A Behavioural Lens on Consumer Privacy

Melanie Kim, Kim Ly, and Dilip Soman

15 September, 2015

Rotman School of Management
UNIVERSITY OF TORONTO

Research Report Series
Behavioural Economics in Action

Rotman School of Management
University of Toronto

Correspondence and Acknowledgements

For questions and enquiries, please contact:

Professors Dilip Soman or Nina Mažar
Rotman School of Management
University of Toronto
105 St. George Street
Toronto, ON M5S 3E6

Email: dilip.soman@rotman.utoronto.ca or nina.mazar@rotman.utoronto.ca
Phone Number: (416) 946-0195

We thank Liz Kang, Vivian Chen and Zohra Ilhom for research assistance, and to Omkar Chetty, Emita Latif, Howard Deane, Cristina Onose, Nina Mazar and Avi Goldfarb for inputs and comments. We also thank Daisy Deng for creating the illustrations. All errors are our own.

Table of Contents

List of Figures

1. Introduction

A walk on the face of a beach will leave behind a set of footprints that others who walk can see and track. However, these footprints are temporary – a few hours later when the tide rolls in again or when they have been walked over by other travelers, they get washed off. Imagine a scenario in which the footprints are indelible and can never be removed. Imagine, further, that the footprints can be shared by anyone anywhere in the world. A walk on the beach can never be a private and personal experience anymore.

A metaphorical walk through the world of the Internet also leaves behind a set of digital footprints that are indelible and can be easily shared (Madden et al., 2007). Consequently, in recent years, a number of high-profile cases involving the violation of customer privacy online have raised public alarm. Home Depot made headlines last year because of a massive theft of its consumer credit and debit card database, which affected more than 56 million customers (Soergel, 2014). Earlier, in 2012, retailer Target was in the spotlight because of a newsworthy privacy violation. The company's data-driven algorithm correctly identified a customer's pregnancy and sent the teenage girl coupons for baby gear. The teenage girl kept the pregnancy a secret, yet her father became aware of the fact when the company began sending coupons to their home (Duhigg, 2012). Finally, one of the most recent cases of privacy violation happened even while we were preparing this report. In the summer of 2015, a data breach occurred at Ashley Madison, an extra-marital affairs website. More than 30 million accounts were stolen and posted online for anyone to search, including ones that were supposedly deleted. (Bora, 2015)

Privacy concerns ring louder when considering the broad spectrum of personal data amassed online. With an increasing number of online transactions and a growing assortment of devices connected to the Internet, there is, for the first time, one pipeline through which almost all our personal information flows. For instance, a mobile device such as a smartphone might be a conduit for a consumer's email and social communications, banking accounts, travel arrangements, home energy systems and even details of family and friends. When much of consumers' private information resides in one conduit, even a single vulnerability can cause significant harm. A security hack such as Stagefright, a virus that can access and control parts of an Android phone without the user's knowledge, can leave information – ranging

from e-mails to the user's location to personal photos – susceptible to compromise (Rundle, 2015). Likewise, digital hacks on vehicles to remotely control the wheel can put the personal safety of passengers at major risk (Greenberg, 2015).

Why have we seen such a large increase in these high-profile privacy violations? We believe that there are two forces that have fueled this trend:

1) The first set of forces has to do with the fact that there is more consumer information available online than there has ever been. This is because ***companies have a greater incentive*** to, and ***reduced costs*** of, collecting and sharing data on their online customers. Since a growing number of consumer activity (information search, browsing, and even actual transactions) happens online or through other electronic formats (such as in-store kiosks), it is very easy to collect and build large datasets on consumer behaviour. Having more data on customers allows firms to build a richer profile, which in turn has implications for their ability to more narrowly target advertising and marketing offers. It also allows for companies to gain easier access to their target segments and to use the benefits of network effects to create positive word of mouth through easy online information sharing. In addition, the collected data can be re-packaged and sold to companies, creating a secondary market for aggregate consumer information.

2) ***There have been tremendous advancements in tools and technology*** that improve the ability to aggregate, analyze, and draw sensitive insights from personal information.

Together these two trends have contributed to exponentially *increasing consumer risks of sharing information* online. Economic and social discrimination, censorship, and identity fraud are only a few negative consequences. Yet, it is not clear that consumers typically think about data shared online as a risky situation. We believe that a large percent of online consumers do not even think about the risks of sharing information online, and the ones that do probably do not have the right information to be able to make an accurate assessment of risk levels.

Research in the area of the behavioural sciences has shown that consumers are limited processors of information. They tend to make decisions using heuristics, that is, they often use a number of decision shortcuts rather than processing information fully. This research also shows that humans face

multiple cognitive biases that impede accurate assessment of risky information.

In this report, our goal is to put a behavioural lens on the topic of online customer privacy. In particular, we present the behavioural biases that contribute to the problem of online privacy. Further, we identify behaviourally informed solutions that can best safeguard consumer interests online. In our view, these solutions take three forms:

1) ***Equip the consumer***: The first set of solutions is designed to better equip consumers to assess the risks of sharing data online. The first element of equipping consumers is to sensitize them to the notion that information shared online could constitute a potential risk. Having achieved that goal, the appropriate use of disclosure and privacy policies can then further educate consumers about the level of the risk. More generally, we propose that a program on privacy literacy – which might include advertising and labelling components – will better sensitize consumers to the risks associated with online data sharing.

2) ***Pad the environment***: Padding the environment simply refers to actions that make the environment safe for consumers who might not have the ability or motivation to process information fully. One example of a padding strategy is setting the defaults on online websites to the highest level of consumer privacy. Similarly, the default setting on mobile devices might be to turn location devices off. A second tactic might include the use of reminders or decision points to nudge users about the potential risks associated with sharing information online.

3) ***Incentivize businesses suitably***: In our opinion, it is important to focus privacy efforts not only on consumers, but also on providers of online web content. For example, we believe that it is important to make efforts to ensure that consumer privacy is a central value proposition so that firms can actively incorporate privacy into their marketing and selling efforts. Likewise, we also believe that the use of privacy badges or a rating system that evaluates the privacy policies of a given business will nudge businesses into creating a safer environment for their customers.

The remainder of the report is organized as follows. First, we review relevant research from the field of behavioural insights to develop a framework for why and how consumers may not be able to accurately assess the risks associated

with online data sharing. Next, we develop an understanding of what the actual risks might be, and explore challenges for public policy in the evolving digital landscape. Then we examine key efforts by policymakers, businesses, and third parties through a behavioural lens.

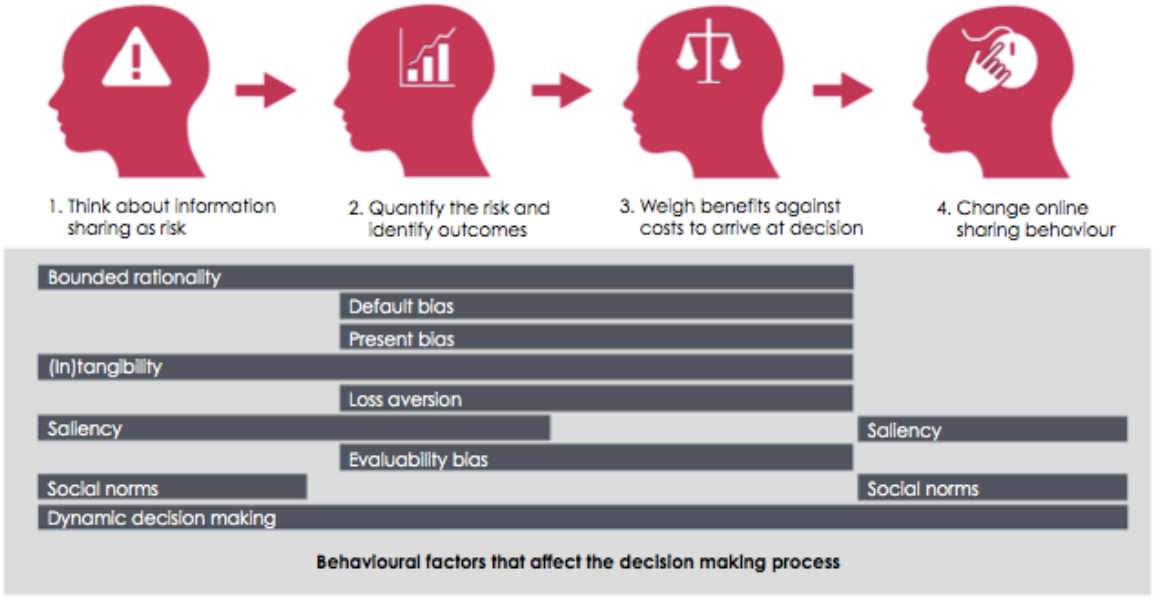
Building on our findings from the previous sections, we develop a set of behaviourally informed prescriptions for how companies, governments, and consumer bodies can better solve the problem of online consumer privacy. Finally, we end with a discussion that includes – among other things – a segment on how privacy efforts might be measured, tracked, and used over time.

2. Behavioural Insights

The increase in privacy-related violations poses an interesting question on what behavioural biases contribute to consumers engaging in risky behaviour online. From a behavioural sciences perspective, we believe that the root of the online privacy challenge is, at least partly, a decision-making problem on the part of consumers.

To make a fully informed decision about what information she should share online on any given occasion, a consumer needs to go through several decision-making steps. The three key steps are illustrated in Figure 2.1. First, the consumer needs to use the appropriate mental model and think about information sharing as a risky prospect, much like one might think about the risk of a side effect after consuming medication or the risk of losing monetarily when trading in risky assets. Second, the consumer needs to use available information to quantify the risk and identify the outcomes. Finally, the consumer would need to integrate the risk level with the outcome information to arrive at a judgment of whether the benefits of sharing information exceed the potential harms.

Figure 2.1. How data sharing decisions ought to be made



However, decades of research in the behavioural sciences show that most humans lack both the cognitive apparatus as well as the motivation to go

through each of the steps. It is not clear whether most people think of information sharing as risky behaviour, and we are all too familiar with people scrolling through detailed disclosures with a flick of their finger so that they can quickly click the "I agree" button and proceed with a download or purchase.

Below are common themes from behavioural sciences that help explain why consumers have difficulty accurately assessing the risks associated with online data sharing:

- *Bounded rationality*: While traditional economic theory suggests that consumers are rational in their decisions and have unbounded capacity to process information, evidence from behavioural sciences indicates otherwise. Consumers are limited processors of information and are unable to fully assess the risks and probabilities associated with sharing personal information online (Acquisti, 2004). They also rely on using decision shortcuts and simplifying heuristics (Kahneman, 2011).

- *Default bias*: To the extent that consumers fail to recognize privacy risks, do not care, or are not motivated to actively address their privacy concerns, they will stay with the status quo (Tannenbaum & Ditto, 2011). In addition, many consumers are uncertain about their privacy-related preferences, and may stick with the default option by interpreting it as a recommendation or reflection of what most individuals prefer (Acquisti, Brandimarte, & Loewenstein, 2015). In the online privacy context, where the default orientation is often being tracked and surrendering data, consumers are likely to stick with that option.

- *Present bias*: Consumers place more weight on immediate benefits and costs relative to those that are distant (O'Donoghue & Rabin, 1999). On many websites, attention is drawn to the immediate benefits of information sharing, such as special promotions, chances to win prizes, or access to the Internet, while the costs of divulgence such as spamming or identity fraud are delayed in time (John, 2015). Consumers' tendency for hyperbolic discounting of future costs and benefits, then, lends to impulsive data-sharing behaviour (Acquisti & Grossklags, 2007).

- *(In)tangibility*: When assessing options, consumers are more strongly influenced by outcomes that are concrete and certain, compared to those that are abstract and probabilistic (Schneider & Ingram, 1990). The potential costs of surrendering personal data, such as identity theft

and economic discrimination, are ambiguous and difficult to quantify, leading consumers to prioritize options with more definite outcomes, such as receiving small discounts in exchange for personal information (Acquisti, John, & Loewenstein, 2013; John, 2015).

- *Loss Aversion*: Consumers place a disproportionately large weight on losses relative to gains of equivalent size (Kahneman, Knetsch, & Thaler, 1991). Research shows that consumers value privacy more when they stand to lose it, compared to when they believe privacy was not theirs to begin with (Acquisti et al., 2013). As the current default in privacy settings is for personal information to be public, consumers may believe they have little privacy to begin with, and as a result, value it less (John, 2015).

- *Saliency*: When attention or cognitive resources are limited, consumers only take into account behavioural cues that are salient (Mann & Ward, 2007). In particular, consumers' attention is drawn to stimuli that are novel, accessible, and simple (Dolan et al., 2012). Privacy information is none of those; it is displayed in long and boring text in disclosure statements, often hard to find, and difficult to read and process. It is unsurprising that privacy is not at the top of mind of consumers when they are online.

- *Evaluability bias*: Consumers pay more attention to attributes that are easy to evaluate (Hsee, 1996). In particular, quantifying attributes using numerical scales makes for easier evaluation and comparison (Yalch & Elmore-Yalch, 1984). Yet, privacy attributes of online businesses are difficult to evaluate, leading consumers to pay less attention to privacy when deciding between competing alternatives of online businesses or websites. Furthermore, it is uncertain whether consumers are even aware of the dimensions on which to evaluate privacy.

- *Social norms*: Privacy decision making is affected by social norms, which consumers infer partly by observing others' behaviours (Acquisti et al., 2015). As social media sites like Facebook highlight others' information-sharing activities using features such as "News Feed," consumers observe a norm of divulgence, leading them to share more information online (John, 2015).

- *Dynamic Decision Making*: Research in dynamic decision making studies the manner in which consumers make decisions in situations in

which the context and the background variables are changing (Sterman 1989). In essence, dynamic environments are those in which the rules or models that underlie judgments change with time. The general finding from this research is that consumers have difficulty in anticipating changes to the environment and are slow to learn. Consequently they might make decisions that would have been considered good in a past environment but might no longer be appropriate. The Internet is a classic example of a dynamic environment – as technologies and capabilities change, data sharing practices that were once considered safe might now not be safe anymore. For instance, Facebook users could post personal picture and avoid being identified in those pictures by not "tagging" themselves. However, facial recognition technology has evolved and today it is possible for untagged consumers to be identified through their posted photographs (Dean, 2015).

In the online space, the cost of making a cognitive mistake and surrendering too much personal information is significant. The information that consumers give away 1) remains in the digital pipeline forever, 2) the flow of data is rapid and almost instantaneous, and 3) one crack in the pipeline can expose a flood of sensitive data. As cognitive biases influence the millions of decisions that consumers make every day, the vulnerabilities build up rapidly – often without the consumers' knowledge.

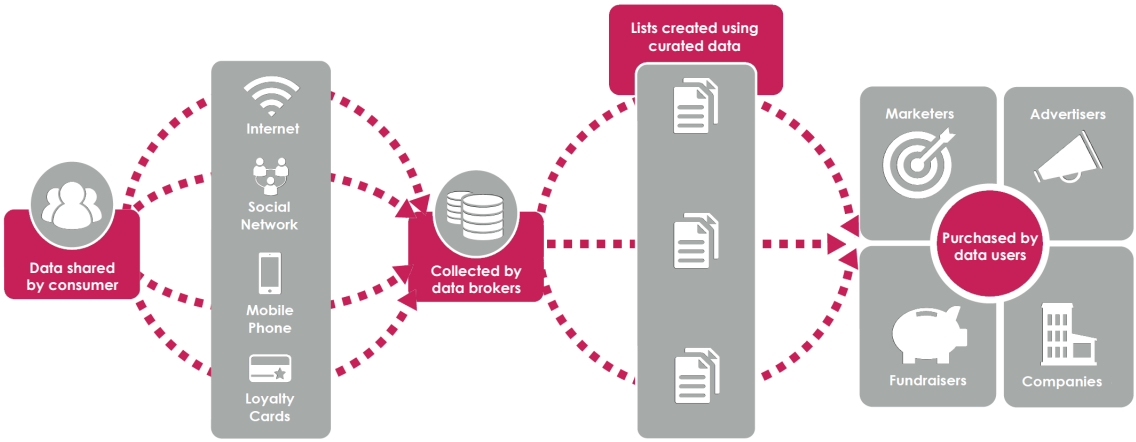
3. Consumer Privacy Risks in the Current Landscape

According to results from the 2012 Canadian Internet Use Survey, a majority of Internet users in Canada did their banking online (72%), visited social networking sites (67%), and ordered goods and services online (56%) (Mazowita & Vézina, 2014). There is little question that consumers appreciate the digitized experience that increases convenience, saves them time and money, and makes their lives more entertaining.

Businesses also benefit from the data economy. Customer data is a valuable asset that allows more narrowly targeted marketing offers, and companies are enthusiastically collecting reams of data, hoping to translate insights into revenue (Morey, Forbath, & Schoop, 2015). In addition, it is getting cheaper to store massive datasets on customers, and advanced technological tools are making it easier for businesses to create profiles on their customers and make predictions about their interests and behaviours (Morey et al., 2015).

At the same time, the flow of data is becoming broader and more complex, opening up more opportunities for misuse (Acquisti et al., 2015). From social networks to Internet companies to data brokers that create dossiers of individuals for sale, it is increasingly difficult to track which entities have access to an individual's personal information (Thompson, Krashinsky, & Dingman, 2014). There is also concern over whether this information is being shared with consumers' awareness and consent. A recent survey shows that less than half (47%) of Canadians expressed confidence that they know how the personal information they share with an organization will be used (Phoenix SPI, 2014). Figure 3.1 shows a path that personal information can take before landing on a particular marketer's curated mailing list.

Figure 3.1. Flow of personal information

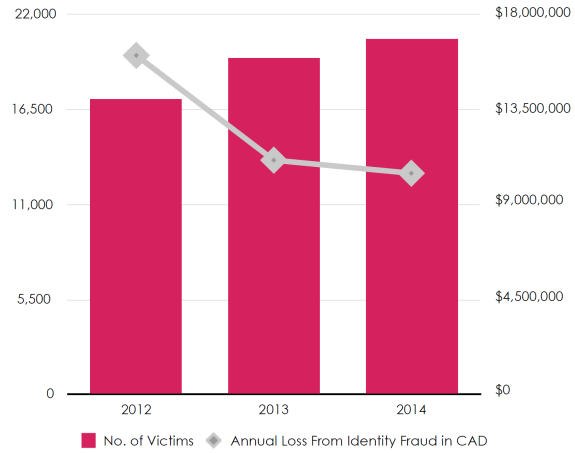


The quickly evolving digital landscape makes risk assessments even more difficult for consumers. For instance, researchers from Carnegie Mellon University found that it is possible to identify strangers, and sometimes even their Social Security numbers, by using a combination of facial recognition software and social network profiles (Hill, 2011). Geotracking systems, intelligent technology in physical products, and vehicles' increasing connection to the Internet are among developments that heighten privacy concerns for consumers (Morey et al., 2015; Greenberg, 2015). More than half (56%) of Canadians report they have insufficient information to understand how new technologies might affect their personal privacy (Phoenix SPI, 2014).

The potential consequences of sharing personal data online come in various forms.

Incidences of identity *theft*, whereby thieves steal an individual's information; and identity *fraud*, whereby thieves use that stolen information for criminal activity, have captured the government's attention lately (Northcott, 2012). Figure 3.2 shows the trend of such incidences over recent years, according to the Canadian Anti-Fraud Centre (CAFC). The total reports of identity theft increased by 29% from 2013 to 2014, and the reports of identity fraud increased by 6% during the same period (CAFC, 2014). The annual cost of identity fraud was over 10 million CAD during both years (CAFC, 2014).

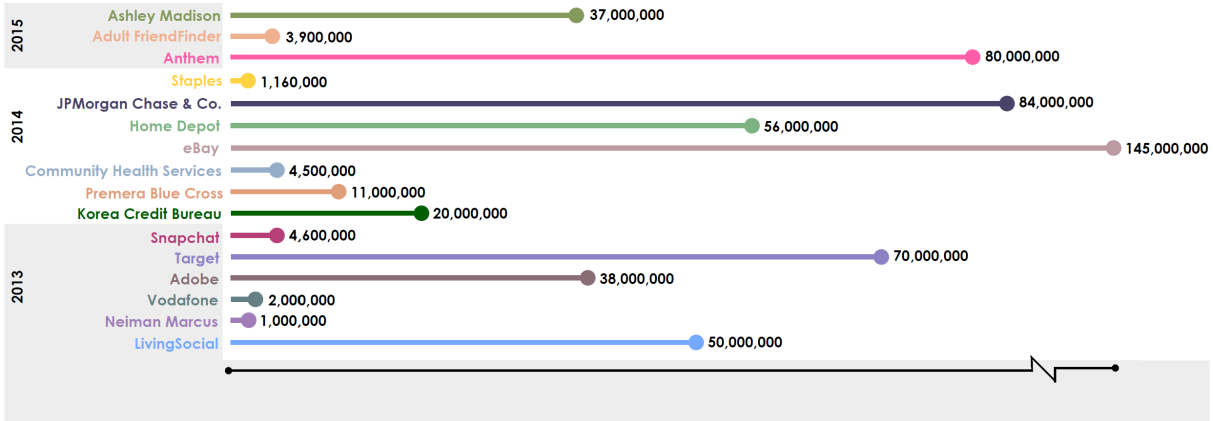
Figure 3.2. Identity fraud trends in Canada



Source: Canadian Anti-Fraud Centre. (2014). Annual statistical report 2014. Retrieved from http://www.antifraudcentre-centreantifraude.ca/reports-rapports/2014/ann-ann-eng.htm#a1

Another risk comes in the form of security breaches by hackers, whereby consumers' personal information such as credit card details, e-mail addresses, and passwords may be compromised. Figure 3.3 shows some of the world's largest data breaches in recent years.

Figure 3.3. Significant data breaches (by accounts compromised)



Source: Quick, M., Hollowood, E., Miles, C., & Hampson, D. (2015). World's biggest data breaches. *Information is Beautiful.* Retrieved from http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Other consequences are more ambiguous, such as the uncomfortable feeling of being monitored, the inconvenience of receiving spam mail, and social and economic discrimination (Acquisti et al., 2015). For instance, marketers

may use ethnicity information to keep attractive offers out of reach to the least profitable and most costly population segments (Noyes, 2015). Knowing that particular demographics are willing to more effectively use social media, businesses may also reward them with better customer service and shorter wait times (Schrage, 2014).

Perhaps one of the biggest challenges to an accurate assessment of risk on the part of the consumer arises due to the dynamic nature of the online environment caused by rapid technological advances. Earlier in the report, we considered the example of posting photographs online. Till fairly recently, it was relatively safe to post photographs in which a consumer did not want to be identified. This could be achieved without "tagging" the photograph. However, technology has evolved and there now exist algorithms that can identify people in photographs even when they are not tagged. A once-safe sharing practice is no longer safe.

A second example of the dynamic of the online environment comes from a Portugese online platform called Eter9 (Brown, 2015). Using artificial intelligence and related modeling techniques, this platform is able to learn a particular consumer's personality on the basis of their historic online activity. Once the model is suitably calibrated, a consumer's online profile can be mimicked by the model. A capability that might have seemed to be straight out of a science fiction movie only a few months ago is now almost reality.

4. Challenges to Policy in the Evolving Landscape

The environment in which personal information is collected, used, and shared has transformed dramatically since the Personal Information Protection and Electronic Documents Act (PIPEDA) came into force in 2001. The fair information principles that businesses must abide by under PIPEDA are listed in Appendix A. The three key themes on which PIPEDA operates – transparency, consent, and accountability – are continuously challenged in the evolving digital landscape:

Transparency of privacy-related practices

PIPEDA requires businesses to be open about their data management practices to customers (Office of the Privacy Commissioner of Canada [OPC], 2014). Yet, research shows that presenting information in the form of privacy disclosure statements does not support customers' assessment of privacy-related trade-offs (McDonald & Cranor, 2008). Over the years, privacy disclosure statements have become lengthier and more transparent, but customers' understanding or motivation to read them has not improved (Cranor, McDonald, Egelman, & Sheng, 2007). As limited processors of information, customers tend to ignore this information altogether.

Informed consent by consumers

Organizations covered by the Act must obtain an individual's consent when they collect, use, or disclose customers' information (OPC, 2014). The challenge, however, lies in ensuring that the consent is *informed*. As most consumers don't read privacy disclosure statements (McDonald & Cranor, 2008), they are likely to miss critical information that may change their decision to check the "I agree" box. There are also other contextual reasons consumers may impulsively consent to privacy policies without being informed. For instance, many websites increase the salience of features like special promotions and discounts that motivate impulsive data-sharing behaviour, leaving privacy concerns in the backseat (John, 2015). Furthermore, new technologies such as facial recognition software and advanced data mining techniques make it more difficult for individuals to understand evolving risks and give meaningful consent (Acquisti et al., 2015).

Accountability of organizations

PIPEDA lacks enforcement mechanisms strong enough to ensure that businesses prioritize customers' privacy rights (Faguy, 2014). The OPC cannot issue binding orders or impose penalties against anyone who breaches the provisions of PIPEDA (Faguy, 2014). The global nature of online businesses further complicates enforcement of any privacy legislation. PIPEDA may apply to over a million businesses across Canada, but many businesses are headquartered in other countries, with or without their own privacy legislations (OPC, 2013).

And, to the extent that companies perceive privacy as a win–lose game, it is difficult to incentivize them to invest appropriately in privacy. And same as the individual consumers, companies suffer from a present bias - investing more in these technologies costs money now, whereas the costs of potentially losing customer trust are delayed and probabilistic (Harvard Business Review [HBR], 2014). Furthermore, the immediate benefits of gaining access to customer data for targeted marketing and perhaps sale to third parties appear too good to forgo (HBR, 2014).

5. Key Efforts by Other Players

Heightened concerns for online privacy in light of the high-profile cases have pushed various actors – policymakers, industry, and third-party organizations – to step up their efforts to safeguard consumer privacy.

Policymakers

Currently, there is no international agreement on online privacy standards, which confounds regulations governing online business practices across jurisdictions. The European Commission plans to unify data protection rules within the European Union under a single law, called the General Data Protection Regulation (GDPR) (DLA Piper, 2014). The key changes from the current data protection framework can be found in Appendix B. The enactment of GDPR is projected to be early 2016, and the rules are expected to have immediate effect in all 28 EU member states after a two-year transition period (DLA Piper, 2014).

This new regulation contains several behaviourally informed elements. It introduces the concept of "privacy by default," whereby default settings must be those that provide the most privacy (EC, 2012). By default, only personal data necessary for specified purposes should be collected, and that data should not be retained beyond the time necessary for those purposes (DLA Piper, 2014). To the extent that consumers favour and stay with the status quo, this default mechanism will ensure that they are navigating the online space under safer conditions.

The regulation also aims to give consumers more control over their personal data. It requires data processors to get unambiguous and explicit consent by individuals, to extend consumers' right of access to their data, and to give them the right to delete their personal data collected by organizations (EC, 2012). These key changes enforce the idea that personal information belongs to individuals and not data processors. The loss aversion theory suggests that as consumers develop a taste for owning privacy, they will place a larger value on privacy and be less willing to part with it.

Furthermore, consumers can benefit from the trendsetter effects when the regulation kicks in. Europe's previous privacy laws have been imitated by many countries including Canada (Faguy, 2014), and as more and more countries adopt similar legislations, privacy-centred practices may become a social norm. These social effects may be powerful in creating an environment

where consumers expect more privacy, and companies, in turn, assume more responsibility and accountability for processing customer data.

Lastly, the GDRP quantifies a concrete figure for the fines for businesses that do not protect customer data in line with the regulation. By quantifying fines as up to 1 million euros or 2% of their global annual turnover (DLA Piper, 2014), companies will be more attentive to implementing mechanisms in line with GDRP so as to avoid the specified potential costs.

Industry

Some Internet companies like Microsoft and Mozilla have attempted to put more privacy control in the hands of consumers by making default settings privacy friendly. In 2013, Microsoft made a move to enable the "Do Not Track" (DNT) option as the default setting on its new Internet Explorer browser (Lardinois, 2015). Enabling this option tells websites and third-party advertisers to voluntarily refrain from collecting data from the user. Though adjusted settings significantly increased the proportion of users with DNT enabled, this initiative was unsuccessful because the voluntary nature of the DNT led most advertising companies to not honour it (Lardinois, 2015). Microsoft abandoned this initiative in April 2015 (Lardinois, 2015).

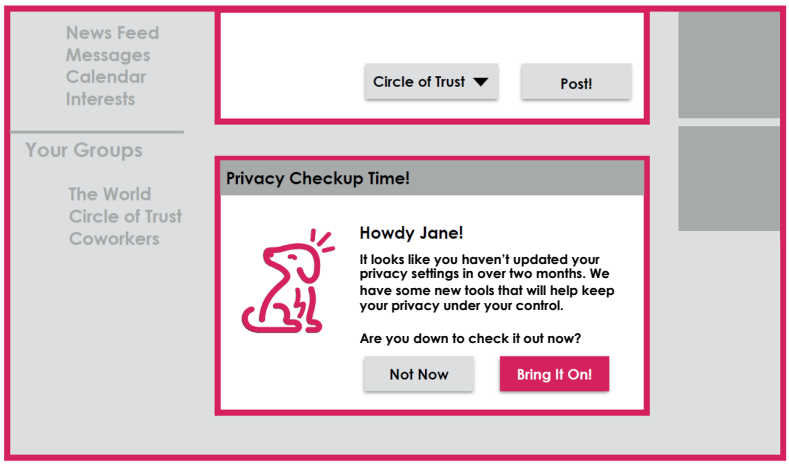
The same year Microsoft enabled the DNT, Mozilla tried to take a stricter stance by planning to block third-party cookies by default on their new Firefox browser (Timberg, 2013). Third-party cookies are placed on website ads so that advertisers and online networks can track a user's activity. Unlike the DNT feature, this default option would not be voluntary, and the implication was that hundreds of companies that used to monitor Firefox users would not be able to do so anymore (Timberg, 2013). Due to heavy opposition by the advertising industry, among other reasons, Mozilla's initiative never took off (Quirk, 2014).

Lately, other online businesses have tried to make privacy settings easier to access and understand. In 2015, Google pulled all its privacy and security controls into a single hub called "My Account," and introduced a privacy checkup tool for users to control what data is being gathered about them (Kelion, 2015). The company also tells users what they are trading off as they change settings – for instance, quicker search queries – which assists them in making decisions in line with their preferences.

Earlier, in 2014, Facebook also launched an interactive walkthrough of its privacy settings, called "Privacy Checkup" (BBC News, 2014). This tool is

guided by a cartoon dinosaur, which pops up when users are posting publicly without having updated their privacy settings for some time (BBC News, 2014). The reminder, then, creates a decision point to get users to deliberate about changing their settings. According to Facebook, more than three-fourths of users in their early test sample who saw the dinosaur – a novel visual stimuli – completed the checkup (Albergotti, 2014). As Internet giants such as Facebook and Google make privacy more salient and attempt to give users greater control of their data, other companies may feel pressured to follow suit. Some key elements of user-friendly privacy checkup features and reminders are illustrated in Figure 5.1.

Figure 5.1. A decision-point approach to privacy



A sample reminder social media sites may use to create a decision point for users

Third-party organizations

Privacy seals that help consumers easily evaluate an organization's privacy practices are an increasingly common feature in the online landscape. For consumers, identifiable seals like TRUSTe and BBB Accreditation seals (see Figure 5.2) may reduce the perception of privacy risk of certified businesses (Salehan, Kim, & Lee, 2015). Some experiments show that privacy seals appear to instil consumers' trust in the website (Hu et al., 2010) and their willingness to purchase from the site (Chang, Fang, & Tseng, 2012).

Figure 5.2. TRUSTe and BBB accreditation seals.

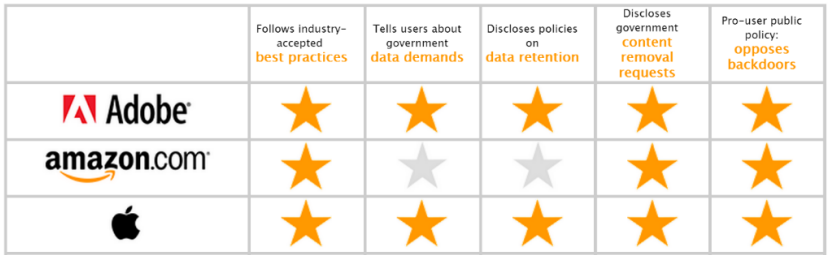
Source: TRUSTe.com; BBB.org

The goal of TRUSTe and BBB seals is to increase perceived security and establish trust among consumers

The confidence that consumers impart on these seals, however, may be unjustified. As consumers are susceptible to a number of decision shortcuts, they are inclined to process the seals as assurance of privacy without checking their authenticity or understanding what protection they offer (LaRose & Rifon, 2007). A study from Harvard shows that sites with TRUSTe certifications are more than twice as likely to be untrustworthy with customers' data as uncertified sites (Edelman, 2010). Credibility of privacy seals and an understanding of what they are signalling are important in creating meaningful behavioural cues for consumers.

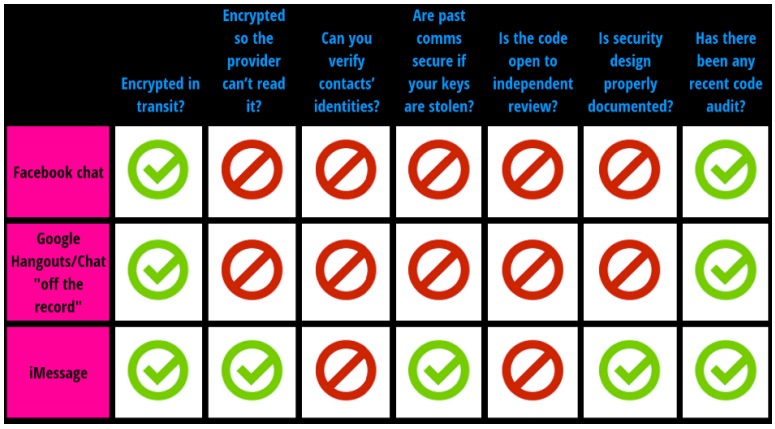
The Electronic Frontier Foundation (EFF) is another organization that evaluates Internet companies, mainly on transparency and privacy practices when it comes to government requests for accessing user data (Lomas, 2015). Figure 5.3 shows EFF's ratings of major Internet companies on a five-star scale, which provides an avenue to discuss and compare data practices of online giants like Amazon and Google (Lomas, 2015). EFF also uses simple and clear criteria to provide useful information for consumers who want to compare messaging tools (See Figure 5.4).

Figure 5.3. EFF's Fifth Annual Who Has Your Back? Report Card



Source: Electronic Frontier Foundation. (2015). *Who has your back?* Retrieved from https://www.eff.org/who-has-your-back-government-data-requests-2015

Figure 5.4. EFF's Secure Messaging Scorecard



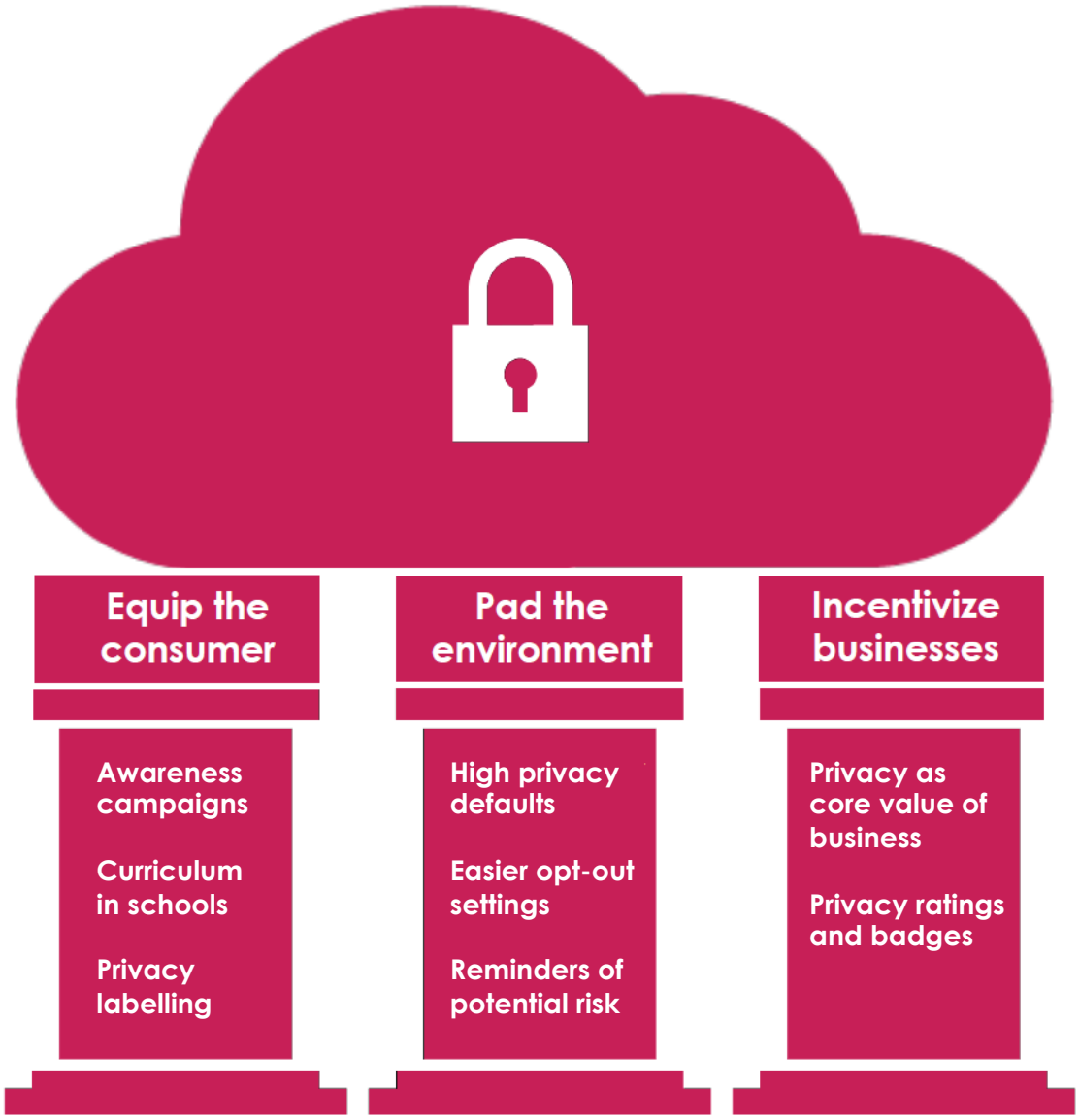
Source: Electronic Frontier Foundation. (2014, November 6). *Secure messaging scorecard*. Retrieved from https://www.eff.org/secure-messaging-scorecard

6. Behaviourally Informed Prescription

Traditional interventions in public policy take the form of regulation or incentives. For example, a regulatory body can enforce a law banning the processing of customer data without consent, and impose a large penalty for companies that don't comply. Policymakers can also provide monetary incentives for companies to invest in more secure technology to safeguard customer data. Another approach – and the one we will pursue here – is to design behaviourally informed solutions.

We acknowledge that consumers are limited processors of information, susceptible to cognitive biases when making privacy-related decisions, and prone to displaying impulsive behaviour online. Using themes from behavioural sciences, we've designed three sets of solutions – equipping consumers, padding the environment, and incentivizing businesses – which can help improve consumers' decision-making processes and assist them in making informed, safer choices. These solutions are summarized visually in Figure 6.1.

Figure 6.1. Three sets of behaviourally informed solutions



Equip the consumer

The first set of solutions is designed to better equip consumers to assess the risks of sharing data online. An important element of equipping consumers is to sensitize them to the notion that information shared online could constitute a potential risk. With less than half (47%) of Canadians expressing confidence that they know how organizations use their personal information (Phoenix SPI, 2014), we believe it is important to propose a program on privacy literacy,

which may include awareness campaigns and curriculums in schools and colleges. Having achieved the goal of sensitizing consumers to the risk, the appropriate use of disclosure – which may include labelling components for easier evaluation of privacy practices – can then further educate on the level of risk.

The food industry, for example, has done a good job in sensitizing consumers to risk. Health risks are similar to privacy risks in that they are difficult to quantify, hard to assess individually, and delayed in time. A particular feature of the food industry's success is nutrition labelling. In part to address low literacy rates, nutrition labelling was designed to simplify information as much as possible for consumers and provide a common terminology to talk about nutrition and health risks (Kelley, Bresee, Cranor, & Reeder, 2009). By standardizing labels across food items, consumers are able to quickly find what information they are looking for in any label and easily compare products (Kelley et al., 2009). A simple, standardized privacy label may serve as a useful tool to help consumers assess and compare risks in the digital space (Kelley et al., 2009).

Pad the environment

Padding the environment refers to actions that make the environment safe for consumers who might not have the ability or motivation to process information fully. One example of a padding strategy is setting the defaults on online websites to the highest level of privacy. Similarly, the default setting on mobile devices might be to turn location devices off. As discussed in the case of Microsoft and Mozilla, however, it is difficult for individual companies to take drastic action when faced with strong opposition from advertising networks and other third-party marketers. Perhaps the European Commission's regulation that introduces "privacy by default" will help enforce the concept at a larger scale, but it will take time.

A simpler way to pad the environment may be to make it easier for consumers to control privacy settings and opt out of unwanted default settings. The privacy checkup tools of Google and Facebook have both been useful in capturing users' attention on privacy controls and getting them to go over and consider updating their privacy settings (Albergotti, 2014). A second tactic might include the use of reminders or decision points to nudge users about the potential risk associated with sharing information online.

Incentivize businesses

It is important to focus privacy efforts not only on consumers, but also on providers of online web content. For example, we believe that it is important to strive to make consumer privacy a central value proposition so that firms can actively incorporate privacy into their marketing and selling efforts. If consumers start recognizing the importance of privacy and have the ability to measure the privacy quality of a given website, there would be increased demand for higher levels of security, which, in turn, might push privacy as a central value proposition for online businesses.

How can consumers be given a tool to assess the privacy quality of websites, and how can businesses be nudged into improving privacy? In an unrelated domain, restaurant hygiene quality grade cards are a good example of how this solution may work. When Los Angeles County introduced these grade cards to be displayed in restaurant windows, the restaurants' health inspection scores increased, consumers became more sensitive to restaurant hygiene, and the number of hospitalizations due to foodborne illnesses dropped by 13% (Simon et al., 2005). These grade cards, which provided consumers with a simple way of evaluating and comparing a complex variable such as hygiene were successful in convincing restaurants to incorporate hygiene as an important value proposition in their business. Likewise, we believe that the use of privacy badges or a rating system that evaluates the privacy policies of a given business will nudge businesses into creating a safer environment for their customers.

There is another important consideration, however. As in the case with TRUSTe seals, consumers may take into account these ratings or badges without a good understanding of what they measure (LaRose & Rifon, 2007). Hence, it's important for the organization supplying these ratings to be trustworthy, to conduct periodic reevaluations, and to clearly communicate to consumers what their ratings are signaling.

7. Discussion

With increased connectedness and activity online, we now face an era where there is one pipeline through which all our personal information flows. It used to be that one piece of information was used for a handful of purposes. Now, with this single pipeline wherein all personal data lie, businesses and marketers can easily create digital profiles of consumers with details about their social network, interests, and habits – for use in previously unthinkable ways. The rich streams of data, characterized by the timelessness of their existence and by the fast speed at which they can be shared, introduce new and evolving risks for consumers.

The multiple cognitive biases identified in this article indicate that consumers can't always be relied on to accurately assess complex privacy-related trade-offs. Acknowledging their cognitive limitations, we believe that the responsibility for ensuring public welfare lies equally with businesses and government. Yet, most privacy policies and efforts do not take into account the human tendencies of the ultimate users for which these initiatives are designed. One well-known example would be the lengthy disclosure statements that businesses display to obtain "informed" consent – the same ones that consumers routinely ignore before clicking the "I agree" button to proceed with a download or a purchase. Further, considering that Internet users include children, the elderly, and individuals with disabilities who may face greater difficulty evaluating privacy trade-offs, the need to put safeguards in the environment becomes more evident.

The recommendations made in this paper aim to incorporate our understanding of behavioural science to help policymakers and businesses better assist consumers in navigating the complex online space. To result in better privacy outcomes, privacy initiatives must be designed for real humans – those who are limited processors of information, susceptible to cognitive biases, and prone to displaying impulsive behaviour online.

Perhaps one key thrust of ongoing research and efforts in this area has to do with developing the appropriate metrics for measuring privacy. In particular, we call for the development of scales to measure two distinct sets of outcomes:

a) Privacy literacy: Consumers' knowledge about potential risks and their ability to gauge and assess these risks;

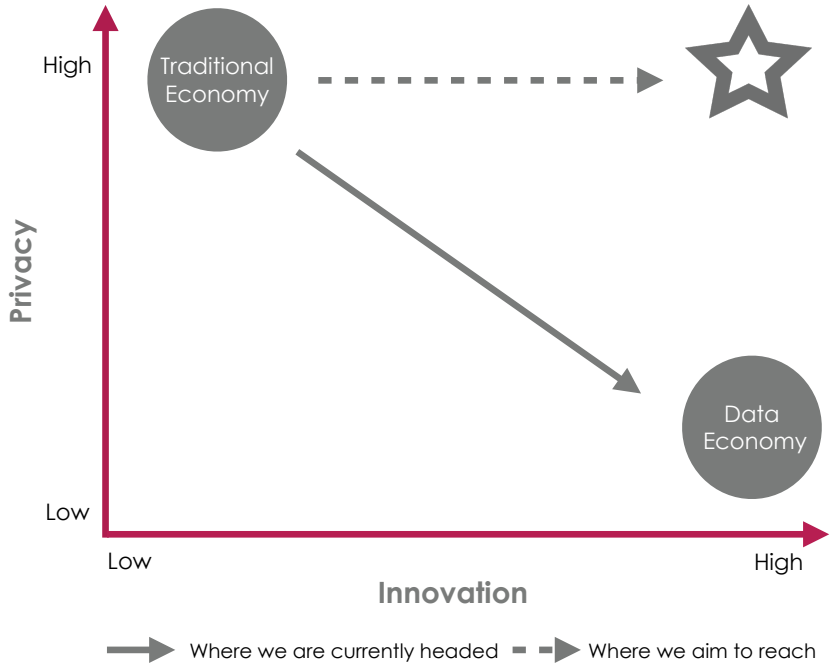
b) Efforts by businesses: Steps that businesses take to protect and safeguard consumers' private information.

The first variable involves increasing awareness and understanding by consumers on how their personal information is collected, used, and shared. After receiving appropriate literacy education, consumers should be able to translate their knowledge into actual behaviour – such as changing their online settings to suit their privacy preferences. The second variable calls for greater efforts by businesses to put privacy controls in the hands of consumers. This can entail using badges or privacy meters to help consumers assess and compare risk levels, making prominent features that remind consumers to verify their privacy settings, as well as investing more in secure data management systems.

We believe that the development of a "privacy dashboard" and related privacy metrics is crucial for several reasons. First, as business pundits and academic research suggest, "whatever is measurable will be attended to." Knowing that privacy efforts are being measured and scaled will make it more likely that companies will invest additional effort. Second, from a consumers' perspective, measurement will allow them to make more informed, and consequently better choices. Third, the development of a standard dashboard will better allow researchers, policy makers and businesses alike to document the effects of various interventions and policies.

Is the decline of consumer privacy a necessary cost to the development of innovative products and solutions? As we progress from the traditional economy characterized by less innovation and higher levels of privacy, to one led by the data revolution with ample opportunities for innovation, should privacy levels necessarily fall? We believe that if governments and businesses work with consumer groups to build up the three pillars described in the report (equip the consumer, pad the environment, incentivize businesses), the data revolution can deliver all of its promises without compromising the safety of consumers who are enabling it. Figure 7.1 illustrates the direction we hope to see in innovation and privacy headed over the coming years. We can aim to reach the ideal situation – indicated by the star – where online transactions and innovation arising from the data collected are not reduced by privacy efforts, but rather enhanced through higher consumer confidence in the online space.

Figure 7.1. The Privacy – Innovation Grid



References

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. *Proceedings of the fifth ACM conference in electronic commerce (EC '04)*, 21–29.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514.

Acquisti, A., & Grossklags, J. (2007). What can behavioral economics teach us about privacy? *Digital Privacy: Theory, Technologies, and Practices*, 363–377.

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth? *The Journal of Legal Studies, 42*(2), 249–274.

Albergotti, R. (2014, September 4). Facebook rolls out privacy checkups to all 1.3 billion users. *Wall Street Journal*. Retrieved from http://blogs.wsj.com/digits/2014/09/04/facebook-rolls-out-privacy-checkups-to-all-1-3-billion-users/

Bora, K. (2015, July 20). Ashley Madison Hack: Sensitive Data Leaked, Hackers Threaten To Post Customer Details If Site Does Not Go Offline. *International Business Times*. Retrieved from http://www.ibtimes.com/ashley-madison-hack-sensitive-data-leaked-hackers-threaten-post-customer-details-if-2015385

BBC News. (2014, September 8). Blue dinosaur to help Facebook privacy push. *BBC News*. Retrieved from http://www.bbc.com/news/technology-29111393

Benchley, R. S. (2013). Big data: Turning insight into action. *BusinessMiami* (Fall 2013).

Brown, E. (2015, August 19). New social network ETER9 brings AI to your interactions. *ZDNet*. Retrieved from http://www.zdnet.com/article/new-social-network-eter9-brings-ai-to-your-interactions/

Canadian Anti-Fraud Centre. (2014). Annual statistical report 2014. Retrieved from http://www.antifraudcentre-centreantifraude.ca/reports-rapports/2014/ann-ann-eng.htm#a1

Chang, R. D., Fang, C. J., & Tseng, Y. C. (2012). The effects of WebTrust assurance on consumers' web purchase decisions: An experiment. *Online Information Review, 36*(2), 218–240.

Cranor, L. F., McDonald, A. M., Egelman, S., & Sheng, S. (2007). 2006 Privacy policy trends report.

Dean, J. (2015, June 24). Facebook can identify its faceless users. *The Times*. Retrieved from http://www.thetimes.co.uk/tto/technology/internet/article4478251.ece

DLA Piper. (2014). Data protection laws of the world. Retrieved from http://dlapiperdataprotection.com/#handbook/world-map-section

Dolan, P., Hallsworth, M., Halpern, D., King, D., Metcalfe, R., & Vlaev, I. (2012). Influencing behaviour: The mindspace way. *Journal of Economic Psychology, 33*(1), 264–277.

Duhigg, C. (2012, February 16). How companies learn your secrets. *The New York Times Magazine*. Retrieved from http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=0

Edelman, B. (2010). Adverse selection in online "trust" certifications and search results. *Electronic Commerce Research and Applications.* doi:10.1016/j.elerap.2010.06.001

Electronic Frontier Foundation. (2014, November 6). *Secure messaging scorecard*. Retrieved from https://www.eff.org/secure-messaging-scorecard

Electronic Frontier Foundation. (2015). *Who has your back?* Retrieved from https://www.eff.org/who-has-your-back-government-data-requests-2015

European Commission. (2012). How does the data protection reform strengthen citizens' rights? Retrieved from

http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf

Faguy, Y. (2014, November 11). Privacy in the age of big data. *National*. Retrieved from http://www.nationalmagazine.ca/Articles/November-2014-Web/Privacy-in-the-age-of-Big-Data.aspx

Greenberg, A. (2015, July 15). Senate bill seeks standards for cars' defenses from hackers. *Wired*. Retrieved from http://www.wired.com/2015/07/senate-bill-seeks-standards-cars-defenses-hackers/

Harvard Business Review Staff. (2014, November). With big data comes big responsibility. *Harvard Business Review*. Retrieved from https://hbr.org/2014/11/with-big-data-comes-big-responsibility

Hill, K. (2011, August 1). How facial recognition technology can be used to get your Social Security number. *Forbes*. Retrieved from http://www.forbes.com/sites/kashmirhill/2011/08/01/how-face-recognition-can-be-used-to-get-your-social-security-number/

Hsee, C. K. (1996). The evaluability hypothesis: An explanation for preference reversals between joint and separate evaluations of alternatives. *Organizational Behavior and Human Decision Processes, 67*(3), 247–257.

Hu, X., Wu, G., Wu, Y., & Zhang, H. (2010). The effects of web assurance seals on consumers' initial trust in an online vendor: A functional perspective. *Decision Support Systems, 48*(2), 407–418.

John, L. K. (2015). The consumer psychology of online privacy. Working Paper.

Kahneman, D. (2011). *Thinking, fast and slow*. UK: Penguin Books Ltd.

Kahneman, D., Knetsch, J. L., & Thaler, R. H. (1991). Anomalies: The endowment effect, loss aversion, and status quo bias. *The Journal of Economic Perspectives*, 193–206.

Kelion, L. (2015, June 1). Google overhauls privacy and security settings. *BBC News*. Retrieved from http://www.bbc.com/news/technology-32958765

Kelley, P. G., Bresee, J., Cranor, L. F., & Reeder, R. W. (2009). A nutrition label for privacy. *Proceedings of the 5th symposium on usable privacy and security*.

Lardinois, F. (2015, April 3). Microsoft will remove "do not track" as the default setting in its new browsers. *TechCrunch.* Retrieved from http://techcrunch.com/2015/04/03/microsoft-disables-do-not-track-as-the-default-setting-in-internet-explorer/

LaRose, R., & Rifon, N. J. (2007). Promoting i-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *Journal of Consumer Affairs, 41*(1), 127–149.

Lomas, N. (2015, June 18). EFF's 2015 data privacy report lauds Apple, Dropbox, slams Verizon. *TechCrunch.* Retrieved from http://techcrunch.com/2015/06/18/eff-2015-data-report/#.ifzsyv:gRj2

Madden, M., Fox, S., Smith A., & Vitak, J. (2007, December 16). Digital Footprints: Online identity management and search in the age of transparency. *Pew Research Center*. Retrieved from http://www.pewinternet.org/files/old-media/Files/Reports/2007/PIP_Digital_Footprints.pdf.pdf

Mann, T., & Ward, A. (2007). Attention, self-control, and health behaviors. *Current Directions in Psychological Science, 16*(5), 280–283.

Mazowita, B., & Vézina, M. (2014). Police-reported cybercrime in Canada, 2012. *Statistics Canada*.

McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *A Journal of Law and Policy for the Information Society.*

Morey, T., Forbath, T. T., & Schoop, A. (2015). Customer data: Designing for transparency and trust. *Harvard Business Review, 93*(5), 96–105.

Northcott, M. (2012). Identity-related crime: What it is and how it impacts victims. *Victims of Crime Research Digest, 5*, 7–12.

Noyes, K. (2015, January 15). Will big data help end discrimination – or make it worse? *Fortune*. Retrieved from http://fortune.com/2015/01/15/will-big-data-help-end-discrimination-or-make-it-worse/

O'Donoghue, T., & Rabin, M. (1999). Doing it now or later. *American Economic Review, 89*(1), 103–124.

Office of the Privacy Commissioner of Canada. (2013, May). The case for reforming the Personal Information Protection and Electronic Documents Act. *Government of Canada*. Retrieved from http://publications.gc.ca/site/eng/9.698355/publication.html

Office of the Privacy Commissioner of Canada. (2014, March). Privacy toolkit: A guide for businesses and organizations. Retrieved from https://www.priv.gc.ca/information/pub/guide_org_e.asp

Phoenix SPI. (2014, December). 2014 survey of Canadians on privacy prepared for the Office of the Privacy Commissioner of Canada.

Quick, M., Hollowood, E., Miles, C., & Hampson, D. (2015). World's biggest data breaches. *Information is Beautiful.* Retrieved from http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Quirk, M. B. (2014, February 11). Mozilla to display ads within Firefox. *Consumerist*. Retrieved from http://consumerist.com/2014/02/11/mozilla-goes-from-blocking-third-party-ads-by-default-to-displaying-ads-within-firefox/

Rundle, M. (2015, July 27). "Stagefright" Android bug is the "worst ever discovered." *Wired.* Retrieved from http://www.wired.co.uk/news/archive/2015-07/27/stagefight-android-bug

Salehan, M., Kim, D. J., & Lee, J. N. (2015). Antecedents, processes and consequences of web assurance seals: A meta-analysis approach. Paper presented at Pacific Asia Conference on Information Systems.

Simon, P. A., Leslie, P., Run, G., Jin, G. Z., Reporter, R., Aguirre, A., & Fielding, J. E. (2005). Impact of restaurant hygiene grade cards on foodborne-

disease hospitalizations in Los Angeles County. *Journal of Environmental Health, 67*, 32–36.

Schneider, A., & Ingram, H. (1990). Behavioral assumptions of policy tools. *The Journal of Politics, 52*(02), 510–529.

Schrage, M. (2014, January 29). Big data's dangerous new era of discrimination. *Harvard Business Review*. Retrieved from https://hbr.org/2014/01/big-datas-dangerous-new-era-of-discrimination/

Soergel, A. (2014, November 7). 53 million email addresses stolen in Home Depot hack. *U.S. News & World Report.* Retrieved from http://www.usnews.com/news/newsgram/articles/2014/11/07/53-million-customer-email-addresses-leaked-in-home-depot-hack

Sterman, J. D. (1989). Modeling managerial behavior: Misperceptions of feedback in a dynamic decision making experiment. *Management Science, 35*(3), 321-339.

Tannenbaum, D., & Ditto, P. H. (2011). Information asymmetries in default options. Working Paper in preparation for submission to *Organizational Behavior and Human Decision Processes*.

Thompson, S. A., Krashinsky, S., & Dingman, S. (2014, February 24). How big data profits from your personal information. *The Global and Mail*. Retrieved from http://www.theglobeandmail.com/globe-debate/follow-your-data-from-your-phone-to-the-marketplace/article17056305/

Timberg, C. (2013, June 19). Firefox web browser to move ahead plan to block tracking. *The Washington Post*. Retrieved from http://www.washingtonpost.com/business/technology/firefox-browser-to-move-ahead-with-do-not-track/2013/06/19/b0ad618c-d8f6-11e2-a9f2-42ee3912ae0e_story.html

Yalch, R. F., & Elmore-Yalch, R. (1984). The Effect of Numbers on the Route to Persuasion. *Journal of Consumer Research*, 522–527.

Appendices

Rotman School of Management
UNIVERSITY OF TORONTO

Appendix A

The 10 fair information principles under the Personal Information Protection and Electronic Documents Act (PIPEDA)

Be accountable	Organizations are responsible for complying with PIPEDA's principles by developing and implementing proper policies and practices. The accountability for protection holds for all personal information transferred to a third party for processing.
Identify the purpose	Individuals must be informed of the reasons for collecting information before or at the time of collection.
Obtain informed consent	Organizations must inform consumers in a meaningful way the purposes for the collection, use, and disclosure of personal data. If there is a new purpose for the information, consent by the individual is required before use.
Limit collection	Information should not be collected indiscriminately, and consumers must not be deceived or misled about the reasons for collection.
Limit use, disclosure, and retention	Personal data should be used and disclosed only for the purposes for which it was collected, and that information should be kept only as long as necessary to satisfy the purposes. Any data that is no longer required must be deleted or rendered anonymous.
Be accurate	By keeping information accurate and up to date, organizations must minimize the possibility of using incorrect information when making a decision about the individual or disclosing data to third parties.
Use appropriate safeguards	Appropriate safeguards must be in place to protect information against loss, theft, unauthorized access, disclosure, or use.
Be open	Organizations must be open about their information management policies and practices, and make them easy for consumers to understand and access.
Give individuals access	Individuals have a right to access the personal information that an organization holds about them.
Provide recourse	Simple and easily accessible complaint procedures must be available for consumers. Further, all complaints received must be investigated, and appropriate measures must be taken by organizations to correct information handling practices.

Source: Office of the Privacy Commissioner of Canada. (2014, March). Privacy Toolkit: A Guide for Businesses and Organizations. Retrieved from https://www.priv.gc.ca/information/pub/guide_org_e.asp

Appendix B

Key changes of General Data Protection Regulation (GDPR) from the EU's current data protection framework

In 2012, the European Commission published a draft of the GDPR to signal the start of a legislative process that would unify data protection rules in Europe. Unlike the existing 1995 Data Protection Directive, where each state passed their own modified legislations, this regulation will have immediate effect on all 28 EU member states after a two-year transition period. The enactment of GDPR is expected to be early 2016, and the rules are expected to apply in the first half of 2018. Below are the key changes:

1. A "right to be forgotten," whereby consumers can require their data to be deleted if there are no legitimate grounds for retaining it.
2. Easier access to personal data collected by organizations.
3. Easier transfer of personal data from one service provider to another.
4. When consent is required, consumers must be asked to give it explicitly.
5. More transparency about how consumers' data is handled, with easy-to-understand information, especially for children.
6. Businesses and organizations will need to inform consumers about data breaches that could adversely affect individuals without undue delay, within 24 hours where feasible. The relevant data protection authority will also be notified.
7. Improved administrative and judicial remedies in cases of violation of data protection rights.
8. Increased responsibility and accountability for those processing personal data – through data protection risk assessments, data protection officers, and the principles of "privacy by design" and "privacy by default."

Source: European Commission. (2012). How does the data protection reform strengthen citizens' rights? Retrieved from http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf