality of life and Canada's competitiveness in the global information age.

APPENDIX A

Bibliography

Access to Information Act. R.S.1985, c. A-1.

Basbanes, Nicholas. *On Paper: The Everything of Its Two-Thousand-Year History.* New York: Vintage, 2014.

Best, Jacqueline. *The Limits of Transparency.* Ithaca: Cornel University Press, 2005.

Centre for Law and Democracy. *Canada*. http://www.rti-rating.org/view_country/?country_name=Canada (accessed May 30th, 2016).

—. *Global Right to Information Rating*. http://www.rti-rating.org/country-data/ (accessed May 30, 2016).

CIGI-Centre for International Governance Innovation. *2016 CIGI-Ipsos Global Survey on Internet Security and Trust*. www.cigionline.org/internet-survey-2016 (accessed May 25, 2016).

Derder, Fathi. *Le Prochain Google Sera Suisse.* Geneva: Slatkine, 2015.

Dobby, Christine. "Ontario Court Rules Police Orders Breached Cellphone Users' Charter Rights." *The Globe and Mail*, January 14, 2016.

European Commission. *Factsheet on the "Right to Be Forgotten" Ruling*. European Commission: Brussels, 2014.

European Data Protection Supervisor. *Towards a New Digital Ethics.* European Data Protection Supervisor: Brussels, 2015. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-09-11_Data_Ethics_EN.pdf (accessed May 18, 2016).

Hill, Kashmir. "How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did." *Forbes*, February 16, 2012.

Innovation, Science and Economic Development Canada. *SME Research and Statistics.* www.ic.gc.ca/eic/site/061.nsf/eng/02804.html (accessed May 30, 2016).

Métayer, Estelle. "Data." *Canadian Privacy Summit 2016: Finding Solutions for Canada's Top Privacy Challenges*. Held at Vancouver, British Columbia, April 13–14, 2016.

—. "The Privacy Conundrum." *Canadian Privacy Summit 2016: Finding Solutions for Canada's Top Privacy Challenges*. Held at Vancouver, British Columbia, April 13–14, 2016.

Office of the Privacy Commissioner of Canada (OPC), Policy and Research Group. *Consent and Privacy*. Gatineau: OPC, 2016.

—. *Results of Commissioner Initiated Investigation Into Bell's Relevant Ads Program*. www.priv.gc.ca/cf-dc/2015/2015_001_0407_e.asp (accessed May 31, 2016).

Personal Information Protection and Electronic Documents Act. S.C. 2000, c. 5. http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html (accessed May 17, 2016).

Privacy Act. R.S.C. 1985, c. P-21. http://laws-lois.justice.gc.ca/eng/acts/p-21/page-1.html (accessed May 16, 2016).

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001. Public Law 107-56-Oct 26, 2001.

Westin, Alan. *Privacy and Freedom*. London: The Bodley Head, 1970.

APPENDIX B

Complete Summit Program and Session Descriptions

Canadian Privacy Summit 2016: Finding Solutions for Canada's Top Privacy Challenges

April 13–14, 2016

Morris Wosk Centre for Dialogue, Vancouver, British Columbia

Day 1—Wednesday, April 13, 2016

8:00 a.m.—**Registration and Continental Breakfast**

8:30 a.m.—**Welcoming Remarks From the Co-Chairs**

Andrew Pender, Associate Director, Executive Networks,
The Conference Board of Canada

Elizabeth Denham, Information and Privacy Commissioner, Office of the Information and Privacy Commissioner for British Columbia

9:00 a.m.—**Plenary Session 1**

Keynote Presentation: The Privacy Conundrum
Estelle Métayer, Founder and Principal, Competia

Everywhere, customers and the public are happily, or grudgingly, giving up privacy in exchange for personalized services or products, and simpler interfaces. The inability to control this urge is fast "fracking" our deepest beliefs and institutions as far as data privacy is concerned.

This important summit examined how countries, and private sector and government stakeholders, in various regions of the world have tackled the issue and where they are heading. Is there a best practice model out there? Is the global thinking converging, or will we see a quasi-feudal privacy landscape in the future? Where will the next threats on data security come from?

With the shift of so many business models and the high stakes at play (the growth and survival of our companies depends both on their ability to tag along with the data disruption, and to protect their data), the clash is inevitable. Since few industries will remain undisturbed in the "uberization" tsunami, the summit further explored how companies, governments, and organizations are unlocking data, how far they are willing to stretch the boundaries of privacy, and what to expect from the future monetization models of data and the upcoming economics of personal information.

The summit also investigated why we are heading for a generational schism in our acceptance of the use of personal data, and a shifting definition of privacy.

10:00 a.m.—**Networking and Refreshment Break**

10:30 a.m.—**Plenary Session 2**

Transparency and Consent
Session Chair:
Amanda Maltby, *General Manager, Compliance and Chief Privacy Officer, Canada Post Corporation*

Panellists:
Abubakar Khan, Director, Toronto Regional Operations, Office of the Privacy Commissioner of Canada

Adam Kardash, Partner and Practice Leader of the National Privacy Group, Osler, Hoskin & Harcourt LLP

Pippa Lawson, Consultant, Philippa Lawson, Barrister & Solicitor

Della Shea, Vice-President, Data Governance and Chief Privacy Officer, Symcor Inc.

The panel explored whether the current Canadian legislative model can meet the challenges presented by the data-driven world of today and tomorrow. Panellists discussed the application of concepts such as individual control, consent, transparency, and harm, with a view to identify strengths and pain points and begin to outline a way forward to allow Canadians and Canadian companies to reap the economic and societal benefits related to data use while achieving meaningful privacy.

11:45 a.m.—**Networking Luncheon**

1:00 p.m. —**Plenary Session 3**

Global Trends in Accountability
Session Chair:
Elizabeth Denham, Information and Privacy Commissioner for British Columbia

Panellists:
Anick Fortin-Cousens, Chief Privacy Officer, Canada, Latin America, Middle East & Africa, and Program Director, Corporate Privacy Office, IBM Canada Ltd.

Pamela Snively, Chief Data and Trust Officer, TELUS Communications Inc.

Jennifer Stoddart, Regulator Advisor, Nymity Inc.

Accountability frameworks, codes of conduct, and cross-border data flows are just some of the global trends in accountability. The concept of "accountability" is not new. However, the expectations around what it means to be an accountable organization, and how one achieves accountability, continue to evolve. This panel discussed recent international developments on this issue, and how they may influence Canadian law and practices. It also discussed how accountability schemes can play a critical role where individual control may not be fully effective. The intent of this panel was to spark ideas as to how accountability schemes can be leveraged to achieve both privacy-protective outcomes and data-driven innovation.

2:15 p.m.—**Networking and Refreshment Break**

2:30 p.m.—**Interactive Sessions—Set A**

Interactive Session A1
Big Data Use Case #1: Data as a Business
Moderators:
Stephanie Rich, Assistant General Counsel, Privacy and Ethics Officer, Aimia Canada Inc.

Benjamin J. Goold, Professor, The University of British Columbia

Interactive Session A2
Big Data Use Case #2: Employee Analytics and Employee Monitoring
Moderators:
Drew McArthur, Principal and Founder, The McArthur Consulting Group

Michael McEvoy, Deputy Commissioner, Office of the Information and Privacy Commissioner for British Columbia

3:45 p.m.—**Breakout Report-Back**

4:15 p.m.—**Plenary Session 4**

Online Tracking and Behavioural Advertising
Session Chair:
Dr. Éloïse Gratton, Partner and National Co-Leader, Privacy and Data Security, Borden Ladner Gervais LLP

Panellists:
Colin McKay, Head of Public Policy and Government Relations, Google

Wally Hill, Senior Vice-President, Public Affairs & Communications, Canadian Marketing Association

Tamir Israel, Staff Counsel, Canadian Internet Policy and Public Interest Clinic (CIPPIC)

Patricia Kosseim, Senior General Counsel and Director General, Office of the Privacy Commissioner of Canada

Sabrina Anzini, Director, Law and Corporate Affairs, LoyaltyOne Inc.

Online tracking and behavioural advertising are not new. Moreover, while there are established guidelines and industry frameworks, there remains a high degree of variability in how they may be applied. In addition, online activities and capabilities are increasingly affecting all of us, as individuals and organizations; the lines between online and offline activities are not as clear as they once were; and the Internet continues to create new markets where products and services are sold in ways that

are often not easily understood. These are all reasons that this remains an area of uncertainty both for individuals and for organizations. This panel and dialogue explored these practices, their objectives, risks, consumer expectations, and other contextual factors within the current legal framework, including relevant recent decisions.

5:15 p.m.—**Day 1 Closing Remarks**

Andrew Pender, Associate Director, Executive Networks,
The Conference Board of Canada

5:30 p.m.—**Reception**

Day 2—Thursday, April 14, 2016

8:00 a.m.—**Continental Breakfast**

8:30 a.m.—**Welcoming Remarks From the Co-Chairs**

Andrew Pender, Associate Director, Executive Networks,
The Conference Board of Canada

Elizabeth Denham, Information and Privacy Commissioner for British Columbia

8:45 a.m.—**Plenary Session 5**

Privacy and Surveillance/Law Enforcement and Customer Privacy
Session Chair:
Dr. Colin Bennett, Professor, Political Science, University of Victoria

Speakers:
David Fraser, Partner, McInnes Cooper

Deborah Evans, Director, Consumer Policy & Associate Chief Privacy Officer, Rogers Communications Inc.

Brian Beamish, Information and Privacy Commissioner of Ontario

Ray Boisvert, President and Chief Executive Officer, I-Sec Integrated Strategies (ISECIS)

Law enforcement and national security access to customer information continues to be in the news. Following a high-profile case in Ontario that suggests businesses have an obligation to stand up for their customer's privacy in the face of government demands, business can expect to face pressure from both sides on these important issues. Things get even

more complicated if there is an inter-jurisdictional aspect. This panel discussed the ongoing tension between privacy and the public interest associated with law enforcement and national security investigations.

10:00 a.m.—**Networking and Refreshment Break**

10:30 a.m.—**Interactive Session—Set B**

Interactive Session B1
Big Data Use Case #3: Health
Moderators:
Cory Olson, Compliance Director, TELUS Communications Inc.

Dr. Khaled El Emam, Founder and Chief Executive Officer, Privacy Analytics

Interactive Session B2
Big Data Use Case #4: Personalization in the Financial and Insurance Sectors
Moderator:
John Russo, Vice-President, Legal Counsel and Chief Privacy Officer, Equifax Canada Co.

Micheal Vonn, Policy Director, British Columbia Civil Liberties Association

11:45 a.m.—**Networking Luncheon**

1:00 p.m.—**Use Case Breakout Report-Back**

1:30 p.m.—**Plenary Session 6**

Perspectives of Privacy Regulation in Canada
Session Chair:
Chantal Bernier, Counsel, Dentons Canada LLP

Panellists:
Susanne Morin, Vice-President, Assistant General Counsel, Quebec and Enterprise CPO, Sun Life Financial Inc.

Vincent Gogolek, Executive Director, BC Freedom of Information and Privacy Association (FIPA)

Cara-Lynn Stelmack, Director, Mediation and Investigation, Office of the Information and Privacy Commissioner of Alberta

Catherine Tully, Information and Privacy Commissioner for Nova Scotia

The good, the bad and the ugly: How do privacy regulations measure up? Where do we go from here and what should privacy regulations look like in the future for a better Canada? This animated discussion looked at privacy in Canada through various lenses.

2:45 p.m.—**Networking and Refreshment Break**

3:00 p.m.—**Plenary Session 7**

Moderated Dialogue: What Have We Learned and Where Do We Go From Here?
Speaker:
Andrew Pender, Associate Director, Executive Networks,
The Conference Board of Canada

Participants had the opportunity to provide additional input on the two days of dialogue and session topics. This group dialogue enabled participants to expand on their opinions and perspectives, and suggest ways forward on the issues addressed in the summit.

4:00 p.m.—**Plenary Session 8**

Next Steps and Future Actions
Co-Chairs:
Andrew Pender, Associate Director, Executive Networks,
The Conference Board of Canada

Elizabeth Denham, Information and Privacy Commissioner for British Columbia

This session recapped the Summit and outlined next steps and actions, based on stakeholders' input over the two days.

4:45 p.m.—**Closing Remarks**

Andrew Pender, Associate Director, Executive Networks,
The Conference Board of Canada

5:00 p.m.—**Summit Adjourned**

APPENDIX C

Sponsors and Supporters

The Canadian Privacy Summit would not have been possible without the generous contributions of our sponsors and supporters.

In Partnership With

- The Office of the Information and Privacy Commissioner of British Columbia

Major Sponsor

- Symcor

Sponsors

- Aimia
- Canadian Marketing Association
- Equifax
- Google Canada
- IBM Canada
- LoyaltyOne
- Sun Life Financial
- TELUS

The More Enlightened Way to Make Business Decisions.

If your organization, program, or project requires expertise in economic or organizational performance or public policy, talk to us first. You'll find the expertise and knowledge you need to make more enlightened decisions with The Conference Board of Canada.

Services

Executive Networks
Exchange ideas and make new contacts on strategic issues

e-Library
Access to in-depth insights … when you need them most

The Niagara Institute
Develop leaders of the future through interactive and engaging leadership development programs

The Directors College
Canada's university-accredited corporate director development program

Custom Research
Tap into our research expertise to address your specific issues

Customized Solutions
Help your organization meet challenges and sustain performance

e-Data
Stay on top of major economic trends

Conferences, Seminars, Webinars, and Workshops
Learn from best-practice organizations and industry experts

The Conference Board of Canada | Le Conference Board du Canada

conferenceboard.ca

About The Conference Board of Canada

We are:

- The foremost independent, not-for-profit, applied research organization in Canada.
- Objective and non-partisan. We do not lobby for specific interests.
- Funded exclusively through the fees we charge for services to the private and public sectors.
- Experts in running conferences but also at conducting, publishing, and disseminating research; helping people network; developing individual leadership skills; and building organizational capacity.
- Specialists in economic trends, as well as organizational performance and public policy issues.
- Not a government department or agency, although we are often hired to provide services for all levels of government.
- Independent from, but affiliated with, The Conference Board, Inc. of New York, which serves nearly 2,000 companies in 60 nations and has offices in Brussels and Hong Kong.

Insights. Understanding. Impact.

The Conference Board of Canada

255 Smyth Road, Ottawa ON
K1H 8M7 Canada
Tel. 613-526-3280
Fax 613-526-4857
Inquiries 1-866-711-2262
conferenceboard.ca

PUBLICATION 8239 | 8240
PRICE: Complimentary