ONLINE PRIVACY PROTECTION

Consumers as Agents

union des consommateurs

Final report of the research project presented by Union des consommateurs to the Office of Consumer Affairs of innovation, Science and Economic Development Canada

October 2021

THE TEAM

PRODUCTION OF THE REPORT

Union des consommateurs

RESEARCH AND WRITING

Anaïs Beaulieu-Laporte

EDITORIAL MANAGEMENT

Marcel Boucher

TRANSLATION

Moderna Reg'd – Mark Manning

COLLABORATION

Our thanks to Professors Ignacio Cofone and Céline Castets-Renard as well as Ms. Cynthia Chassigneux and Mr. Julien Lamalice.

7000 du Parc Avenue, Suite 201
Montreal, Quebec H3N 1X1
Telephone: 514 521-6820
Fax: 514 521-0736
info@uniondesconsommateurs.ca
www.uniondesconsommateurs.ca

Member organizations of Union des consommateurs:

ACEF Appalaches Beauce Etchemins
ACEF de l'Île Jésus
ACEF du Nord de Montréal
ACEF Estrie
ACEF Montérégie-Est
ACQC
CIBES de la Mauricie
ACEF de l'Est de Montréal
ACEF du Grand-Portage
ACEF du Sud-Ouest de Montréal
ACEF Lanaudière
ACEF Rive-Sud de Québec
Centre d'éducation financière
OBC
SAC de la Mauricie

THE REPORT

Union des consommateurs received funding from Innovation, Science and Economic Development Canada's Contributions Program for Non-profit Consumer and Voluntary Organizations. The views expressed in this report are not necessarily those of Innovation, Science and Economic Development Canada or the Government of Canada.

The masculine is used generically in this report.

UNION DES CONSOMMATEURS,

Strength through Networking

Union des consommateurs is a non-profit organization comprised of 14 consumer rights groups.

UC's mission is to represent and defend the rights of consumers, with special emphasis on the interests of low-income households. Its activities are based on values cherished by its members: solidarity, equity and social justice, and improving consumers' economic, social, political and environmental living conditions.

UC's structure enables it to maintain a broad vision of consumer issues while developing in-depth expertise in certain programming sectors, particularly via its research efforts on the emerging issues confronting consumers. Its activities, which are nation-wide in scope, are enriched and legitimated by its field work and the deep roots of its member associations in their communities.

Union des consommateurs acts mainly at the national level, by representing the interests of consumers before political or regulatory authorities, in public forums or through class actions. Its priority issues, in terms of research, action and advocacy, include the following: household finances and debt, energy, issues related to telecommunications, broadcasting, cable television and the Internet, health, financial products and services, as well as social and fiscal policies.

TABLE OF CONTENTS

GLOSSARY

Some basic digital terms [1]

English terms	French terms and better-known English terms	
Internet	Internet	A worldwide computer network made up of a multitude of networks (public and private), which allows, from a local connection, communication between computers and servers using standardized protocols.
World Wide Web (www)	*World Wide Web* (www)	An Internet application that enables Internet navigation by means of a hypertext system. By extension, the Web is generally understood as the set of websites accessible through this application.
IP address	Adresse IP	A unique number used to identify and locate a device connected to the Internet.
Operating system	Système d'exploitation	Software used to manage the operation of a device (computer, smartphone, tablet, "connected object") and the execution of its programs.
Application	Application	Software or programs used by an Internet user to perform a specific task or activity using a device.
Browser	Navigateur	Software used for viewing websites and accessing search engines.
Search engine	Moteur de recherche	A program that indexes the content of websites and is used for searching and accessing content based on keywords.
Plug-in / Extension module / Browser extension	Module d'extension / Extension de navigation / *Plug-in*	Software that is grafted onto other software to offer new features.

[1] OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE. Le grand dictionnaire terminologique, online: http://gdt.oqlf.gouv.qc.ca/index.aspx; LAROUSSE. French dictionary, online: https://www.larousse.fr/ THE TRANSLATION BUREAU OF CANADA. Termium Plus, online: https://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-eng.html?lang=eng&index=alt; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. Technology, online: https://www.priv.gc.ca/en/privacy-topics/technology/

Widget	Objet-fenêtre / *Widget*	A small application that integrates directly into a Web page or operating system and offers additional content (e.g. calendar, weather).
Big data	Mégadonnées / *Big data*	A large set of data from multiple sources and in a variety of formats that can be cross-processed to provide new opportunities for exploration, cross-referencing and inference.
Algorithm	Algorithme	A sequence of instructions or operations applied to data in order to solve a problem, draw inferences, etc.
Artificial Intelligence (AI)	Intelligence artificielle (IA) / *AI*	A system designed to enable a machine to reproduce human cognitive faculties (e.g. recognition, analysis, calculation).
Encryption	Chiffrement / Cryptage	Transformation of a clear text into an unintelligible text that cannot be used by anyone who does not have the decryption key.
Cookie	Témoin / *Cookie*	A small file that is sent by a server to the browser when a website is visited and that stores data about the user's use of the website. Sometimes described as the browser's memory.
Pop-up window / Pop-up	Fenêtre publicitaire ou contextuelle / *Pop-up*	An unsolicited advertising window that opens automatically on some websites.

Some legal acronyms

Francophones	Anglophones	
-	*APIPA*	*Personal Information Protection Act* (Alberta law)
-	*BCPIPA*	*Personal Information Protection Act* (British Columbia law)
CAI	-	Commission d'accès à l'information (Quebec)
-	*CCPA*	*California Consumer Privacy Act of 2018*
OPC	OPC	Office of the Privacy Commissioner of Canada / Commissariat à la protection de la vie privée du Canada
	FTC	Federal Trade Commission (United States)
GT Art. 29	Art. 29 WP	Article 29 Working Party (replaced by the European Data Protection Board (EDPB/EDPS))

LCAP	*CASL*	*Loi canadienne anti-pourriel / Canada's anti-spam legislation*
LPRPDE	*PIPEDA*	*Loi sur la protection des renseignements personnels et les documents électroniques / Personal Information Protection and Electronic Documents Act (Canadian law)*
LPRPSP	*APPIPS*	*Loi sur la protection des renseignements personnels dans le secteur privé / Act respecting the protection of personal information in the private sector* (Quebec law)
LPVPC	*CPPA*	*Loi sur la protection de la vie privée des consommateurs / Consumer Privacy Protection Act* (legislation developed in Canada's Bill C-11)
LPRPPVI	*PIPITPA*	*Loi sur la protection des renseignements personnels et la prévention du vol d'identité / Personal Information Protection and Identity Theft Prevention* Act (Manitoba)
RGPD	*GDPR*	*Règlement général sur la protection des données / General Data Protection Regulation* (EU regulation)

INTRODUCTION

Canadians are using the Internet more than ever before. They use it to work, study, obtain information, have fun, shop, interact with others, access and create content.

With some 1.88 billion websites[2], the Internet allows access and dissemination of information on a completely different scale than before. 1.2 billion searches are performed on *Google* every year[3]. 70 million publications are presented each month on the *WordPress*[4] website and blog platform. More than 306 billion emails are exchanged daily[5]. Nearly 350,000 ephemeral posts are shared on *Instagram* every minute[6].

Those numbers are staggering. They can also be a cause for concern.

Indeed, the advent of the Internet and its widespread use are not without consequences for the exercise of human rights, particularly the right to privacy. Experts estimate that by 2025, nearly 463 trillion bytes (the equivalent of 212,765,957 DVDs) of data will be generated every day on the network[7]. Amid this data, we find a lot of personal information, information collected, exploited or sold by companies, while the people concerned have very little control over those activities.

This situation is of growing concern to consumers according to numerous surveys conducted in recent years. However, those surveys are generally American and European. Do they reflect the point of view of Canadian consumers? Our research aims to provide a Canadian perspective on this issue. What are Canadian consumers concerned about online? Are their privacy and personal information adequately protected online, either through the safeguards they adopt or through Canadian laws that are supposed to ensure that?

This report is divided into six parts. First, we will attempt to define what privacy is, based on the definitions proposed by certain authors and on the conceptions of privacy adopted by the European, American and Canadian legal systems.

The second and third parts of the report will document consumers' concerns about their online privacy and personal information, and the protective measures and behaviours they

---

[2] Estimates range from 1.7 billion to 1.88 billion websites: ARMSTRONG, M. "How Many Websites Are There?," Statista, August 6, 2021, online: https://www.statista.com/chart/19058/number-of-websites-online/; WEBSITESETUP. "How Many Websites Are There in 2021?," online: https://www.statista.com/chart/19058/number-of-websites-online/ (consulted on October 6, 2021).
[3] INTERNET LIVE STATS. "Google Search Statistics," online: https://www.internetlivestats.com/google-search-statistics/ (consulted on October 6, 2021).
[4] WORDPRESS. "A live look at activity across WordPress.com," online: https://wordpress.com/activity/ (consulted on October 6, 2021).
[5] STATISTA. "Number of sent and received emails per day worldwide from 2017 to 2025," April 7, 2021, online: https://www.statista.com/statistics/456500/daily-number-of-emails-worldwide/
[6] *Stories* publications: STATISTA. "Media usage in an internet minute as of August 2020," online: https://www.statista.com/statistics/195140/new-user-generated-content-uploaded-by-users-per-minute/ (consulted on October 6, 2021).
[7] DESJARDINS, J. "How much data is generated each day?," World Economic Forum, April 17, 2019, online: https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/

adopt to safeguard it. In particular, we will report the results of a survey and interviews among Canadian consumers that were conducted in the winter of 2020. We will also briefly discuss the online privacy paradox as debated in the literature.

In the fourth part, we will examine online privacy-enhancing technologies, which are strongly recommended by experts, but are apparently still unknown to Canadian Internet users. We will analyze the presentation of the various tools available online to see how much it enables Canadian consumers to understand the usefulness of those tools and to dispel distrust toward them.

That will be followed by an analysis of existing privacy legislation in Canada. There are currently four pieces of legislation applicable to the private sector: one federal and three provincial. We will look at how those laws address issues of concern to consumers, if at all. We will also examine the laws' compatibility with the actual online behaviour of Canadian consumers, as revealed by our investigations.

In the sixth and final part of this document, we will report the views of experts from the Canadian academic community who were consulted in the course of this research. What do they think of the Canadian legislative approach? How it deals with consumer responsibility and consent? The experts address a variety of aspects that legislators will have to take into account in the upcoming revision of Canadian laws that many now consider outdated.

The findings of our research will be followed by our recommendations.

It should be noted that this study focuses on the protection of Internet users' privacy with respect to the private and consumer sector and does not address considerations relating to potential breaches by the state (police surveillance, profiling for political purposes, etc.) or by other actors in a position of authority (employer, landlord, etc.).

PRIVACY: BACKGROUND INFORMATION

Defining privacy is complex. This is evidenced by the fact that authors and disciplines have produced a variety of definitions over time. Some of the contemporary conceptions of privacy will be discussed in this chapter, but first it is useful to briefly outline the historical progression of individuals' quest for privacy.

1.1 A Short History of Privacy

The concept of privacy reportedly appeared toward the end of the Middle Ages, when the private realm gradually began to be distinguished from the public realm. Before that, the individual was part of a community with whom he shared all his possessions and made all his decisions[8].

With the rise of individualism in 18th century England, the concept of privacy became more important[9]. Several privacy areas were recognized, such as the family, the diary, the office (the "study") or the wardrobe[10]. The popularization and democratization of reading also contributed to the development of a greater sense of personal autonomy[11]. But the search for solitude and the desire to be out of sight were still very much frowned upon[12].

The subsequent emergence of tabloid newspapers that publicized gossip about public figures gave rise to the first tensions between privacy and communications technology[13] – a tension that is still very much with us today.

The 19th century led to the enshrinement of privacy by the individualization process that persists to this day (because of medical and hygienic progress for example), by the importance attached to domestic life, and by urbanization (given the new proximity to neighbours)[14].

---

[8] "Vie privée ?," L'Influx, December 2013, online: http://www.linflux.com/societe/droit-justice/vie-privee/#
It should be noted that some authors refer to the writings of Aristotle and other Greek thinkers to establish that the concept of privacy was already present in antiquity, in that a distinction was made between the notions of *oikos* (family) and *polis* (public and political sphere). Note, however, that the *oikos* differs considerably from the family home as it is understood today: KEULEN, S. and KROEZE, R. "Privacy from a Historical Perspective" in VAN DER SLOOT, B. and DE GROOT, A., eds., *The Handbook of Privacy Studies: An Interdisciplinary Introduction*, Amsterdam University Press, 2018, p.24.
[9] KEULEN and KROEZE. "Privacy from a Historical Perspective," *supra* note 8, pp. 24-25.
[10] *Ibid.*, pp. 25-26.
[11] *Ibid.*, p.26.
[12] *Ibid.*, pp. 25-26.
[13] *Ibid.*, pp. 27 and 31-32.
[14] LUKÁCS, A. "What is privacy? The history and definition of privacy," 2016, p. 257, online: https://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf; LEPORE, J. "The Prism: Privacy in an Age of Publicity," The New Yorker, June 24, 2013, online: https://www.newyorker.com/magazine/2013/06/24/the-prism

The rise of liberalism following the First World War would again confirm the importance of privacy for individuals, this time in opposition to the state. The latter modernized and offered more support and services to its citizens (including a social safety net), but in exchange imposed surveillance and disclosure of personal information[15].

Lastly, the development of the Internet and the World Wide Web in the 1980s and 1990s, and the recent technological innovations that have resulted from them, are once again changing the environment and daily life of individuals and influencing their perception of privacy and the potential threats to which it is subject.

> Changes in modern communication techniques, from the printing press and telephone to the computer and Internet, have had a great impact on the way privacy was understood as well. All these changes have made privacy a slippery concept that is difficult to grasp in general terms[16].

1.2 How to Define Privacy?

There is no universal definition of privacy[17]. Without being exhaustive, this section aims to present the perspectives of a selection of authors on the subject. We also discuss the approaches taken by the European, American and Canadian legal systems to the notion of privacy.

1.2.1 Many definitions proposed over time

There are two main conceptions of privacy in the literature. One is more related to the concept of isolation from the public space and the other to the concept of control. From those concepts, privacy can take various more specific forms according to the authors who lend themselves to the difficult exercise of defining privacy.

1.2.1.1 A question of isolation from the public space

Warren and Brandeis provided the best-known definition of privacy in 1890; their article in the *Harvard Law Review* is considered one of the most influential legal articles of all time[18].

---

[15] KEULEN and KROEZE. "Privacy from a Historical Perspective," *supra* note 8, p. 34.
[16] *Ibid.,* p. 40.
[17] LUKÁCS, A. "What is privacy?," *supra* note 14, pp. 256-258.
[18] *Ibid.,* pp. 257-258; BRATMAN, B. E. "Brandeis and Warren's The Right To Privacy and the Birth of the Right to Privacy," Tennessee Law Review vol. 69, 2002, p. 624; HOLVAST, J. "History of Privacy" in MATYÁŠ, V. *et al*, eds., The Future of Identity in the Information Society, IFIP Advances in Information and Communication Technology, vol. 298, 2009, p. 18; WALDMAN, A. Privacy as Trust: Information Privacy for an Information Age, Cambridge University Press, 2018, p. 11.

According to these two American lawyers, privacy is defined as the right to be left alone[19]. The individual must be able to have a private space to develop his beliefs and opinions, without fearing the judgment of others and the pressures of his community[20].

The authors are particularly critical of journalists and the snapshot photos that regularly accompany articles in the tabloids of the time[21]. According to the authors, that undesirable exposure of individuals to the masses' attention ultimately harms individuals' ability to develop and is responsible for the decline of morality in society[22].

Since the publication of Warren and Brandeis' article, many authors have been inspired by it to propose a revisited definition of privacy centred around the limited access of others to oneself[23].

Gavison states, for example, that:

> I suggest that an individual enjoys perfect privacy when he is completely inaccessible to others. This may be broken into three independent components: in perfect privacy no one has any information about X, no one pays any attention to X, and no one has physical access to X. Perfect privacy is, of course, impossible in any society. The possession or enjoyment of privacy is not an all or nothing concept, however, and the total loss of privacy is as impossible as perfect privacy[24].

The author identifies three elements related to the limited access of others to oneself: solitude, anonymity and secrecy[25]. This last element has been specifically retained by some, such as Judge Posner and the author Parent, who conceive of privacy as keeping an individual's personal information secret[26]. For Parent, physical access to individuals becomes secondary since Warren and Brandeis' desire for peace and tranquility would now be fulfilled by the contemporary Western lifestyle[27]. And Posner in turn refers to another concept relevant to his definition of privacy: the protection of individuals' reputation. If personal information must be kept secret, it is to ensure the reputation of each and every one of us[28].

---

[19] WARREN, S. D. and BRANDEIS, L. D. "The Right to Privacy," Harvard Law Review, vol. 4, No. 5, December 15, 1890, p. 195. This expression was first used by Justice Thomas Cooley in a book on common law *torts* ten years before Brandeis and Warren's article: SOLOVE, D. J. "Conceptualizing privacy," California Law Review, vol. 90, No. 4, 2002, p. 1100.
[20] BEZANSON, R. P. "The Right to Privacy Revisited: Privacy, News, and Social Change, 1890-1990," California Law Review, vol. 80, No. 5, October 1992, p. 1134.
[21] WARREN and BRANDEIS. "The Right to Privacy," *supra* note 19, p. 213; BRATMAN. "Brandeis and Warren's The Right To Privacy," *supra* note 18, pp. 624-630; LUKÁCS. "What is privacy?," *supra* note 14, pp. 257-258.
[22] BEZANSON. "The Right to Privacy Revisited," *supra* note 20pp. 1138-1139.
[23] SOLOVE. "Conceptualizing privacy," *supra* note 19, pp. 1102.
[24] GAVISON, R. "Privacy and the Limits of Law," The Yale Law Journal, vol. 89, No. 3, 1980, p. 428.
[25] *Ibid.*
[26] According to Posner, privacy is an individual's right to keep discrediting information about himself secret: POSNER, R. A., The Economics of Justice, Harvard University Press, 1983.
According to Parent, privacy is "the condition of not having undocumented personal information about oneself known by others": PARENT, W. A. "A New Definition of Privacy for the Law," Law and Philosophy, vol. 2, No. 3, 1983, p. 306.
[27] POSNER, R. A. "Privacy, Secrecy, and Reputation," Buffalo Law Review, vol. 28, 1979, pp. 4-5.
[28] *Ibid.* pp. 5-6.

It is worth noting that secrecy-based conceptions of privacy have been criticized by many for their simplistic distinction between private and public information[29]. Does personal information lose its privacy once it is disclosed directly or indirectly to someone? The general physical characteristics and capabilities of an individual who is in the public arena are disclosed to the public. And an individual presumably leaves biological traces in his wake (DNA, hair, etc.). Does that information then become public? An affirmative answer to that question is certainly difficult to support and seems rather inappropriate for today's times.

> When understood as a right to separate and exclude, privacy vanishes the moment we let others in. That erases privacy in today's technology-driven world, where some amount of disclosure of data is inevitable and often mandatory[30].

1.2.1.2 A question of control

There is a second school of thought that is more focused on the concept of control. Privacy would not be linked to the capacity of each individual to isolate himself from the rest of society, but to his capacity to determine to whom and what he gives access[31]. Gerety writes for example about the autonomy exercised by each individual regarding the privacy of his personal identity[32].

Moore, on the other hand, restricts his definition of privacy to a person's control over others' access to himself and his personal information[33]. While this definition may seem similar to Gavison's definition of limited access by others to oneself, it differs in that the focus is on the control that is exercised, not the outcome. Thus, an individual who allows broad public access to different facets of his person would theoretically maintain his privacy, according to Moore, as long as the extent of that access resulted from his own choices[34].

More restrictive, the Westin and Fried definitions are limited to control over personal information disclosed to others[35].

> Privacy, thus, is control over knowledge about oneself. But it is not simply control over the quantity of information abroad; there are modulations in the quality of the knowledge as well[36].

In addition to control over access to the individual and his personal information, some authors have added a third component to the definition of privacy: the ability to make

---

[29] MOORE, A. D. "Privacy: Its Meaning and Value," American Philosophical Quarterly, vol. 40, July 2003, p. 218; SOLOVE. "Conceptualizing privacy," *supra* note 19, p. 1107.
[30] WALDMAN. Privacy as Trust, *supra* note 18p. 26.
[31] FRIED, C. "Privacy," The Yale Law Journal, vol. 77, 1968, p. 482.
[32] GERETY, T. "Redefining Privacy," Harvard Civil Rights-Civil Liberties Law Review, vol. 12, No. 2, 1977, p. 236.
[33] MOORE. "Privacy," *supra* note 29, p. 218; MOORE, A. "Defining Privacy," Journal of Social Philosophy, vol. 39, No. 3, 2008, p. 420.
[34] AUSTIN, L. M. "Rereading Westin," Theoretical Inquiries in Law, vol. 20, No. 1, 2019.
[35] *Ibid.* SOFFER, T. and COHEN, A. "Privacy Perception of Adolescents in a Digital World," Bulletin of Science, Technology & Society, vol. 34, No. 56, Oct. 1, 2014, p. 147; FRIED, C. "Privacy," *supra* note 31p. 483.
[36] FRIED. "Privacy," *supra* note 35, p. 483.

important decisions about one's lifestyle and family[37]. In this regard, it should be noted that the right to abortion has historically been associated with the right to privacy in the United States[38].

Like the definition of access, the definition of privacy that focuses on control has been criticized for being circular:

> Gavison and other critics of the assumption that privacy functions through control contend that this assumption makes it impossible to escape from within privacy because every choice is an exercise of control[39].

1.2.1.3 Perspectives that have much in common

From this overview of the major definitions of privacy, it is clear that there are some similarities between them, particularly with respect to their close connection to the concept of freedom.

Thus, definitions of privacy generally derive from a recognition of each individual's freedom, a freedom that is addressed in different ways:

> Today, the function of privacy relating to freedom of the individual as an individual is the dominant one; the function of privacy relating to social control is greatly diminished. The freedoms protected by today's more individualistic idea of privacy are of two sorts: freedom from intrusiveness and freedom to achieve identity[40].

The definitions of privacy also have in common their approach based on the recognition of a fundamental right of individuals[41]. There are, however, some authors, such as Lessig, who disagree with this analysis and believe that privacy is more a matter of property[42]. Others, such as Jarvis Thomson, do not conceive of privacy as a right in itself, but rather as the product or amalgam of a multitude of rights.

> For if I am right, the right to privacy is "derivative" in this sense: it is possible to explain in the case of each right in the cluster how come we have it without ever once mentioning the right to privacy. Indeed, the wrongness of every violation of the right to privacy can be explained without ever once mentioning it[43].

---

[37] STANFORD ENCYCLOPEDIA OF PHILOSOPHY. "Privacy," online: https://plato.stanford.edu/entries/privacy/#VieMeaValPri
[38] *Roe* v *Wade*, 410 U.S. 113.
[39] INNESS, J. C. Privacy, Intimacy, and Isolation, Oxford University Press, 1996, p. 52.
[40] BEZANSON. "The Right to Privacy Revisited," *supra* note 20p. 1144.
[41] WALDMAN. Privacy as Trust, *supra* note 18p. 11.
[42] See for example: LESSIG, L. "Privacy as Property," Social Research, vol. 69, No. 1, spring 2002, pp. 257-262.
[43] JARVIS THOMSON, J. "The Right to Privacy," Philosophy & Public Affairs, vol. 4, No. 4, 1975, p. 313.

1.2.1.4 The different dimensions of privacy

Given the complexity that interferes with any attempt to define privacy on a single conceptual basis, some authors have instead attempted to define it by identifying its different dimensions or elements[44].

In practice, it will be noted that the authors who have carried out this exercise substantially echo the perspectives of the authors mentioned above, but under different classifications, which supports the thesis of a complementarity of possible definitions of privacy.

Examples of the dimensions identified include:

Table 1
The dimensions of privacy according to a selection of authors

<table>
<tr><th>J. K. Burgoon (1982)[45]</th><th>R. Clarke (1992, 2013)[46]</th><th>S. Gutwirth et al (2011)[47],</th></tr>
<tr><td>Social privacy
(related to interpersonal relationships)</td><td rowspan="2">Communicative privacy
(related to exchanges between people)</td><td>Communicative privacy</td></tr>
<tr><td>Psychological privacy
(related to intimate exchanges between persons)</td><td>Associative privacy
(related to associations between persons)</td></tr>
<tr><td rowspan="2">Physical privacy
(related to home, body, etc.)</td><td rowspan="2">Physical privacy</td><td>Personal privacy
(related to the body)</td></tr>
<tr><td>Spatial privacy</td></tr>
</table>

[44] KOOPS, B-J. *et al*. A "Typology of Privacy," University of Pennsylvania Journal of International Law, vol. 38, No. 2, 2017, pp. 483, online: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1938&context=jil

[45] "*Social privacy,*" "*physical privacy*" and "*psychological privacy*": BURGOON, J. K. "Privacy and communication" in BURGOON, M., ed., Communication Yearbook 6, SAGE, 1982, pp. 206-249; VON PAPE, T., TREPTE, S. and MOTHES, C. "Privacy by Disaster? Press Coverage of Privacy and Digital Technology," European Journal of Communication, vol. 32, No. 3, June 2017, p.191.

[46] "Privacy of the physical person," "privacy of personal communications," "privacy of personal data," "privacy of personal behavior," and "privacy of personal experience": CLARKE, R. A Framework for Analyzing Technology's Negative and Positive Impacts on Freedom and Privacy, Aug. 16, 2015, online: http://www.rogerclarke.com/DV/Biel15-DuDA.html#App3 (consulted on Dec. 2, 2019); KOOPS. "A Typology of Privacy," *supra* note 44, pp. 497-500.

[47] "Privacy of communication," "privacy of the person," "privacy of location and space," "privacy of association," "privacy of behaviour and action," "privacy of thoughts and feelings" and "privacy of data and image": GUTWIRTH, S. *et al.*" Legal, social, economic and ethical conceptualisations of privacy and data protection," Prescient project, March 23, 2011, pp. 63 et seq, online: http://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT-D1---final.pdf

	Behavioural privacy (related to actions)	(related to movement in public, semi-public and private spaces)
		Behavioural privacy
	Informational privacy (related to personal information)	Informational and visual privacy
	Experiential privacy (related to the ideas, concepts and contents experienced and consulted)	Emotional and ideational privacy (related to thoughts and feelings)

1.2.2 Different legal perspectives on the subject

As the privacy literature has developed, some state actors have also had to take sides in the debates surrounding the definition of privacy. This is the case for legislators and judges, among others. Like the literature, the different legal systems present various conceptions of privacy, which are of course in line with certain aspects of human science theories on the subject, but which deserve to be analyzed separately, since certain underlying foundations are articulated differently.

Accordingly, we will briefly discuss in this section the European, American and Canadian legal perspectives on the subject. While our neighbour to the south commonly influences Canada's legal system[48], the old continent also deserves our attention given its status as a forerunner in consumer privacy protection; the Wall Street Journal once described Europe as the "Privacy Cop to the World[49]."

We note at the outset that despite important nuances, Canadian, American and European laws have two common foundations:

1. The laws focus their intervention on informational privacy, in that the existing frameworks focus mainly on the collection, processing and management of individuals' personal information;

[48] See for example: MANFREDI, C. "The Use of United States Decisions by the Supreme Court of Canada Under the Charter of Rights and Freedoms," Canadian Journal of Political Science, vol. 23, No. 3, 1990.
[49] SCHEER, D. "Europe's New High-Tech Role: Playing Privacy Cop to World," Wall Street Journal, October 10, 2003, online: https://www.wsj.com/articles/SB106574949477122300

2. The laws attach a fundamental importance to the concepts of individual choice and consent, thus coming closer to the concept of control put forward by authors such as Moore, Westin and Fried[50]. In this regard, it should be noted that generally, the procedures and the actual capacity of individuals to exercise this control are much more highly developed in Europe than in Canada and the United States.

1.2.2.1 Consumer privacy in European law: a question of human dignity

Within the European Union, individual privacy protection is first addressed in legal instruments recognizing human rights. "Everyone has the right to respect for his private and family life, his home and his correspondence." This is what the European Convention on Human Rights[51] and the European Charter of Fundamental Rights[52] provide.

The European regime also distinguishes the right to privacy from the right to protection of personal information, in contrast to the authors mentioned above, for whom personal information or information about individuals is generally seen as a component of privacy. These two rights are explicitly linked in the European instruments, but are dealt with in separate articles[53], since the right to the protection of personal information is said to derive only partially from the right to privacy[54]. The protection of personal information is also subject to a broad framework specific to it, namely the *General Data Protection Regulation* (*GDPR*) adopted in April 2016 and implemented in May 2018.

In addition to a specific mention in the *GDPR* preamble[55], the type of framework chosen by the European Parliament is particularly indicative of the status (legal and philosophical) of personal information protection as a fundamental right. It is an omnibus regulation that concerns both private and public actors[56] and applies to all the information of an identified or identifiable person[57], thus covering a very wide range of situations. And it provides a series of minimum protections that are automatically applicable and that a consumer cannot waive in a private agreement[58].

---

[50] WALDMAN. Privacy as Trust, *supra* note 18, p. 30.
[51] COUNCIL OF EUROPE. European Convention on Human Rights, ECHR No.: 005, art 8.
[52] EUROPEAN UNION. Charter of Fundamental Rights of the European Union, 2000/C 364/01, art II-7: "Everyone has the right to respect for his or her private and family life, home and communications."
[53] *Ibid.,* arts. II-7 and II-8.
[54] EUROPEAN UNION. "Explanations Relating to the Charter of Fundamental Rights," Official Journal of the European Union, C 303, 14.12.2007, pp. 17-35, online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32007X1214(01)&from=EN; MOSTERT, M. *et al*. "From Privacy to Data Protection in the EU: Implications for Big Data Health Research," European Journal of Health Law, vol. 25, No. 1, December 2017, p.5, online: https://bartvandersloot.com/onewebmedia/From%20privacy%20to%20Data%20Protection.pdf
[55] "The protection of natural persons with regard to the processing of personal data is a fundamental right": EUROPEAN UNION. General Data Protection Regulation, 2016/679, preamble, para (1) [GDPR].
[56] SCHWARTZ, P. M. and SOLOVE, D. J. "Reconciling Personal Information in the United States and European Union," California Law Review, vol. 102, No. 4, 2013, pp. 880-881.
[57] GDPR, *supra* note 55, s. 4(1). For an explanation of identifiability, see Preamble, para (26).
[58] LYNSKEY, O. The foundations of EU data protection law, Oxford University Press, 2015, p.40.

The European vision of privacy and personal information protection is closely linked to the safeguarding of individuals' human dignity, honour and reputation.

> Despite its almost invisible presence in the GDPR, human dignity is the fundamental concept that provides the framework within which one needs to interpret what the GDPR – and more generally European culture and jurisdiction – understand by informational privacy (henceforth only privacy)[59]. [citations omitted]

In general, the regulations in place in the European Union are intended to give individuals control over the disclosure of their personal information with the ultimate goal of avoiding unwanted public exposure and the embarrassment or humiliation that might accompany it[60]. This European perspective on privacy is reminiscent of Warren and Brandeis' concerns on the subject.

The "right to be forgotten," first conceived and implemented in European law, is a clear example of the importance given to the protection of reputation in the exercise of the right to privacy. This right, sometimes called "digital redemption[61]," allows Europeans, under certain circumstances, to request that search engines dereference hyperlinks about them[62]. Examples provided by Google include the removal of hyperlinks to news articles about convictions that are years old and for which sentences have been served, charges that did not lead to convictions, personal bankruptcies, or statements made by people who were minors at the time[63].

In this European perspective on privacy, which differs considerably from that of the Americans, the fears are greater when intrusions are made by private actors than by public actors, because intrusions made by private actors are more likely to damage the public reputation of individuals.

> Dignity is protected first and foremost in society, so one's dignity does not necessarily suffer from government actions as much as it potentially suffers from the thoughts and perceptions of other members of society. If the goal of privacy protection is ultimately the protection of dignity, then it is clear that privacy must be protected first and foremost in society, and that government intrusions are less worrisome.[64]

---

[59] FLORIDI, L. "On Human Dignity as a Foundation for the Right to Privacy," Philosophy & Technology, vol. 29, No. 4, December 2016, p.307.
[60] The Two Western Cultures of Privacy: Dignity versus Liberty. 113, No. 6, January 2004, p. 1161.
[61] JONES, M. Ctrl + Z: The Right to Be Forgotten. New York University Press, 2016, p.81.
[62] COMMISSION NATIONALE DE L'INFORMATION ET DES LIBERTÉS. "Droit au Déréférencement. Les critères communs utilisés pour l'examen des plaintes," online: https://www.cnil.fr/sites/default/files/typo/document/Droit_au_dereferencement-criteres.pdf (consulted on August 6, 2021).
[63] GOOGLE. "Requests for removal of content under EU privacy legislation," online: https://transparencyreport.google.com/eu-privacy/overview (consulted on April 5, 2021).
[64] LEVIN, A. and NICHOLSON, M. J. "Privacy Law in the United States, the EU and CanadaPrivacy Law in the United States, the EU and Canada: The Allure of the Middle Ground," University of Ottawa Law & Technology Journal, vol. 2, No. 2, 2005, pp. 388-389.

1.2.2.2 Consumer Privacy in U.S. Law: The Free Market First

While the European framework explicitly recognizes a general right to privacy, this right, when directed at the private sector, is less explicit in the U.S. An indirect reference to privacy is found in the Fourth Amendment to the U.S. Constitution, which prohibits unreasonable searches and seizures by the state[65]. Over time, the interpretation of this right has been expanded to cover broader protection against state intrusion into the lives of Americans and particularly into the personal decisions they make (property, health, etc.)[66].

And unlike the European conception of privacy, which has human dignity as its pillar, the American conception focuses more on the right to freedom; a freedom that is exercised above all in opposition to the state.

> America, in this as in so many things, is much more oriented toward values of liberty, and especially liberty against the state. At its conceptual core, the American right to privacy still takes much the form that it took in the eighteenth century: It is the right to freedom from intrusions by the state, especially in one's own home. The prime danger, from the American point of view, is that "the sanctity of [our] home[s]," in the words of a leading nineteenth-century Supreme Court opinion on privacy, will be breached by government actors[67].

What about the private sector? When it comes to consumer privacy, not in relation to the state, but rather in relation to merchants and third parties, the American perspective is primarily based on the proper functioning of the free market[68]. The U.S. federal government limits its interventions to the protection of the most sensitive information, such as health information[69] or information about minors[70], for which markets would not provide adequate protections. In doing so, the current U.S. regime is a quilt of sector-specific regulations and industry self-regulation[71]. The Federal Trade Commission (FTC) has the authority to protect consumer privacy against unfair and/or deceptive business practices[72].

---

[65] UNITED STATES. Constitution, Amendment IV.
[66] WHITMANT, J. Q. "The Two Western Cultures of Privacy," *supra* note 60, pp. 1212 and 1214.
[67] *Ibid.,* pp. 1161-1162.
[68] ASHWORTH, L., & FREE, C. "Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns," Journal of Business Ethics, vol. 67, No. 2, 2006, p.109; LEVIN. "Privacy Law in the United States," *supra* note 64, p. 362.
[69] UNITED STATES. Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 201.
[70] UNITED STATES. Children's Online Privacy Protection Act, 15 U.S.C. 91.
[71] GADY, F-S. "EU/U.S. Approaches to Data Privacy and the "Brussels Effect": A Comparative Analysis," Georgetown Journal of International Affairs, 2014, p.15; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Consent and Privacy – A discussion Paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act," May 2016, online: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/
[72] FEDERAL TRADE COMMISSION. "What We Do," online: https://www.ftc.gov/about-ftc/what-we-do
EIJK, N. V., HOOFNAGLE, C. J., and KANNEKENS, E. "Unfair Commercial Practices: A Complementary Approach to Privacy Protection," European Data Protection Law Review, vol. 3, 2017, p. 325; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. Consent and Privacy," *supra* note 71.

And since consumer privacy is not given as much weight in the U.S. regime as it is in the European regime, it rarely wins out when pitted against other rights, such as freedom of trade and freedom of expression[73].

However, a few states -- California, Colorado and Virginia -- have implemented a more comprehensive consumer privacy regime[74]. Several other states are also considering this option in the face of failed attempts to do so at the federal level[75].

1.2.2.3 Consumer Privacy in Canadian Law: Halfway between Europe and the United States

The Canadian legal conception of individual privacy is halfway between those of Europe and the United States. The Canadian conception incorporates concepts of human rights protection (and thus of human dignity), but its framework is primarily aimed at regulating markets. In this sense, Canadian thinking on consumer privacy protection may seem somewhat incomplete, as if it did not know where to start...

The right to privacy is recognized (indirectly) in the *Canadian Charter of Rights and Freedoms,* under the rights *to liberty and to be secure against unreasonable search and seizure*[76]. This protection is limited to intrusions by the state. When it comes to potential intrusions by the private sector, the relevant federal legislation is the *Personal Information Protection and Electronic Documents Act*[77] (*PIPEDA*). Three provinces have enacted "substantially similar" legislation that applies in lieu of *PIPEDA*[78]. The specific operation of those statutes and the rules they provide for will be discussed in Chapter 5.

It should also be noted that the province of Quebec formally recognizes the right to privacy in its *Charter of Human Rights and Freedoms*, both in relation to the state and the private sector[79]. Ultimately, since the various laws applicable in Canada are all "substantially similar," this Quebec particularity has little effect on our analysis of the conception of privacy by the Canadian legal system.

---

[73] HOOFNAGLE, C. J., VAN DER SLOOT, B and ZUIDERVEEN BORGESIUS, F. "The European Union general data protection regulation: what it is and what it means," Information & Communications Technology Law, vol. 28, No. 1, 2019, p.75; SCHWARTZ. "Reconciling Personal Information," *supra* note 56, pp. 880-881.
[74] STATE OF CALIFORNIA. California Consumer Privacy Act of 2018; STATE OF CALIFORNIA. California Privacy Rights Act of 2020; STATE OF COLORADO. Colorado Privacy Act; STATE OF VIRGINIA. Consumer Data Protection Act.
[75] IAPP. "US State Privacy Legislation Tracker," online: https://iapp. org/resources/article/us-state-privacy-legislation-tracker/ (consulted on June 10, 2021).
[76] CANADA. Constitution Act, 1982, Schedule B to the Canada Act 1982 (U.K.), 1982, c 11, arts. 7 and 8.
[77] CANADA. Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 [PIPEDA].
[78] QUEBEC. An Act respecting the protection of personal information in the private sector, RSQ c P-39.1 [APPIPS], ALBERTA. Personal Information Protection Act, statutes of Alberta, 2003, c P-6.5 [APIPA], BRITISH COLUMBIA. Personal Information Protection Act, SBC 2003, c 63 [BCPIPA]. There are also provincial statutes that deal solely with personal health information (New Brunswick, Nova Scotia, Ontario, Newfoundland and Labrador).
[79] QUEBEC. Charter of Human Rights and Freedoms, RSQ c C-12, art 5.

Like the European and American regulatory frameworks, the Canadian framework concerns only the protection of personal information. Since there is no rule in Canada that distinguishes the right to privacy from the right to protection of personal information, we are inclined to think that the former is perceived more as a component of the latter than as a truly distinct element.

While *PIPEDA* does not formally state that it is intended to protect privacy, it does state that it sets out rules for the collection, use and disclosure of personal information "in a manner that recognizes the right of privacy of individuals with respect to their personal information[80]." Also, like the *GDPR*, it adopts a broad and inclusive definition of personal information[81] and does not limit its application to certain sensitive personal information. Similarly, *PIPEDA* and equivalent provincial legislation cover the entire private sector with a few exceptions[82]. This is a far cry from the weak U.S. protections available only for health information or information about minors.

But while *PIPEDA* thus shows signs of a Canadian perspective on privacy on the basis of recognizing and protecting a fundamental right, the document's origins are far removed from that perspective!

Canadian legislators had two objectives in adopting the Act, both of which were primarily focused on the development of the digital economy, which in 2000 was still in its infancy. First, the Act was intended to foster public confidence in electronic commerce and thus "mo[ve] Canada to the forefront of the global digital economy," as the then Minister of Industry put it[83]. This objective is very clearly reflected in the full title of the Act, in which the protection of personal information is reduced to a way of facilitating commerce:

> An Act to facilitate and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information and transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act [84]

The second objective of *PIPEDA* was to ensure continued trade with the European Union, given the European Parliament's development of Directive 95/46/EC a few years earlier[85]. Article 25 of that directive prohibited the transfer of EU Member State residents' personal data to third countries unless the latter also ensured an adequate level of protection for the data in question[86]. Canada obtained that "certification" thanks to *PIPEDA* in 2002[87].

---

[80] PIPEDA, *supra* note 77, s. 3.
[81] "Any information about an identifiable individual": *Ibid.* s. 2.
[82] *Ibid.* s. 4; APPIPS, *supra* note 78, s. 3 *a contrario*; APIPA, *supra* note 78, s. 4; BCPIPA, *supra* note 78, s. 3.
[83] LEVIN. "Privacy Law in the United States," *supra* note 64, p. 379.
[84] PIPEDA, *supra* note 77.
[85] EUROPEAN UNION. Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 95/46/EC.
[86] The adequacy criterion of a third country's legislation is now provided for in GDPR, *supra* note 55, art. 45.
[87] COMMISSION OF THE EUROPEAN COMMUNITIES. Decision 2002/2/EC, Official Journal L 002 of 04/01/2002, pp. 13-16, online: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32002D0002

The summary offered by Canadian privacy law professor Teresa Scassa illustrates the surprising lack of consideration for the protection of such a fundamental right in the development of the law that affects it:

> To understand why PIPEDA is such a mess requires some history. PIPEDA was passed by Parliament in 2000. Its enactment followed closely on the heels of the EU's Data Protection Directive, which, like the GDPR, threatened to disrupt data flows to countries that did not meet minimum standards of private sector data protection. Canada needed private sector data protection legislation and it needed it fast. [...] The private sector did not want such legislation. As a compromise, the government decided to use the CSA Model Code - a voluntary privacy code developed with multi-stakeholder input - as the normative heart of the statute. There had been enough buy-in with the Model Code that the government felt that it avoid excessive pushback from the private sector. The Code, therefore, originally drafted to provide voluntary guidance, was turned into law. The prime minister at the time, the Hon. Jean Chretien, did not want Parliament's agenda overburdened with new bills, so the data protection bill was grafted onto another bill addressing the completely different issue of electronic documents[88].

The weak enforcement powers of the Office of the Privacy Commissioner of Canada, which is charged with overseeing compliance with *PIPEDA,* also suggest that consumer privacy is not viewed (at least not fully) as a human rights issue.

The Canadian conception of privacy therefore seems more difficult to define than that of its European and American counterparts. In its desire to present and frame the protection of personal information from the perspective of a fundamental right, it was nevertheless quick to adopt a framework focused on reprehensible commercial practices relating to personal information.

Canadian reforms that could potentially change the game

We note that we are witnessing a trend toward the standardization of privacy laws around the world, based on the European framework[89]. Canada is no exception to this trend: The year 2020 saw the introduction of two bills inspired by the *GDPR*, one in the federal Parliament and the other in the Quebec National Assembly. The Quebec bill has since been adopted as Bill 25 and is scheduled to come into force in September 2023 (with the exception of a few provisions). The federal bill died on the order paper in the summer of 2021. Is the Canadian legal approach to privacy changing?

Not necessarily. Both bills proposed the addition of new rights for consumers in the use of their personal information (the right to mobility of personal information, for example), but did not really challenge the existing balance between the needs of consumers and the

---

[88] SCASSA, T. "PIPEDA reform should include a comprehensive rewrite," July 9, 2018, online: https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=279:pipeda-reform-should-include-a-comprehensive-rewrite&Itemid=80&tmpl=component&print=1

[89] BERNIER, C. "The Evolution of Distinctions between Canadian and Foreign Privacy Rights," Canadian Bar Association, November 19, 2020, online: https://www.cba.org/Sections/Privacy-and-Access/Articles/2020/The-evolving-distinctions-between-Canadian-and-for

needs and desires of businesses. The title of the federal bill was changed to reflect some of the changes, but the explicit objectives of facilitating and promoting electronic commerce remained central, and the protection of personal information remained a means to those ends.

PIPEDA	Bill C-11
An Act to facilitate and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information and transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act	An Act to facilitate and promote electronic commerce through the protection of personal information collected, used or disclosed in the course of commercial activities

Ironically, the short title of the new federal legislation planned in Bill C-11 would have been the "Consumer Privacy Act." Perhaps this is a further indication of Canadian ambivalence about privacy, or simply a marketing exercise by the federal government…

1.3 What about Online Privacy?

This report will focus specifically on online privacy in the chapters that follow. Is the Internet a game-changer for consumer privacy?

The Internet has certain technical characteristics that simplify the sharing of personal information and access to information by everyone, at no or very low cost. Connecting devices, such as computers and other connected objects, allow for the collection and processing of this shared information and even information about individuals' own use of the network without them necessarily being aware of that[90]. Some say that the network never forgets. While this expression is not entirely accurate[91], the Internet does enable and facilitate a greater preservation of information. More broadly, the network is at the origin of major changes in society.

> Together these technological advancements have contributed to incredible social shifts in the way information is created, shared, and understood, leaving overwhelming information vulnerabilities[92].

[90] JONES. Ctrl Z, *supra* note 61, p. 83.
[91] Studies show that the vast majority of content available online disappear within a year of publication. See for example: AMBROSE, M. "It's About Time: Privacy, Information Life Cycles, and the Right to Be Forgotten." Stanford Technology Law Review, vol. 16, No. 2, 2013, p. 369.
[92] JONES. Ctrl Z, *supra* note 61, p. 83.

The Internet's importance in consumers' lives today and its impact on their privacy results of course from a long (and still ongoing) process of consumer adaptation and technological development. The authors Yun, Lee and Kim have developed a general timeline of the Internet's evolution and Internet users' perception[93]:

- 1991-2000: beginnings of the Internet – "Introduction" period (World Wide Web, Google, blogs, etc.)
- 2001-2007: advent of social media – a period of "awareness" (YouTube, Facebook, Netflix, podcasts, etc.)
- 2008-2013: implementation of the sharing economy – a period of "development" (smartphones, big data, cloud computing, etc.)
- 2014-present: transition to technological automation – "extension" period (Internet of Things, Airbnb, etc.)

As was the case with privacy in general, we find that there is no common definition of digital privacy. Legislators do not approach the protection of personal information and privacy by private entities in the physical and digital worlds any differently, but in the view of many, legislation generally lags strikingly behind technological developments[94].

Despite the absence of a specific and universal definition of privacy in a digital context, we nevertheless observe certain developments that can help define the concept of privacy in this context:

- Online privacy is now seen more as a consumer protection issue than a socio-political issue[95]
- The protection of personal information is currently seen as the dominant element of online consumer privacy[96]
- The distinction between so-called private and public personal information is increasingly difficult to make in the digital environment:

> Electronic media have facilitated the development of a 'middle region' between the frontstage and backstage; they integrate 'formerly private situations into formerly public ones'. Thus, the line between the 'public' frontstage and the 'private' backstage has been substantially blurred. These impacts of the media and ICTs on the public/private distinction are apparent in a number of areas, most notably in surveillance, webcam broadcasting, the work/home division, and the

[93] YUN, H., LEE, G., and KIM, D. J. "A Chronological Review of Empirical Research on Personal Information Privacy Concerns: An Analysis of Situational Contexts and Research Constructs," Information & Management, vol. 56, No. 4, June 1, 2019, p. 574.
[94] See for example: TENE, O. "Privacy: The New Generations," International Data Privacy Law, vol. 1, No. 1, 2011, pp. 11-13, online: https://www.researchgate.net/publication/228226941_Privacy_The_New_Generations
[95] CAMPBELL, J. E. and CARLSON, M. "Panopticon.com: Online Surveillance and the Commodification of Privacy," Journal of Broadcasting & Electronic Media, vol. 46, No. 4, 2002.
[96] SHAPIRO, S. "Places and Spaces: The Historical Interaction of Technology, Home, and Privacy," Information Society, vol. 14, No. 4, October 1998.

> social web. (…) the public/private distinction is best thought of as a continuum. This continuum is anchored on one end by the 'private' and on the other by the 'public'[97].

As we will see in Chapter 3, information that was historically considered private by consumers is no longer so clearly defined today, particularly because of its increased presence on social media.

But first, it's important to draw a general portrait of Internet users' concerns, which are influenced by their conceptions of privacy and vice versa.

ONLINE PRIVACY AND CONSUMERS: A REVIEW OF THE LITERATURE

2.1 A Portrait of Consumers' Concerns about Their Privacy Online

The purpose of this section is to outline the literature's broad findings regarding consumers' concerns about their privacy online. What concerns have been identified? What potential risks are Internet users particularly concerned about? To facilitate understanding, the elements identified are accompanied by concrete examples of risks or company practices that justify or support consumers' concerns in this area. We will also discuss the personal or societal factors likely to influence Internet users' general level of concern or more specific worries.

It should be noted that the concerns and risks raised in this section are based primarily on polls and surveys of Internet users in the United States and Europe[98]. However, as we will see in the next section, the results of the 2020 Canada-wide survey demonstrate that Canadian Internet users have similar concerns and risks.

2.1.1. Internet users are increasingly concerned about their privacy

A Westin[99] study of various U.S. public opinion surveys on privacy from the late 1970s to the early 2000s reveals some historical trends. The author notes a shift in public opinion in the mid-1990s with respect to the handling of personal information by private

[97] FORD, S. M. "Reconceptualizing the public/private distinction in the age of information technology," Information, Communication & Society, vol. 14, No. 4, 2011, pp. 555 and 560.
[98] HONG, W., CHAN, F., and THONG, J. "Drivers and Inhibitors of Internet Privacy Concern: A Multidimensional Development Theory Perspective," Journal of Business Ethics, vol. 168, No. 3, 2019.
[99] WESTIN, A. F. "Social and Political Dimensions of Privacy," Journal of Social Issues, vol. 59, No. 2, 2003.

companies[100]. While government was still the primary source of concern at the time, private companies were now a close second and the level of concern about them continued to grow. Banks, insurers and all companies operating on the Internet were of particular concern. This progression has continued over the last twenty years.

Today, the gold standard for assessing privacy concerns is the annual survey conducted by Ipsos on behalf of the Centre for International Governance Innovation, the Internet Society and the United Nations Conference on Trade and Development. Some 25,000 Internet users are surveyed, spanning five continents. In 2019, nearly 8 in 10 respondents said they were concerned about their online privacy; 3 in 10 said they were very concerned[101]. Those percentages are steadily rising, as each year a majority of respondents say they are more concerned than they were the year before:

Table 2

Internet users' overall level of concern about online privacy compared to the previous year

	2014	2016	2017	2018	2019
% of respondents who say they are more concerned about their online privacy than they were 12 months ago	64%[102]	57%[103]	55%[104]	52%[105]	53%[106]
Much more concerned	31%	31%	28%	22%	22%
Somewhat more concerned	33%	26%	27%	30%	31%

* Data are not available for 2015 and 2020 (as of summer 2021).

[100] See also on the subject: O'NEIL, D. "Analysis of Internet Users' Level of Online Privacy Concerns," Social Science Computer Review, vol. 19, No. 1, February 2001, p. 18.
[101] CENTRE FOR INTERNATIONAL GOVERNANCE INNOVATION and IPSOS. "2019 CIGI-Ipsos Global Survey on Internet Security and Trust," Parts I & II, p.8, online: https://www.cigionline.org/internet-survey-2019 (consulted on November 20, 2020).
[102] *Ibid.,* Presentation, p. 17.
[103] *Ibid.,* Data table, question 1.
[104] *Ibid.,* Presentation, p. 4.
[105] *Ibid.*
[106] *Ibid.,* parts I & II, p. 10.

What can explain this continual increase in Internet users' level of concern about their privacy? Several factors are generally raised by authors. The most important is undoubtedly the transfer of individuals' privacy concerns to the Web and its related technologies, whose rapid development significantly affects the handling of personal information.

> While consumers have had privacy concerns long before the advent of the Internet, their PIP [personal information privacy] concerns have evolved significantly with time in part due to the emergence of disruptive technologies including ecommerce, mobile computing, social media, location-based service (LBS), radio-frequency identification (RFID), IoT (Internet of Things), and big data analytics[107].

Online privacy issues have gained more prominence in the media and the news in recent years, which may also explain an increased public awareness of the risks to their online privacy. We note, for example, that large-scale data leaks (Facebook in 2018, Sony in 2014, etc.)[108] were widely reported. Similarly, the information and lobbying campaigns of some influential groups, such as Electronic Privacy Information Center (EPIC), may also have contributed to the current widespread concern[109].

Lastly, while concerns about governments have risen following the Wikileaks and Cambridge Analytica scandals, online retailers and Web companies remain strongly distrusted. When asked about the sources of their distrust of the Internet, respondents to the Ipsos survey cited above pointed to:[110]

- Social media platforms (75%)
- Search engines (65%)
- Internet service providers (63%)
- E-commerce platforms (61%)
- Online and mobile banking platforms (56%)

[107] YUN. "A chronological review," *supra* note 93, p. 572.
[108] HONG. "Drivers and Inhibitors," *supra* note 98; WIRTZ, J., LWIN, M., & WILLIAMS, J. "Causes and consequences of consumer online privacy concern," International Journal of Service Industry Management, vol. 18, No. 4, 2017 , p.327; METZGER, M. J. "Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce," Journal of Computer-Mediated Communication, vol. 9, No. 4, June 2006.
[109] WIRTZ. "Causes and consequences," *supra* note 108, p. 327.
[110] CENTER FOR INTERNATIONAL GOVERNANCE INNOVATION. "Global Survey, *supra* note 101, Parts I & II, p. 116.

2.1.2.The main concerns of consumers

When it comes to the more specific privacy concerns of online consumers, many refer to the work of Malhotra, Kim and Aagarwal[111] . Dissatisfied with past writings on the subject – because they were either not well adapted to the digital context or were too abstract[112] – those authors sought to define more specifically the major privacy concerns of online consumers. The authors have identified three concerns, related to information collection, control and knowledge.

2.1.2.1 Concerns about the extent of online personal information collection

The first concern of Internet users identified by Malhotra, Kim and Agarwal is the extent to which personal information is collected online[113]. This concern is not surprising, given that on a daily basis, an Internet user will voluntarily or unknowingly provide an impressive amount of personal information about himself when using the Internet.

- Browsing the Web: On average, 77% of the Web pages visited by an Internet user include tracking devices (e.g., cookies)[114];
- Using a social network: Nearly 30% of Facebook subscribers share content on the platform every day[115];
- Using a mobile application: 93% of game applications available on the Google Play Store reportedly have at least one third-party tracker[116];
- Using a smartphone: An Android phone on which the Chrome browser is activated communicates geolocation data to Google an average of 14 times per hour, even if the user does not interact with the device[117].

---

111 MALHOTRA, N. K., KIM, S. S., and AGARWAL, J. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," Information Systems Research, vol. 15, No. 4, December 2004, pp. 336-35; PREIBUSCH, S. "Guide to measuring privacy concern: Review of survey and observational instruments," International Journal of Human-Computer Studies, vol. 71, 2013, pp. 1136.
112 MALHOTRA. "IUIPC," *supra* note 111, pp. 337-338 and 340.
113 *Ibid.* pp. 338-339.
114 KARAJ, A. *et al*. "WhoTracks. Me: Shedding light on the opaque world of online tracking," 2018, p.1, online: https://arxiv.org/abs/1804.08959
115 FRACTL. "Average Facebook User Sharing Habits Study," 2016, online: https://www.frac.tl/work/marketing-research/facebook-user-sharing-habits-study/
116 BINNS, R. et al. "Third Party Tracking in the Mobile Ecosystem," April 2018, p.6, online: https://arxiv.org/pdf/1804.03603.pdf
117 SCHMIDT, D. C. "Google Data collection," Digital Content Next, August 2018, online: https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf

The digital footprint

All the digital data disclosed by an Internet user during his Internet use form his digital footprint[118]. This is made up of two components: personal data shared or provided actively by the person online on the one hand, and personal data collected passively, i.e. without his knowledge (tracking data, data related to device use, geolocation data, etc.) on the other hand.

The digital footprint (active and passive components) and the subsequent processing of data from both components generally provide a very detailed portrait of the person concerned[119]. As an example, a group of researchers from Stanford and Cambridge Universities who have been working on the ability of artificial intelligence to evaluate an individual's personality in light of his digital footprint on social media have obtained some impressive results:

> The results show that by mining Facebook Likes, the computer model was able to predict a person's personality more accurately than most of their friends and family. Given enough Likes to analyze, only a person's spouse rivaled the computer for accuracy of broad psychological traits[120].

The digital footprint goes far beyond the context of social media such as Facebook. However, that footprint now appears to originate on social media, even before the person concerned is old enough to use the Internet! A 2010 study on the phenomenon of "sharenting" estimated, for example, that 84% of children under the age of 2 had a digital presence in Canada (notably through photos or other information about them on social media used by their entourage)[121]. A recent study by the Children's Commissioner for England estimated that by the age of 13, a child is the subject of 1,300 online posts on average by his parents[122]. And the child himself will make an average of 70,000 social media posts before reaching the age of majority[123].

---

[118] OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE. "Trace numérique," online: http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26508672

[119] For more details on artificial intelligence's data analysis capability, see the section on profiling (section 2.1.2.2)

[120] CAMBRIDGE UNIVERSITY. "Computers using digital footprints are better judge of personality than friends and family," January 12, 2015, online: https://www.cam.ac.uk/research/news/computers-using-digital-footprints-are-better-judges-of-personality-than-friends-and-family

[121] MANOTIPYA, P. and GHAZINOUR, K. "Children's Online Privacy from Parents' Perspective," Procedia Computer Science, vol. 177, 2020, p. 178.

[122] CHILDREN'S COMMISSIONER. "Children's Commissioner's report calls on internet giants and toy manufacturers to be transparent about collection of children's data," November 8, 2018, online: https://www.childrenscommissioner.gov.uk/2018/11/08/childrens-commissioners-report-calls-on-internet-giants-and-toy-manufacturers-to-be-transparent-about-collection-of-childrens-data/

[123] *Ibid.*

The multiplicity of stakeholders

While we're quick to point to (and criticize) major Web companies such as Facebook, Amazon and Google for their massive collection of personal information, they are far from being the only ones involved. Based on the work of Yun, Lee and Kim[124], we note three main types of stakeholders involved in the collection or transmission of personal information online, many of which are generally unknown to the consumer:

> Type 1 - The Internet user himself, who voluntarily or actively posts or transmits personal information about himself online, for example on social media or in online transactions.
>
> Type 2 - Businesses that the Internet user deals with directly when purchasing a good or using an online service. The business may collect information:
>
> - Actively provided by the user (e.g., financial information to complete a transaction);
> - Passively provided by the Internet user as part of the transaction and his use of the product or service (e.g., the company's cookies on its website, usage data from a connected object, etc.).
>
> Type 3 - Third parties that don't have a direct relationship with the individual to whom the personal information relates, such as:
>
> - Companies that collect data from tracking devices (such as cookies and Web beacons);
> - Data mining companies that use data harvesting, data crawling and data mining processes to collect data on a large scale from the Internet;
> - Data brokerage firms that buy and sell personal information about Internet users, including from companies that have done business with them directly and from data tracking and mining companies;
> - Hackers who gain unauthorized access to personal information (through hacking, phishing, spyware, etc.).

[124] YUN. "A Chronological Review," *supra* note 93, p. 585.

The big data phenomenon

It is also important to briefly discuss the existence of big data, which certainly contributes to consumers' concerns about the amount of their personal information flowing online.

Big data actually consists of data sets, structured or not, that can be described by three "v's": volume, variety and velocity[125]. It is a very large amount of data from a wide variety of sources. And it is stored and processed particularly fast using advanced technological tools (traditional data processing tools are not powerful enough). The variety of sources of big data and the formats in which it is stored are the distinguishing features of big data compared to traditional[126] databases.

According to the World Economic Forum, some 463 exabytes[127] of data will thus be created every day from 2025[128].

2.1.2.2 Concerns about loss of control over personal information online

The second concern of Internet users that Malhotra, Kim and Agarwal identified is the loss of control over their personal information online[129], whether at the point of collection, disclosure or use. Given the scale of data collection described above, it is hardly surprising that several U.S. and European surveys confirm the widespread feeling among Internet users about this loss of control[130].

Although consumer consent is commonly sought by a business to collect personal information online, consumers often have no real choice but to consent if they wish to access the business' website or use its service. The "control" that the individual could then exercise, for example, by refusing collection, is accompanied by negative consequences, such as loss of access or loss of choice in the services and products available. Moreover, in some cases, this loss of access does not guarantee the absence of intrusion into one's

---

[125] OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE. "Megadata," online: http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26507313 (consulted on April 10, 2021).
[126] IPPOLITO, P. P. "Big Data Analysis: Spark and Hadoop," Towards data science, July 11, 2019, online: https://towardsdatascience.com/big-data-analysis-spark-and-hadoop-a11ba591c057
[127] 1,000,000,000,000,000,000 bytes.
[128] Or the equivalent of 212,765,957 DVDs per day. DESJARDINS, J. "How much data is generated each day?," World Economic Forum, April 17, 2019, online: https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/
[129] MALHOTRA. "IUIPC," *supra* note 111, p. 339.
[130] KEDMEY, D. "9 in 10 Americans Feel They've Lost Control of Their Personal Data," Time, November 12, 2014, online: https://time.com/3581166/privacy-personal-data-report/; NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION. "Most Americans Continue to Have Privacy and Security Concerns," August 20, 2018, online: https://www.ntia.doc.gov/blog/2018/most-americans-continue-have-privacy-and-security-concerns-ntia-survey-finds; AXCIOM and DMA. "Data privacy: What the consumer really thinks," February 2018, p.15, online: https://dma.org.uk/uploads/misc/5a857c4fdf846-data-privacy---what-the-consumer-really-thinks-final_5a857c4fdf799.pdf

private life. Facebook has been severely criticized in the past for collecting personal information from users who don't even use the service![131]

To explain the basis of this concern of Internet users about the control they exercise over their personal information, the authors refer to the desire for justice intrinsic to individuals. A situation will be perceived as more acceptable – more just – if it follows a procedure over which the consumer has had some control[132]. In this sense, the absence or very low degree of control that Internet users now have over the collection of their personal information online and its subsequent uses have made them naturally more concerned about their online privacy[133].

2.1.2.3 Concerns about lack of knowledge regarding online privacy

The final general concern identified by Malhotra, Kim and Agarwal pertains to the lack of information available and Internet users' lack of knowledge about the practices of private online entities involved in the handling of their personal information[134]. This concern, which relates more broadly to issues of transparency, is particularly important given that the choices Internet users make when using the Internet depend on their understanding of companies' practices and policies in this regard.

The authors Correia and Compeau have examined Internet users' awareness with respect to the protection of their online privacy. The authors identify various aspects of the enormous task that has to be undertaken by anyone who wants to be informed and understand the digital environment in which his personal information circulates[135]:

---

131 INGRAM, D. "Facebook fuels broad privacy debate by tracking non-users," Reuters, April 15, 2018, online: https://www.reuters.com/article/us-facebook-privacy-tracking-id; BRANDOM, R. "Shadow profiles are the biggest flaw in Facebook's privacy defense," The Verge, April 11, 2018, online:https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy

132 MALHOTRA. "IUIPC," *supra* note 111, p. 339.

133 See also KUO, K-M and TALLEY, P. C. "An empirical investigation of the privacy concerns of social network website users in Taiwan," 2014, p. 6, online: https://pdfs.semanticscholar.org/e2c0/e03165b91bdcab6e9e2d9858b5d3be015489.pd

134 MALHOTRA. "IUIPC," *supra* note 111, p. 339.

135 CORREIA, J. and COMPEAU, D. "Information Privacy Awareness (IPA): A Review of the Use, Definition and Measurement of IPA," 50th Hawaii International Conference on System Sciences, 2017, pp. 4023-4024, online: https://pdfs.semanticscholar.org/b9e7/0317060e75bdaf52174391fb1f93e77b5268.pdf

- Knowledge and understanding of current personal information handling practices by online businesses;
- Knowledge and understanding of the technologies used;
- Knowledge and understanding of the relevant legislative and regulatory framework;
- Assessing the impact of those factors on the handling of personal information in a given situation;
- Assessing the impact of actions taken and choices made on the handling of personal information in a given situation.

Other authors have also included Internet users' knowledge of past breaches of their personal information online and those that are likely to occur in the future[136].

Privacy policies

When it comes to Internet users' poor understanding of how their personal information is handled online, and the concerns this creates, the issues surrounding privacy protection policies (sometimes referred to as privacy policies or confidentiality policies) cannot be ignored.

Those documents, which are regularly linked to by windows and banners at the bottom of Web pages, describe an organization's or website's practices regarding the collection, use and disclosure of personal information. While those documents are theoretically "the single most important source of information for users[137]," they are regularly criticized for not really making it as easy as they should for users to understand the information. Why is that?

The documents are too long, which discourages many and makes repeated careful reading unrealistic. A New York Times study of Google's privacy policy exposed the document's drastic evolution over a 20-year period; some thirty different versions, which grew from 600 words in 1999 to 4,000 words in 2019[138]! Reading just one such document will take the average Internet user almost 20 minutes, which makes it all the more implausible[139]. Reading the policies of Facebook, Wikipedia or Netflix exceeds the 20-minute mark each[140].

---

[136] See for example BRECHT, F. *et al*. "Communication Anonymizers: Personality, Internet Privacy Literacy and Their Influence on Technology Acceptance," European Conference on Information Systems 214, 2012, p. 3.
[137] REIDENBERG, J. R. *et al*. Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding," Berkeley Technology Law Journal, vol. 30, 2015, p. 39.
[138] WARZEL, C. and NGU, A. "Google's 4,000-Word Privacy Policy Is a Secret History of the Internet," New York Times, July 10, 2019, online: https://www.nytimes.com/interactive/2019/07/10/opinion/google-privacy-policy.html
[139] That evaluation was made using http://www.combiendemots.com/ from the January 22, 2019 version of Google's policy.
[140] Those evaluations were made using http://www.combiendemots.com/ from the following documents: version of Facebook policy dated April 19, 2018, version of Wikipedia policy dated May 24, 2018, and version of Netflix policy dated April 24, 2019.

The policies are ambiguous, making them difficult to understand. A study by Kaur *et al* of the privacy policies of several thousand websites, including the top 1,000, noted the very common presence of ambiguous terms (*may, generally, appropriate,* etc.)[141]. In fact, nearly 50% of the sentences in the 2,000 documents studied included at least one word described as ambiguous by the authors of the study published in spring 2019[142]. As a result, interpretations, even among experts, can vary widely about the same policy, as reported in a study by Reidenberg *et al*[143].

And the policies are complex. According to a second New York Times study, the complexity of the terms used and the length of many policies' sentences are such that the reading level required is, for the most part, that required for a college or university education. The level required for Airbnb, Twitch and eBay policies is, for example, similar to that required for Immanuel Kant's *Critique of Pure Reason*[144].

2.1.3 The main risks identified by consumers

The literature also identifies a series of more specific risks that consumers are concerned about with respect to their online privacy. Those risks are summarized and put into context in the following pages.

It should be noted that there is a link between the general level of concern about online privacy and the beliefs of Internet users about the risks they face online. With few exceptions, the more concerned Internet users are, the more they will identify risks to their personal information online and the riskier they will consider its online disclosure[145].

It should also be noted that individual consumer concerns are not fixed and can vary considerably depending on the circumstances and especially on the personal information involved. Surveys in the literature generally do not distinguish between types of personal information (e.g., sensitive information) in the questionnaires or in the results.

---

[141] KAUR, J. *et al*. "A comprehensive keyword analysis of online privacy policies," Information Security Journal: A Global Perspective, vol. 27, No. 5-6, 2018, p. 268.
[142] *Ibid.*
[143] "The findings show areas of common understanding across all groups for certain data collection and deletion practices, but also demonstrate very important discrepancies in the interpretation of privacy policy language, particularly with respect to data sharing. The discordant interpretations arose both within groups and between the experts and the two other groups.": REIDENBERG. "Disagreeable Privacy Policies, *supra* note 137, p. 40.
[144] LITMAN-NAVARRO, K. "We Read 150 Privacy Policies. They Were an Incomprehensible Disaster," New York Times, June 12, 2019, online: https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html
[145] KOOHANG, A., PALISZKIEWICZ, J., and GOLUCHOWSKI, J. "Social media privacy concerns: trusting beliefs and risk beliefs," Industrial Management & Data Systems, vol. 118, No. 6, 2018, p. 1214.

2.1.3.1. Information Security Risks

Among the most common risks cited in surveys of Internet users are those related to the security of online information.

However, data security does not pertain a priori to privacy protection. The issue of data security refers to the protections put in place by companies to prevent unauthorized access or loss of data collected, stored and processed by them. The data in question are not necessarily personal information. The issue of online privacy refers only to personal information (i.e., information about an identified or identifiable individual)[146], but covers more than just the security of that information.

So why talk about data security when considering consumers' concerns about their online privacy? Because in practice, consumers do not make this distinction – and neither do legislators – and because a breach in the security of personal information held by a company, for example, can quickly lead to a breach in the privacy of the individual concerned. It is therefore legitimate, indeed essential, for this study to address consumer concerns about data security.

So let's look at the main concerns about this issue that have been identified in past surveys. Many Internet users are concerned that their personal information is stored in an inadequately secure manner[147]. This risk covers both the systems over which they have control (e.g., personal computer, smartphone) and the storage systems offered by companies (e.g., cloud services) or used by companies to store collected, processed or purchased data from another company.

There are concerns about unauthorized access to systems and the information they contain, but also about the loss of information due to technical problems, human error or unforeseen external events (e.g., data centres affected by lightning strikes[148], fires[149] or building collapses[150]).

---

[146] THE INFORMATION AND PRIVACY COMMISSIONER/ONTARIO and DELOITTE & TOUCHE. "The Security-Privacy Paradox: Issues, Misconceptions, and Strategies," August 2003, online: https://www.ipc.on.ca/wp-content/uploads/Resources/sec-priv.pdf; MINORITY HIV/AIDS FUND. "The Difference between Security and Privacy and Why It Matters to Your Program," U.S. Department of Health & Human Services, online: https://www.hiv.gov/blog/difference-between-security-and-privacy-and-why-it-matters-your-program

[147] OFCOM and ICO. "Internet users' experience of harm online: summary of survey research," September 18, 2018, pp. 7-9, online: https://www.ofcom.org.uk/__data/assets/pdf_file/0018/120852/Internet-harm-research-2018-report.pd; KPMG. "Companies that fail to see privacy as a business priority risk crossing the 'creepy line'," November 7, 2016, online: https://home.kpmg/sg/en/home/media/press-releases/2016/11/companies-that-fail-to-see-privacy-as-a-business-priority-risk-crossing-the-creepy-line.html

[148] "Google loses data as lightning strikes," BBC News, April 15, 2015, online: https://www.bbc.com/news/technology-33989384

[149] SAWERS, P. "OVH datacenter disaster shows why recovery plans and backups are vital," VentureBeat, 10 March 2021, online: https://venturebeat.com/2021/03/10/ovh-datacenter-disaster-shows-why-recovery-plans-and-backups-are-vital

[150] GUILBAULT, J-F. "L'infonuagique, nerf du commerce au 21e siècle," Radio-Canada, August 23, 2019, online: https://ici.radio-canada.ca/nouvelle/1267691/infonuagique-commerce-securite-donnees-quebec-analyse-experts

Regarding unauthorized access to personal information, consumers are most concerned about data theft, particularly as a result or by means of cyber attacks (viruses, malware, spyware, Trojan horses[151], etc.)[152]. Consumers are not ultimately concerned about the non-security of databases, but rather about the unauthorized access that could result and the subsequent use that could be made of the personal information contained therein[153].

Cases of personal information hacking on online companies' websites, platforms or servers are frequently in the news. And the amounts of information involved and Internet users targeted can be alarming, as the following examples illustrate:

- 3 billion Yahoo email accounts whose information was hacked in 2013 (contact information, birth dates, phone numbers, encrypted passwords, security questions, etc.)[154]
- 540 million Facebook user files were hacked in 2019[155]
- 383 million Marriott International hotel guest files were hacked in 2018 (contact information, email addresses, passport numbers, payment methods, etc.)[156]
- 145 million files related to eBay users were hacked in 2014 (contact information, encrypted passwords, etc.)[157]
-

Use of personal information for criminal purposes

While consumers regularly raise the distinct issue of data security in privacy surveys, they also tend to include a related issue of criminal use of their personal information (usually as a result of unauthorized access).

---

[151] For explanations of the different types of Trojans (*Backdoor Trojan, Infostealer Trojan, Trojan IM, Ransom Trojan, Fake AV Trojan,* etc.), see: NORTON. "What is a Trojan? Is it a virus or is it malware?", online: https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html (consulted on August 10, 2021).
[152] OFCOM. "Internet users' experience," *supra* note 147, pp. 7-9.
[153] *Ibid.,* p.13; PAINE SCHOFIELD, C. *et al.* "Internet users' perceptions of 'privacy concerns' and 'privacy actions'," International Journal of Human-Computer Studies, vol. 65, 2007, p.531, table 1; CIRA. "Canadians Deserve a Better Internet," June 2019, online: https://www.cira.ca/resources/state-internet/report/canadians-deserve-a-better-internet; MOZILLA. "Hackers, Trackers and Snoops: Our Privacy Survey Results," March 9, 2017, online: https://medium.com/mozilla-internet-citizen/hackers-trackers-and-snoops-our-privacy-survey-results-1bfa0a728bd5
[154] PERLROTH, N. "All 3 Billion Yahoo Accounts Were Affected by 2013 Attack," New York Times, October 3, 2017, online: https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html
[155] SILVERSTEIN, J. "Hundreds of millions of Facebook user records were exposed on Amazon cloud server," CBS News, April 4, 2019, online: https://www.cbsnews.com/news/millions-facebook-user-records-exposed-amazon-cloud-server/
[156] O'FLATHERTY, K. "Marriott CEO Reveals New Details About Mega Breach," Forbes, March 11, 2019, online: https://www.forbes.com/sites/kateoflahertyuk/2019/03/11/marriott-ceo-reveals-new-details-about-mega-breach/#d1045cb155c0
[157] KELLY, G. "eBay Suffers Massive Security Breach, All Users Must Change Their Passwords," Forbes, May 21, 2014, online: https://www.forbes.com/sites/gordonkelly/2014/05/21/ebay-suffers-massive-security-breach-all-users-must-their-change-passwords/#4ef529797492

The surveys indicate a number of concerns about unauthorized use of their information (identity theft[158], unauthorized financial transactions, fraud) and the consequences of that use (financial losses[159], tainted credit reports[160], extortion[161]). There are also concerns about the sale of stolen information, a particularly lucrative market. Research conducted by the BBC Watchdog program revealed, for example, that the value of stolen data had increased significantly in 2019, in some cases tripling[162]. A consumer's bank account, credit card and debit card data would now be worth around $1,500 (€1,025), $50 (€33) and $70 (€46) respectively. Passport data would sell for nearly $3,000 (€2,050) and driver's licence data would sell for $1,400 (€956). More modestly, the cost of Facebook and Netflix account data would only amount to about $20 (€15 at most)[163].

2.1.3.2. Risks related to marketing

Internet users also express concern about the commercialization of their personal information online. They are particularly concerned about profiling[164], exposure to behavioural advertising[165] and the sale of their personal information to third parties[166] as a result of increased tracking of their online activities.

---

[158] NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, *supra* note 130; PAINE SCHOFIELD. "Internet users' perceptions," *supra* note 153, p. 531, table 1; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "2018-2019 Survey of Canadians on Privacy," March 11, 2019, Figure 8, online: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/

[159] OFCOM. "Internet users' experience," *supra* note 147, pp. 7-9 & 13; NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, *supra* note 130; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Qualitative Public Opinion Research with Canadians on Consent," March 2017, online: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/por_201703_consent/

[160] ACCOUNTING TODAY. "One in four Americans victims of information security breaches," April 21, 2015, online: https://www.accountingtoday.com/opinion/one-in-four-americans-victims-of-information-security-breaches-aicpa-survey-finds

[161] CONSUMERS COUNCIL OF CANADA. "Mobile Devices Facing Cyber Threats," June 2013, online: https://www.consumerscouncil.com/site/consumers_council_of_canada/assets/pdf/509822_ccc_cyberthreatsfr.pdf

[162] PARSONS, J. "Revealed: How much your stolen account IDs are worth online," Metro UK, June 6, 2019, online: https://metro.co.uk/2019/06/06/revealed-much-stolen-account-ids-worth-online-9837645/

[163] MIGLIANO, S. "Dark Web Market Price Index 2019," TOP10VPN, June 5, 2019, online: https://www.top10vpn.com/news/privacy/dark-web-market-price-index-2019-june-uk-update/; For more general estimates, see also ELLIS, W. "How Much Does Your Data Cost on the Dark Web? – We Checked," Privacy Australia, June 2, 2019, online: https://privacyaustralia.net/dark-web-personal-data/

[164] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. 2018-2019 Survey, *supra* note 158; MATT, C. & PECKELSEN, P. "Sweet Idleness, but Why? How Cognitive Factors and Personality Traits Affect Privacy-Protective Behavior," 49th Hawaii International Conference on System Sciences, 2016, pp. 174; MOZILLA. "Hackers," *supra* note 153.

[165] OFCOM. "Internet users' experience," *supra* note 147, pp. 7-19; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. 2018-2019 Survey, *supra* note 158, Figure 10.

[166] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Qualitative Research," *supra* note 159; KPMG. "Companies that fail," *supra* note 147.

Profiling

Given the rapid development of technologies that enable the extraction and aggregation of personal information from online users, there is a risk that detailed profiles will be developed about them in a "mosaic effect[167]."

As part of a project on online profiling, the Panoptykon Foundation has developed a classification of information that could be used for this purpose. The Foundation distinguishes between three levels: personal information that a user shares about himself online (on social media, on applications, etc.) and with companies with which the user does business directly; information that is obtained from the basic data and that makes it possible to obtain a portrait of his online behaviour; and information obtained through an algorithmic analysis, using artificial intelligence[168]. Here are some examples of that information (and of the progression of the portrait that can be drawn of the Internet user), according to the levels of information:

Table 3

Examples of personal information collected or inferred during profiling of online consumers, according to the levels of information

Level 1	Level 2	Level 3
Credit card number	Online shopping history and habits	Types of consumers (impulsive, informed, loyal, etc.) Estimated income level
Addresses	Travel habits Device geolocation IP address	New home purchase Mortgage, car loan Unemployment
Search history	Websites visited and content viewed online	Happy events in the family (birth, marriage, etc.) Love interests Political and religious affiliation Health problems
"Likes" and other "reactions"	Ads that the user has clicked on	
Settings of the connected device	How online content is scrolled Typing dynamics (speed, mistakes, etc.)	Signs of depression

[167] MATT. "Sweet Idleness," *supra* note 164, p. 174.
[168] PANOPTYKON FOUNDATION. "Three layers of your digital profile," March 18, 2019, online: https://en.panoptykon.org/articles/three-layers-your-digital-profile; SZYMIELEWICZ, K. "Your digital identity has three layers, and you can only protect one of them," Quartz, January 25, 2019, online: https://qz.com/1525661/your-digital-identity-has-three-layers-and-you-can-only-protect-one-of-them/

Some companies specializing in consumer profiling have developed consumer categories – i.e., typical profiles – on which merchants and marketers can then focus their interventions. For example, the following categories developed in the United States incorporate characteristics related to employment, region, culture, etc.: "Urban Cores (Single City Blues, Hispanic Mix, Inner Cities)," "Affluentials (Young Influentials, New Empty Nests, Boomers & Babies, Suburban Sprawl, Blue-Chip Blues)," and "Inner Suburbs (Upstarts & Seniors, New Beginnings, Mobility Blues, Gray Collars)[169]."

Behavioural advertising

It is possible for advertisers to personalize online advertising on the basis of detailed consumer profiles. This is known as behavioural advertising or targeted advertising. Internet users are thus exposed to advertising likely to suit their tastes and habits and meet their needs or interests.

The use of consumer profiling for advertising purposes can also lead to another phenomenon: pricing of online goods and services that uses algorithms taking into account a customer's personal characteristics (sometimes called personalized pricing)[170]. Prices can thus be adapted to the importance that the consumer attaches to prices in his online consumption habits (*price sensitivity*). It should be noted that this commercial practice is currently used very little by companies, except for the tourism sector[171].

Selling data to third parties

In addition to being used to target potential consumers online, the collection and processing of personal information about Internet users is also a significant source of revenue for some websites and online businesses, as this information can then be sold to third-party companies.

---

[169] ELECTORNIC PRIVACY INFORMATION CENTER. "Privacy and Consumer Profiling," online: https://en.panoptykon.org/articles/three-layers-your-digital-profile (consulted on June 5, 2020).
[170] ZUIDERVEEN BORGESIUS, F. and POORT, J. "Online Price Discrimination and EU Data Privacy Law," Journal of Consumer Policy, vol. 40, 2017, p.348.
[171] EUROPEAN COMMISSION. DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS. "Consumer market study on online market segmentation through personalised pricing/offers in the European Union," June 2018, pp. 43-46, online: https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/aid_and_development_by_topic/documents/synthesis_report_online_personalisation_study_final_0.pdf.

This practice is now widespread. For example, credit card transaction data are regularly sold[172], as are subscribers' geolocation data from the major telecommunications providers, Telus, Rogers and Bell, based on nearby cell towers[173].

But who is buying those data? In 2018, the three providers' joint venture, EnStream, refused to disclose the names of the companies to which those geolocation data were sold.

The mandatory registration of third-party companies that have sold or bought personal data in the State of Vermont over the past few years has provided a picture of the variety of companies involved, which include credit bureaus and companies that specialize in finding or locating people and, not surprisingly, companies that specialize in advertising and marketing[174].

In addition to those companies, there are those whose main activity is specifically the buying and selling of data, i.e. data brokerage companies. There are about 4,000 of them in the world[175], including Acxiom Corporation, one of the largest and probably the best known. In 2012, the company claimed to hold an average of 1,500 types of personal information (*data points*) on some 500 million consumers around the world and to conduct 5 billion data[176] transactions annually. A quick look at a recent promotional document from the company shows that it sells a huge variety of personal information: socio-demographic information (e.g., education, age, marital status), financial information (e.g., annual income, level of financial stability, presence of a mortgage, savings, etc.), identification of goods consumed or owned by individuals (e.g., vehicle and appliance models, food and pharmaceutical products consumed)[177].

---

[172] COHAN, P. "Mastercard, AmEx And Envestnet Profit From $400M Business Of Selling Transaction Data," Forbes, June 22, 2018, online: https://www.forbes.com/sites/petercohan/2018/07/22/mastercard-amex-and-envestnet-profit-from-400m-business-of-selling-transaction-data/#7dea37557722; STURGEON, J. "Grocers are collecting your shopping data-should consumers be wary?," Global News, May 9, 2014, online: https://globalnews.ca/news/1301367/grocers-are-collecting-your-shopping-data-should-consumers-be-wary/

[173] BRAGA, M. "How Rogers, Telus and Bell sell access to your location data to third-party companies," CBC, May 18, 2018, online: https://www.cbc.ca/news/technology/rogers-bell-telus-enstream-location-data-sharing-securus-1.4666739

[174] MELENDEZ, S. and PASTERNACK, A. "Here are the data brokers quietly buying and selling your personal information," Fast Company, March 2, 2019, online: https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information

[175] WEBFX. "What Are Data Brokers - And What Is Your Data Worth?," March 16, 2020, online: https://www.webfx.com/blog/internet/what-are-data-brokers-and-what-is-your-data-worth-infographic/

[176] KROFT, S. "The Data Brokers: Selling your personal information," CBS, March 9, 2014, online: https://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/; SINGER, N. "Mapping, and Sharing, the Consumer Genome," New York Times, June 16, 2012, online: https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?_r=0%20; WEBFX. "What Are Data Brokers," *supra* note 175.

[177] ACXIOM. "Auto: Driving Insights," online: https://www.acxiom.com/wp-content/uploads/2013/10/Industry-Insights-DataPackages.pdf (consulted on July 10, 2021).

2.1.3.3. Reputation and integrity risks

Internet users also note several risks to their online privacy that relate to their reputation and integrity. While the other risks were more likely to occur in the context of economic transactions, these risks are more generally associated with social media, although they are not exclusive to them. These websites are generally structured in a way that makes it easy to identify the individuals targeted or involved in a posting. In addition, the websites use sharing features enabling fast reproduction of the content originally posted and offer features facilitating the search for specific individuals or information[178].

For example, several past surveys have reported a general fear among Internet users of having compromising or embarrassing information about themselves disclosed publicly on the Internet, and ultimately of having their reputation tarnished[179]. This information may concern their political opinions or their medical or sexual history, for example. On this last point, one can think of the phenomenon of *revenge porn*, which consists of disseminating sexual/intimate images or videos without the subject's consent (usually, but not exclusively, following a romantic breakup). According to a 2016 U.S. study, one in 25 people has been a victim or has been threatened with being a victim[180]. The victims are overwhelmingly women[181] and/or people from the LGBTQ community[182].

Information revealed about others online for the purpose of harming them may also concern certain behaviours that are deemed unacceptable in society, or at least by those who denounce them. There are several websites designed to identify and publicly humiliate "offenders" (e.g., Don'tDateHimGirl.com and HollaBackNYC.com, which list men who behave inappropriately, especially on dates or in public[183], BitterWaitress.com, which lists ungenerous restaurant customers[184], and CarpoolCheats.org, which lists "carpool cheaters[185])."

---

[178] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Online reputation What are people saying about me?," January 2016, online: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/or_201601/

[179] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. 2016 Privacy Survey of Canadians, December 2016, Figure 7, online: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/por_2016_12/; OFCOM. "Internet users' experience," *supra* note 147, pp. 7-9.

[180] LENHART, A., YBARRA, M., and PRICE-FEENEY, M. "Nonconsensual image sharing: one in 25 Americans has been a victim of 'revenge porn'," Center for Innovative Public Health Research, memo 12.13.2016, p.4, online: https://datasociety.net/pubs/oh/Nonconsensual_Image_Sharing_2016.pdf

[181] LAIDLAW, E. B. "Online Shaming and the Right to Privacy," Laws 2017, vol. 6, No. 1, p. 5.

[182] LENHART, "Nonconsensual image sharing," *supra* note 180, p. 5.

[183] LEIBOVICH, L. "Don't date him, girl!," Salon, August 7, 2006, online: https://www.salon.com/2006/08/07/dont_date_him_girl/; STONE, G. "Hey, Macho Man: Say Cheese!," Good Morning America, March 12, 2016, online: https://abcnews.go.com/GMA/Technology/story?id=1715494

[184] MOSKIN, J. "The Waiter You Stiffed Has Not Forgotten," New York Times, February 2, 2005, online: https://www.nytimes.com/2005/02/02/dining/the-waiter-you-stiffed-has-not-forgotten.html

[185] CABANATUAN, M. and GATHRIGHT, A. "Commuters' website catches carpool cheats in the act," San Francisco Chronicle, December 22, 2003, online: https://www.sfgate.com/bayarea/article/Commuters-Web-site-catches-carpool-cheats-in-the-2508620.php

It is interesting to note that public humiliation (shaming) and the Internet have a most paradoxical relationship. The authors Laidlaw and Solove explain it this way:

> The internet is a particularly effective place to deploy shaming. In one way, shame sanctions have an important role to play online where laws can be easily circumvented and social norms have a weaker hold. Shaming here has normative force in regulating the rules of behaviour in participating in an online space (…) This is the irony. It is the very weakening of norms in reining in some behavior of users on social media that makes shame sanctions more powerful[186].
>
> Like gossip, shaming has long served as a common practice to keep people from violating society's rules and norms. Shaming helps maintain order and civility. Yet when transplanted to the Internet, shaming takes on some problematic dimensions[187].
>
> Instead of enhancing social control and order, Internet shaming often careens out of control. It targets people without careful consideration of all the facts and punishes them for their supposed infractions without proportionality. Shaming becomes uncivil, moblike, and potentially subversive of the very social order that it tries to protect[188].

Past surveys have also identified several anti-social behaviours that Internet users fear as a result of disclosing their personal information: *cyber-stalking*[189], bullying[190], threats[191] or trolling[192] by other Internet users.

A 2016 Center for Innovative Public Health Research study of U.S. Internet users concluded, for example, that more than two thirds of Internet users had witnessed harassment and bullying on the Internet and that more than one third of Internet users had experienced it[193]. The study lists the many forms that online abuse can take:

- Verbal harassment (insults)
- Spreading false rumors about an Internet user
- Threats to the physical or sexual integrity of an Internet user
- *Brigading* (encouraging and helping others to harm an Internet user)
- *Denial of Service (DoS)* – online attacks *(*flooding or disrupting a network or account to prevent it from functioning for the targeted user)[194]

---

[186] LAIDLAW. "Online Shaming," *supra* note 181, p. 7.
[187] SOLOVE, D. The Future of Reputation: Gossip, Rumor, and Privacy on the Internet, Yale University Press, 2007, p. 12.
[188] *Ibid.,* p. 102.
[189] MOZILLA. "Hackers," *supra* note 153.
[190] OFCOM. "Internet users' experience," *supra* note 147, pp. 7-9.
[191] NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION*, supra* note 130, Figure 2.
[192] OFCOM. "Internet users' experience," *supra* note 147, pp. 7-9.
[193] LENHART, A. *et al*. "Online Harassment, Digital Abuse, and Cyberstalking in America," Center for Innovative Public Health Research, report 11.21.16, pp. 5 and 23, online: https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf; a Pew Research Center survey comes up with relatively similar results (41% victims, 66% witnesses): DUGGAN, M. "Online harassment 2017," Pew research Center, July 11, 2017, online: https://www.pewinternet.org/2017/07/11/online-harassment-2017/
[194] *Ibid.,* pp. 24, 31 and 34.

Added to this list is the recent phenomenon of *swatting*, i.e. (falsely) reporting a crime at an Internet user's address so that police can be sent there, and thus causing him trouble, frightening him or even putting him in danger[195].

Finally, there has also been a rise in cases of online *doxing* (or *doxxing*)[196] in recent years. This practice, which is halfway between damage to reputation and online harassment, consists of disclosing, without consent, personal information about an individual (not necessarily collected illegally), with the aim of harming or humiliating him[197]. This includes disclosing the identity or contact information of protesters[198] or online commentators[199] to people who are hostile to them. What happens next is all too predictable…

2.1.3.4 Risks related to intrusions into daily life

Internet users also identify risks to their online privacy that are more akin to intrusions (unsolicited, of course) into their daily lives[200]. Two elements stand out in the surveys conducted among Internet users on this subject: spam and automated decisions.

Spam

Advertising messages, chain letters, psychic or "inheritance" proposals, bogus business offers, newsletters to which an Internet user has never subscribed, etc.: Unsolicited electronic communications, known as *spam* (or *junk mail*), can take many forms[201].

---

[195] TOGNOTTI, C. "What Is 'Doxxing' And 'Swatting'? You Should Know These Terms & Their Victims," Bustle, February 13, 2015, online: https://www.bustle.com/articles/64275-what-is-doxxing-and-swatting-you-should-know-these-terms-their-victims

[196] Expression that combines the action of "dropping documents" and the .docx format.

[197] "What doxxing is, and why it matters," The Economist, March 10, 2014, online: https://www.economist.com/the-economist-explains/2014/03/10/what-doxxing-is-and-why-it-matters; VIGNEAULT, A. "What is doxxing?," La Presse, March 30, 2019, online: https://www.lapresse.ca/vivre/societe/201903/29/01-5220127-quest-ce-que-le-doxxing.php

[198] On the doxing surrounding the 2017 Charlottville events: BOWLES, N. "How 'Doxxing' Became a Mainstream Tool in the Culture Wars," New York Times, August 30, 2017, online: https://www.nytimes.com/2017/08/30/technology/doxxing-protests.html

[199] WILLIAMS, G. "Twitter's alt-right retaliates against CNN journalist at center of so-called blackmail scandal," Vox, July 5, 2017, online: https://www.vox.com/policy-and-politics/2017/7/5/15924434/twitter-reddit-alt-right-cnn-andrew-kaczynski; HERN, A. "Felicia Day's public details put online after she described Gamergate fears," Guardian, October 23, 2014, online: https://www.theguardian.com/technology/2014/oct/23/felicia-days-public-details-online-gamergate

[200] ARSHAD, J. "Towards a Taxonomy of Privacy Concerns of Online Social Network Sites Users," 2010, p.34, online: https://pdfs.semanticscholar.org/8484/729358966fa3740d8a6e3d382677f6b8a48d.pdf;

[201] Under Canadian anti-spam legislation, those communications are intended to encourage the recipient to engage in a commercial activity (purchase, investment, etc.).): An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain practices that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, S.C. 2010, c. 23, s. 1(1).

Receiving spam is commonly identified by Internet users as a threat to their online privacy[202]. This risk must be distinguished from the risks related to targeted advertising (section 2.1.2.2). This is not the disturbing feeling of being specifically targeted or "known" by the advertiser, but rather the unwanted presence of messages in an Internet user's email box or social media accounts, in what may be their private sphere and may be associated with their "home" in the digital universe. It should be noted that seeing this as a risk is closely related to conceptions of privacy that focus on individuals' ability or possibility to isolate themselves from society, to not be annoyed[203].

Because spam is undeniably annoying. In 2018, approximately 14.5 billion spam messages were sent each day to the email boxes of individuals and companies[204]. Even though the filters developed by email services (Gmail, Hotmail, etc.) are now able to automatically delete the vast majority of those messages[205], receiving unwanted emails is still part of Internet users' daily lives.

But spam is sometimes more than just annoying. It can even lead to major financial consequences, as important as those that would result from identity theft, for example. Spam is regularly used to phish consumers online. Through emails that appear to come from familiar or respectable institutions, Internet users are encouraged to visit seemingly legitimate, but in reality fraudulent, websites where they will provide personal information about themselves[206]. Spam is also occasionally used to transmit malicious software, including ransomware that makes it impossible to access a user's files or systems until he pays a sum of money to those responsible for the attack[207].

---

[202] PAINE SCHOFIELD. "Internet users' perceptions," *supra* note 153, p. 531, table 1; OFCOM. "Internet users' experience," *supra* note 147, pp. 7-9; ELUEZE, I. & QUAN-HAASE, A. "Privacy Attitudes and Concerns in the Digital Lives of Older Adults: Westin's Privacy Attitude Typology Revisited," American Behavioral Scientist, 2018, vol. 62, No. 10, p. 1385.

[203] REJÓN-GUARDIA, F. and MARTÍNEZ-LÓPEZ, F. J. "Online Advertising Intrusiveness and Consumers' Avoidance Behaviors" in MARTÍNEZ-LÓPEZ, F. J., ed, Handbook of Strategic e-Business Management, Springer Berlin Heidelberg, 2014, p. 570; PAINE SCHOFIELD. "Internet users' perceptions," *supra* note 153, p. 534; PODDAR, A., MOSTELLER, J., and ELLEN, P. S. "Consumers' Rules of Engagement in Online Information Exchanges," Journal of Consumer Affairs, vol. 43, No. 3, September 2009, p. 429.

[204] WIGGERS, K. "Gmail is now blocking 100 million more spam emails a day, thanks to TensorFlow," VentureBeat, February 6, 2019, online: https://venturebeat.com/2019/02/06/gmail-is-now-blocking-100-million-more-spam-emails-a-day-thanks-to-tensorflow/

[205] METZ, C. "Google Says Its AI Catches 99.9 Percent of Gmail Spam," Wired, July 9, 2015, online: https://www.wired.com/2015/07/google-says-ai-catches-99-9-percent-gmail-spam/

[206] CANADIAN ANTI-FRAUD CENTRE. "Phishing," online: https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/phishing-hameconnage-eng.htm (consulted on April 10, 2021).

[207] LYNN, S. and THORBECKE, C. "Why ransomware cyberattacks are on the rise," ABC News, June 1, 2021, online: https://abcnews.go.com/Technology/ransomware-cyberattacks-rise/story?id=77832650

Automated or algorithmic decision-making

There are also risks of privacy invasion when decisions are made about individuals on the basis of personal information. Several surveys outline Internet users' concerns about automated decisions being made about them online[208].

The use of algorithms for this purpose has gained in importance in recent years, not least because of the ever-increasing amount of data available[209]. One can think for example of such use in the context of credit or insurance risk assessment[210]. But recent news also shows more surprising examples. The accommodation rental platform Airbnb has developed a tool capable of identifying users deemed "untrustworthy," based on the presence of certain personality traits (narcissism, psychopathy, etc.) that their virtual profile may reveal. The company reportedly performs this risk assessment now, according to available data, before confirming each reservation[211].

There are many fears and criticisms of algorithmic decision-making. On the one hand, some Internet users fear inaccurate or unfair results, either because the analysis includes erroneous information[212], or because the algorithms used reflect certain biases or prejudices[213]. In both cases, the lack of transparency about this decision-making process is disturbing.

On the other hand, some people see in those automated decisions an attack on their human dignity. Reducing a person (in all his complexity) to a number could, according to a study by the European Parliament, be considered a form of alienation or marginalization[214].

---

208 OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. 2018-2019 Survey, *supra* note 158, Figure 7; MATT. "Sweet Idleness," *supra* note 164, p. 173.

209 BARRETT, L. "Deconstructing Data Mining: Protecting Privacy and Civil Liberties in Automated Decision-Making," Georgetown Law Technology Review, vol. 1, No. 1, 2016, p. 154.

210 *Ibid.,* p.154; SWEDLOFF, R. "Risk classification's big data (r)evolution," Connecticut Insurance Law Journal, vol. 21.1, p. 340.

211 HOUSER, K. "Airbnb claims its AI can predict whether guests are psychopaths," The Byte, January 4, 2020, onlinehttps://futurism.com/the-byte/airbnb-ai-predict-psychopaths; BLUNDEN, M. "Booker beware: Airbnb can scan your online life to see if you're a suitable guest," Evening Standard, January 10, 2020, online: https://www.standard.co.uk/tech/airbnb-software-scan-online-life-suitable-guest-a4325551.html; HOLMES, A. "Airbnb has patented software that digs through social media to root out people who display 'narcissism or psychopathy'," Insider, January 6, 2020, online: https://www.businessinsider.com/airbnb-software-predicts-if-guests-are-psychopaths-patent-2020-1

212 MATT. "Sweet Idleness," *supra* note 164, p. 173; Bellman, S. *et al.* "International Differences in Information Privacy Concerns: A Global Survey of Consumers," The Information Society, vol. 20, No. 5, 2004, pp. 317-318.

213 SMITH, A. "Public Attitudes Toward Computer Algorithms," Pew Research Center, November 2018, p.8, online: https://www.pewinternet.org/2018/11/16/public-attitudes-toward-computer-algorithms/; On the topic of algorithm bias, see BAROCAS, S. and SELBST, A. D. "Big Data's Disparate Impact," California Law Review, vol. 104, No. 3, 2016: "Data is frequently imperfect in ways that allow these algorithms to inherit the prejudices of prior decision makers. In other cases, data may simply reflect the widespread biases that persist in society at large. In still others, data mining can discover surprisingly useful regularities that are really just preexisting patterns of exclusion and inequality."

214 EUROPEAN PARLIAMENT. "Understanding algorithmic decision-making: Opportunities and challenges," March 2019, p. I, online: http://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf; see also MATT. "Sweet Idleness," *supra* note 164, p. 173.

2.1.4. Influencing factors

In addition to providing a general portrait of Internet users' concerns about their online privacy, the literature identifies certain personal or situational factors that may influence those concerns. Here is a brief overview.

It should be noted that some of those factors will be discussed in the review of the pan-Canadian survey results in Chapter 3, and that they appear to influence respondents' online behaviour more than their concerns.

2.1.4.1. Differences according to consumers' personal characteristics

Personality traits

Several researchers have studied the influence of personality traits on Internet users' privacy concerns and have identified tendencies. For example, people who are introverted[215], conscientious[216], open-minded[217], friendly[218], anxious or emotionally unstable[219] are more likely to be concerned about their privacy. Note that research has so far focused largely on this taxonomy of personalities (the *Big Five*)[220].

The conception of privacy and the value attached to it

The different conceptions of privacy among Internet users are likely to influence how they perceive risks to their online privacy.

An individual who shares Warren and Brandeis' conception of privacy (the right to be left alone) or Gavison's (others' limited access to oneself and one's private space) may well perceive the receipt of unwanted email as a serious violation of his privacy, while others may be relatively indifferent.

---

[215] In e-commerce situations only: BANSAL, G *et al*. "Do context and personality matter? Trust and privacy concerns in disclosing private information online," Information & Management, vol. 53, 2016, pp. 9-10.
[216] JUNGLAS, I.A., JOHNSON, N.A. and SPITZMÜLLER, C. "Personality traits and concern for privacy: an empirical study in the context of location-based services," European Journal of Information Systems, 2008, vol. 17, No. 4, p. 396; KORZAAN, M. L. and BOSWELL, K. T. "The influence of personality traits and information privacy concerns on behavioral intentions," Journal of Computer Information Systems, vol. 48, No. 4, p. 19; OSATUYI, B. "Personality Traits and Information Privacy Concern on Social Media Platforms," Journal of Computer Information Systems, 2015, vol. 55, No. 4, p. 16.
[217] JUNGLAS. "Personality Traits," *supra* note 216, pp. 393 and 396.
[218] "Agreeableness is a personality trait that reflects social conformity. People with this trait are described as being warm, kind, cooperative, trusting, generous, flexible, considerate, and agreeable": BANSAL. "Do context and personality matter? Bansal, *supra* note 215, pp. 5-10; Korzaan, "The influence of personality traits. "The influence of personality traits," *supra* note 216, p. 19; OSATUYI. Personality Traits," *supra* note 216, p. 16.
[219] BANSAL. "Do context and personality matter? "*supra* note 215, pp. 6 and 11.
[220] JUNGLAS. "Personality Traits," *supra* note 216.

Similarly, an Internet user who shares Posner and Parent's definition of privacy (relating to the secrecy of personal information) would likely be very critical of the ways social media use information and the amount of information that circulates on them. Conversely, this use would be much more acceptable to those who adhere more to the views of Moore, Westin *et al* (relating to control), since an Internet user has a choice as to whether or not to disclose information on those platforms[221].

It is also important to consider that even among those who share a common understanding of privacy, not everyone will attach the same importance to its protection; that will ultimately influence their perception of potential breaches.

> [D]isposition to value privacy [the extent to which a person displays a willingness to preserve his or her private space or to disallow disclosure of personal information to others across a broad spectrum of situations and persons], as a personal characteristics, directly affects the perception of intrusion, and indirectly, through the latter, privacy concerns[222].

Westin has historically segmented consumers into three broad categories based on the importance they place on their privacy[223]. There are "data fundamentalists," who refuse to provide personal information even in exchange for a service or service improvement. For their part, "data pragmatic" Internet users are open to sharing their personal information and will assess on a case-by-case basis whether the service or service enhancement being offered is worth what is being requested. "Data unconcerned" Internet users, as their name suggests, are not interested in or concerned about these issues.

Quan-Haase and Elueze have since proposed a revised segmentation that distinguishes certain privacy-related attitudes within the same category of Internet users[224]:

- "Data fundamentalist" Internet users
- "Intense pragmatist" Internet users, who are bothered by the disclosure of personal information online, but are willing to make occasional compromises when using the Internet
- "Relaxed pragmatist" Internet users, who are less bothered by the disclosure of personal information when using an online service and are therefore more willing to compromise
- "Marginally concerned" but not indifferent Internet users
- "Cynical expert" Internet users, who believe that breaches of their online privacy are beyond their control and inevitable

---

[221] TREPTE, S. and REINECKE, L. "The Social Web as a Shelter for Privacy and Authentic Living" in TREPTE, S. and REINECKE, L., eds., Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 69-70.
[222] XU, H. *et al.* "Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View," ICIS 2008 Proceedings. Paper 6, p. 6.
[223] AXCIOM. "Global data privacy," *supra* note 130, p. 6.
[224] ELUEZE. "Privacy Attitudes and Concerns in the Digital Lives of Older Adults," *supra* note 202, pp. 1378-1383.

Personal privacy history

Studies confirm the influence of Internet users' personal privacy history on their level of privacy concerns. Previous experience with a privacy breach would lead to a consumer's greater level of concern, both online[225] and offline[226].

The level of online privacy literacy

Internet users' knowledge of companies' online practices is reportedly another factor that influences their level of concern about online privacy protection and about certain risks. It is difficult, however, to identify a precise correlation[227].

On the one hand, one of the most recurring concerns of Internet users is their general lack of knowledge and understanding of how personal information is handled online. On the other hand, the authors note that the value placed by each individual on his online privacy is positively influenced by his level of literacy on the subject[228]. The more risk-aware an Internet user is, the more he values privacy and is concerned about online personal information collection practices, about intrusions into his online privacy. But at the same time, an Internet user who is not informed about companies' practices, but who would like to be, will also be more concerned about his online privacy[229].

Gender

Since there are differences in Internet use between men and women, authors have looked at the influence of gender on Internet users' concerns about their online privacy. While not unanimous[230], the literature suggests that, in general, women are more concerned about their online privacy than men[231].

---

[225] AWAD, N. F. and KRISHNAN, M. S. "The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization," MIS Quarterly, vol. 30, No. 1, 2016, p. 24; XU, H. *et al.* "Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services," Information Systems Research, vol. 23, No. 4, 2012, p. 1358; YEH, C-H. *et al*. "What drives internet users' willingness to provide personal information?", Online Information Review, vol. 42, No. 6, 2018, p. 931; CHO H., RIVERA-SANCHEZ M. and LIM S. S. "A multinational study on online privacy: global concerns and local responses," New Media & Society, vol. 11, No. 3, p. 406.
[226] HONG. "Drivers and Inhibitors of Internet Privacy Concern," *supra* note 98.
[227] OMRANI, N. and SOULIÉ, N. "Culture, Privacy Conception and Privacy Concern: Evidence from Europe before PRISM," 2017, International Telecommunications Society, p. 4.
[228] XU. "Examining the Formation of Individual's Privacy Concerns," *supra* note 222, pp. 6-7.
[229] KUO. "Taiwan," *supra* note 133, p. 13.
[230] See LEE, H. *et al*. "Information privacy concerns and demographic characteristics: Data from a Korean media panel survey," Government Information Quarterly, vol. 36, No. 2, 2019, p. 296.
[231] GRUBBS HOY, M. and MILNE, G. "Gender Differences in Privacy-Related Measures for Young Adult Facebook Users," Journal of Interactive Advertising, vol. 10, No. 2, 2010, p. 33; BARTEL SHEEHAN, K. "An investigation of gender differences in on-line privacy concerns and resultant behaviors," Journal of Interactive Marketing, vol. 13, No. 4, 1999, pp. 30-32; FOGEL, J. and NEHMAD, N. "Internet Social Network Communities: Risk Taking, Trust and

In a study focusing on gender differences regarding privacy on social media, Tifferet proposed some explanations for the higher level of concern among women, including a generally higher level of anxiety among women[232] and greater vulnerability to threats to their privacy, both online and offline (particularly those related to their reputation and their physical and psychological integrity)[233].

Age and generation

It is recognized that members of different generations may differ considerably in their experience, education or socialization[234], but what about their Internet use and, more specifically, their privacy on the Internet today?

Some commentaries and editorials have suggested that the sustained use of social media by younger generations is a sign of their lack of concern for their online privacy;[235] however, that isn't so clear according to the available literature and data. The few studies that have looked at the topic have indeed found conflicting results[236].

2.1.4.2. Regional and cultural differences

Some international surveys have noted considerable differences in the level of concern among Internet users depending on their nationality or place of residence. For example, Internet users in Eastern and Northern Europe are generally less concerned about their online privacy than those in Central Europe[237]. Similarly, Internet users in Western countries, such as the United States and Australia, are more concerned about their online

---

Privacy Concerns," Computers in Human Behavior, vol. 25, 2009, p. 157; MOSCARDELLI, D. and DIVINE, R. "Adolescents' Concern for Privacy When Using the Internet: An Empirical Analysis of Predictors and Relationships With Privacy-Protecting Behaviors," Family and Consumer Sciences Research Journal, vol. 35, No. 3, 2007, p. 243; WILLS, C. E. and ZELJKOVIC, M. "A personalized approach to web privacy: awareness, attitudes and actions," 2011, p. 11, online: http://web.cs.wpi.edu/~cew/papers/imcs11.pdf

[232] TIFFERET, S. "Gender differences in privacy tendencies on social network sites: A meta-analysis," Computers in Human Behavior, vol. 93, 2018, p. 4

[233] *Ibid.* , p. 6.

[234] OBAL, M. and KUNZ, W. "Trust development in e-services: A cohort analysis of Millennials and Baby Boomers," Journal of Service Management, vol. 24, No. 1, 2013.

[235] See for example: MCCULLAGH, D. "Why no one cares about privacy anymore," Cent, March 12, 2010, online: https://www.cnet.com/news/why-no-one-cares-about-privacy-anymore/; NUSSBAUM, E. "Say Everything," New York Magazine, February 2, 2007, online: http://nymag.com/news/features/27341/; for example, Mark Zuckerberg claimed in 2010 that privacy was no longer a social norm with the rise in popularity of social media: JONHNSON, B. "Privacy no longer a social norm, says Facebook founder," The Guardian, January 11, 2010, online: https://www.theguardian.com/technology/2010/jan/11/facebook-privacy

[236] BERGSTRÖM, A. "Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses," Computers in Human Behavior, vol. 53, 2015, p. 420.

[237] CECERE, G., LE GUEL, F. and SOULIÉ, N. "Perceived Internet privacy concerns on social networks in Europe," Technological Forecasting and Social Change, vol. 96, 2015, pp. 284.

privacy than those in Asian countries, such as India and South Korea[238]. How can these differences be explained?

Based on Hofstede's theory of cultural dimensions[239], several studies have noted the particular influence of three dimensions on Internet users' privacy concerns:

- A society's Individualism or collectivism
- A society's equality or inequality ("power distance")
- A society's "masculinity"

According to those studies, the level of concern about online privacy is generally higher in societies characterized by its members' strong individualism[240]. Unlike members of collectivist societies, who are more committed to their common destiny, organization and goals, Internet users from individualist societies would attach more value to their independence from the community, hence a greater desire to protect their privacy online and offline[241].

Members of societies that place more importance on "stereotypical male values" also show a higher level of concern for their online privacy[242]. These values generally relate to materialism, ambition, and competitiveness (as opposed to stereotypical female values that focus more on human relationships)[243].

Similarly, members of a society in which power is unequally distributed would be more concerned about their online privacy[244]. There would be a greater sense of distrust of others in such societies, which again may explain a greater desire to protect one's privacy[245].

Some studies offer additional nuances on the subject. A study by Bellman *et al* concluded, for example, that cultural differences influence only certain concerns of Internet users (e.g., database errors) and not in a generalized way[246]. Globalization and the development of diasporas may also reduce the accuracy of this type of analysis, according to Cho, Rivera-Sanchez and Lim[247].

---

[238] CHO. "A multinational study," *supra* note 225, pp. 404-405.
[239] HOFSTEDE, G. Culture's consequences: Comparing values, behaviors, institutions, and organizations across nations, 2nd ed., Sage Publications, 2001.
[240] CHO. "A multinational study," *supra* note 225, p. 411; MILTGEN C. L. & GUILLARD, D. P. "Cultural and generational influences on privacy concerns: a qualitative study in seven European countries," European Journal of Information Systems, vol. 23, 2014, p.21 *a contrario.* Cecere *et al.* arrive at a different result on the subject: CECERE. "Perceived Internet privacy concerns," *supra* note 237, p. 284.
[241] HUANG, H-Y. & BASHIR, M. "Privacy by region: Evaluation online users' privacy perceptions by geographical region," 2016, p.974; CHO. "A multinational study," *supra* note 225, p. 411.
[242] CECERE. "Perceived Internet privacy concerns," *supra* note 237, p. 284.
[243] OMRANI. "Culture, Privacy Conception and Privacy Concern," *supra* note 227, p. 5; HOFSTEDE, G. "The 6-D model of national culture," online: https://geerthofstede.com/culture-geert-hofstede-gert-jan-hofstede/6d-model-of-national-culture/ (consulted on March 28, 2021).
[244] CECERE. "Perceived Internet privacy concerns," *supra* note 237, p. 284; OMRANI. "Culture, Privacy Conception and Privacy Concern," *supra* note 227, p. 12.
[245] CECERE. "Perceived Internet privacy concerns," *supra* note 237, p. 278.
[246] BELLMAN. "International Differences," *supra* note 212, p. 320.
[247] CHO. "A multinational study," *supra* note 225, p. 411.

Lastly, there are also differences according to place of residence due to the level of privacy regulation. In general, Internet users who are most concerned about their online privacy come from states with "moderate" regulation. Internet users who come from a state that has a high degree of intervention in the privacy practices of businesses will be less concerned, presumably because the most objectionable practices are prohibited and adequately addressed. But Internet users from states with little or no privacy regulation will also be less concerned about their online privacy[248]. In this case, it is difficult to determine whether the inaction of local legislators is due to a lack of public interest or whether the opposite is true...

2.1.4.3. Differences in circumstances

Internet users' level of concern about their online privacy will also vary from time to time, depending on the specific circumstances in which they find themselves.

Thus, the nature of personal information requested or obtained from an Internet user online will influence his level of concern for privacy at that moment. Personal information that can be collected online falls into three categories: public, private and sensitive. Sensitive personal information is a narrow category of private information, in that its disclosure is particularly likely to harm the individual financially or socially[249].

The more sensitive the information, the more likely its collection or use online will increase an individual's overall level of concern for online privacy[250].

It should be noted that, while some laws list or define what information will be considered sensitive[251], there is no general consensus on what characteristics would cause personal information to be systematically considered sensitive information[252]. The assessment of information "sensitivity" could therefore vary from one Internet user to another. We will come back to this in the analysis of our Canada-wide survey results.

In addition to the nature of the information involved, the entity that initiates a request for consent to collect or use the data influences Internet users' level of concern[253]. For example, a website's reputation (expertise in products and services, etc.) and an Internet user's feeling of familiarity reduce his level of concern[254]. The type of websites involved also

---

[248] MILBERG, S. J. *et al.* "Values, personal information privacy, and regulatory approaches," Communications of the ACM, vol. 38, No. 12, 1995, p. 72.
[249] BANSAL. "Do context and personality matter?", *supra* note 215, p. 3.
[250] HONG. Drivers and Inhibitors of Internet Privacy Concern," *supra* note 98; KAYHAN, V. O. & DAVIS, C. J. "Situational Privacy Concerns and Antecedent Factors," Journal of Computer Information Systems, vol. 56, No. 3, 2016, p. 233.
[251] See for example: PIPEDA, *supra* note 76, Schedule 1, s. 4.3.4.
[252] WIRTH, J. *et al*. "Perceived information sensitivity and interdependent privacy protection: A quantitative study," Electronic Markets, vol. 29, No. 3, 2019, p. 362.
[253] KAYHAN. "Situational Privacy Concerns," *supra* note 250, p. 229.
[254] LI, Y. "The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. Decision Support Systems," Decision Support Systems, 2013, p. 350.

has an influence. Generally, disclosing personal information to a transactional website will cause more concern than disclosing it to a relational website (social media)[255].

From the results of the survey conducted as part of this research, we note that there are also differences in Internet users' level of concern and possibly in their specific types of concerns depending on the method or tool used for connecting to the Internet (computers, cell phones, connected objects, etc.). The literature offers very little detail or clarification on this subject.

2.2. Overview of Online Privacy Protections Available to Consumers

Surveys of Internet users identify many of the behaviours or actions they favour to protect their privacy online[256]. In addition, there is advice provided by experts and the media. This section provides an overview of the main behaviours and measures that Internet users can adopt to better protect their privacy, according to the various risks identified above. It should be noted that this is not a technical study of the actual effectiveness of the protective measures that Internet users may use.

Privacy protections can be divided into two broad categories: passive and active[257]. Passive measures avoid or reduce possible uses of the Internet. The Internet user thus tries to avoid infringements of his online privacy by rejecting the riskiest situations and activities or, even more drastically, by simply withdrawing from the Internet. Active measures, which are more technical[258], concern self-protection behaviours adopted by Internet users as part of their (continuous) use of the Internet.

---

[255] TANG, J-H. and LIN, Y-J. "websites, Data Types and Information Privacy Concerns: A Contingency Model," Telematics and Informatics, vol. 34, 2017, p. 1279.
[256] CENTER FOR INTERNATIONAL GOVERNANCE INNOVATION. "Global Survey," *supra* note 101, Part I and II, p. 55; MADDEN, M. and RAINIE, L. "Americans' Attitudes About Privacy, Security and Surveillance," Pew Research Center, May 20, 2015, pp. 33-34, online: https://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/; MADDEN, M. and RAINIE, L. Anonymity, Privacy, and Security Online, Pew Research Center, September 2013, online: https://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online; NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, *supra* note 130; MALWAREBYTES LABS. "Labs survey finds privacy concerns, distrust of social media rampant with all age groups," March 5, 2019, online: https://blog.malwarebytes.com/security-world/2019/03/labs-survey-finds-privacy-concerns-distrust-of-social-media-rampant-with-all-age-groups/
[257] BARTH, S. "The privacy paradox - Investigating discrepancies between expressed privacy concerns and actual online behavior - A systematic literature review," Telematics and Informatics, vol. 34, No. 7, 2017.
[258] Park distinguishes between technical and social behaviour rather than passive and active behaviour: PARK, Y. J. "Digital literacy and privacy behavior online," Communication Research, vol. 40, No. 2, 2013, pp. 222 and 226.

2.2.1. Passive online privacy measures

2.2.1.1. Reduction of Internet use

There were some 4.44 billion Internet users worldwide in 2019[259]. The most drastic behaviour they could adopt to further protect their privacy would be to stop using the Internet entirely. Of course, this is not the most popular behaviour! And these days, it's hard for most people to even consider it. "Disconnection and remaining in society are mutually incompatible": That's how an expert consulted by the Pew Research Center put it[260].

Nevertheless, we observe that there is indeed a movement toward temporary Internet disconnection from the Internet (or more specifically from social media), sometimes referred to as "digital detox[261]." However, this practice appears to be based on health considerations (addiction, stress, posture, attention span, fear of missing out, insomnia, etc.)[262] and not on privacy.

While voluntary disconnection from the Internet remains marginal, we note some concrete examples.

For example, some consumers are choosing to purchase older cell phones or newer models that are not "smart" in order to avoid connecting to the Internet and thus limit the collection of information about them through that network[263]. In 2018, a British media outlet reported that sales of phones that cannot connect to the Internet increased more than those of smartphones[264].

Some Internet users also avoid accessing the Internet through a public Wi-Fi connection, given the lower security that this type of connection provides for personal information

---

[259] MORGAN, S. "Humans On The Internet Will Triple From 2015 To 2022 And Hit 6 Billion," CyberSecurityVentures, July 18, 2019, online: https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/

[260] RAINIE, L. and ANDERSON, J. "Theme 2: Unplugging isn't easy now, and by 2026 it will be even tougher," Pew Research Center, June 6, 2017, online: https://www.pewresearch.org/internet/2017/06/06/theme-2-unplugging-isnt-easy-now-and-by-2026-it-will-be-even-tougher/

[261] CHEN, B. X. "It's Time for a Digital Detox. (You Know You Need It.)," New York Times, November 25, 2020, online: https://www.nytimes.com/2020/11/25/technology/personaltech/digital-detox.html

[262] FOX, M. "8 Reasons Why You Should Unplug One Day A Week," Forbes, September 24, 2019, online: https://www.forbes.com/sites/meimeifox/2019/09/24/8-reasons-why-you-should-unplug-one-day-a-week/?sh=75aa3b3b1b79; "The benefits of unplugging from electronics," Adventist Health, March 14, 2019, online: https://www.adventisthealth.org/blog/2019/march/the-benefits-of-unplugging-from-electronics/;

[263] VOINIGESCU, E. "Basic ways to help protect your personal data online," April 11, 2019, online: https://www.cbc.ca/life/culture/basic-ways-to-help-protect-your-personal-data-online-1.5094766; BOGOST, I. "The Wisdom of Nokia's Dumbphone," The Atlantic, February 28, 2017, online: https://www.theatlantic.com/technology/archive/2017/02/the-wisdom-of-the-dumbphone/518055/

[264] HOSIE, R. "'Dumbphone' sales rise as people seek to disconnect and be more mindful," the Independent, August 20, 2018, online: https://www.independent.co.uk/life-style/dumb-phones-sales-rise-disconnect-technology-mindfulness-social-media-a8499086.html

circulating through it[265] (due to the lack of encryption on most public access points[266]). Indeed, there are reportedly risks that a device connecting to an unsecured network could be hacked or hijacked through the creation of dummy access points[267].

2.2.1.2. Reduction of online consumption activities

While not entirely foregoing Internet use or some of its access modes, some Internet users are choosing to limit their consumption activities and transactions online. For example, 15% of Canadians don't shop online and just under a third don't contact their bank via the Internet, according to CIRA's most recent data[268]. It should also be noted that, as was the case with temporary Internet disconnection, the studies don't show that privacy considerations are a major factor in some people's choice not to participate in e-commerce (difficulty of use and lack of interest in the goods and services offered would be more important)[269].

The choice of websites on which consumers will actually make purchases and other transactions appears to be more influenced by privacy considerations. On the recommendation of experts, many consumers only use encrypted websites or platforms, to reduce the risk that personal information they provide will be hacked[270]. The Web address of those websites is preceded by the *HTTPS* designation, which is a secure extension of the *HTTP* protocol, and a padlock or key symbol is found near the address.

---

[265] NIELD, D. "Simple Steps to Protect Yourself on Public Wi-Fi," Wired, August 5, 2018, online: https://www.wired.com/story/public-wifi-safety-tips/

[266] FEDERAL TRADE COMMISSION. "Tips for Using Public Wi-Fi Networks," March 2014, online: https://www.consumer.ftc.gov/articles/0014-tips-using-public-wi-fi-networks

[267] PIERCE, D. "Public Wi-Fi Is Safer Than Ever-But You Still Need to Be Careful," Wall Street Journal, August 4, 2019, online: https://www.wsj.com/articles/public-wi-fi-is-safer-than-everbut-you-still-need-to-be-careful-11564923600

[268] CIRA. "Canada 2020 Internet Resource Kit," 2020, online: https://www.cira.ca/fr/resources/dossier-documentaire/dossier-documentaire-sur-internet-au-canada-2020

[269] See for example: MOHAMMED, Z. A., and TEJAY, G. P. "Examining privacy concerns and ecommerce adoption in developing countries: The impact of culture in shaping individuals' perceptions toward technology," Computers & Security, vol. 67, 2017, p.267 (hypotheses 3(b) and 3(c) rejected); MCCLOSKEY, D. "Evaluating Electronic Commerce Acceptance with the Technology Acceptance Model," Journal of Computer Information Systems, vols. 44, No. 2, 2004, p. 53.

[270] FEDERAL TRADE COMMISSION. "Computer Security," June 2017, online: https://www.consumer.ftc.gov/articles/0009-computer-security; SILVER, J. "20 ways to keep your internet identity safe from hackers," The Guardian, May 12, 2013, online: https://www.theguardian.com/technology/2013/may/12/20-ways-keep-internet-identity-safe; EDUCALOI. "Achats en ligne: 6 précautions à prendre," online: https://www.educaloi.qc.ca/capsules/achats-en-ligne-6-precautions-prendre (consulted on September 14, 2021).

2.2.1.3. Reducing the disclosure of personal information online

Beyond minimizing consumer actions, which is primarily aimed at protecting financial privacy, consumers can take a variety of steps to reduce the online dissemination of other types of information about themselves.

Not surprisingly, social media are particularly targeted in that regard, ranging from the use of false names when registering[271] to the complete closure of accounts on those platforms[272]. More generally, many consumers are choosing to reduce the amount of personal information they share on a daily basis with their subscribers on those platforms. As the FTC reminds us, some apparently trivial information can ultimately be used by fraudsters attempting to steal an individual's identity[273].

Some practices of spreading inaccurate information on social media are particularly elaborate. For example, the website *Fakenamegenerator.com* offers to create a complete fictitious identity for free. Name, address, date of birth, astrological sign, mother's name, favourite car, blood type, employer, email address, etc. Everything is there... and everything is fake, but plausible! For the phone number, it is recommended to provide numbers used in movies and series, which then have very little chance of actually being in service[274].

Others choose instead to "drown out" their real personal information by adding incorrect hobbies or preferences to their accounts or by subscribing to Web pages or accounts of celebrities or businesses that don't match their real interests. "The trick is to populate your Facebook with just enough lies as to destroy the value and compromise Facebook's ability to sell you," Forbes reports[275].

Finally, it is recommended to avoid logging in to other services through a social media account[276]. This way of doing things, called *social login*, certainly simplifies the Internet user's life by avoiding the need to fill out forms and memorize passwords, but it is not without consequences. It allows the companies to which the individual connects to have access to his profile and thus to more personal information – on his interests, preferences

---

[271] O'REILLY, D. "Enhance privacy by being deliberately inaccurate," CNET, October 10, 2013, online: https://www.cnet.com/how-to/enhance-privacy-by-being-deliberately-inaccurate/
[272] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Staying safe on social media," August 1, 2019, online: https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/online-privacy/social-media/02_05_d_74_sn/
[273] FEDERAL TRADE COMMISSION. "How to Keep Your Personal Information Secure," July 2012, online: https://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure
[274] HOPPING, C. and IRVINE, R. "How to stay anonymous online," IT Pro, August 9, 2018, online: https://www.itpro.co.uk/privacy/30584/how-to-stay-anonymous-online
[275] HILL, K. "Fooling Facebook: Telling Lies To Protect Your Privacy," Forbes, September 7, 2012, online: https://www.forbes.com/sites/kashmirhill/2012/09/07/fooling-facebook-telling-lies-to-protect-your-privacy/#49622531158b
[276] DREBES, L. "How Social Login Is Changing Business--and Your Privacy," Forbes, February 28, 2012, online: https://www.forbes.com/sites/forbesleadershipforum/2012/02/28/how-social-login-is-changing-business-and-your-privacy/#43497a2d7485; MATSAKIS, L. "The Security Risks of Logging in With Facebook," Wired, April 19, 2018, online: https://www.wired.com/story/security-risks-of-logging-in-with-facebook/

and political and religious affiliations, for example – than he would have provided by logging in manually.

2.2.1.4. Non-consultation of certain contents

Faced with the risk of falling victim to a computer virus and having their computer, tablet or smartphone compromised and their personal information hacked, many consumers are cautious about the content they access. They are not exploring certain websites or using applications that they feel are less secure[277], and they are avoiding opening emails from unknown recipients or opening the hyperlinks therein[278].

2.2.2. Active online privacy measures

2.2.2.1. Using antivirus software and installing a firewall

Active measures to protect the security of connected devices and online privacy include the use of antivirus software and firewalls on computers, tablets and smartphones. We will see below that this is a very popular protection tool for Canadian consumers.

An antivirus program is software that can detect, remove or take other measures to counter the action of malicious software files (*malware*), such as computer viruses, Trojans and worms[279]. A firewall, on the other hand, filters traffic from the outside and protects a computer system from external threats only. A firewall can prevent a hacker from accessing a device and using it without the owner's knowledge[280]. Note that most antivirus software includes a firewall. Similarly, the Microsoft and Mac OS operating systems have built-in firewalls.

Unfortunately, using an antivirus can sometimes lead, paradoxically, to violations of the user's privacy, due to the provider of the tool itself! The free antivirus company AVG (Avast), which has some 400 million users, has made headlines in recent years by admitting that it sold its users' browsing and search history to third parties[281]. It's normal for an antivirus to monitor a user's Internet traffic in order to identify and block potential computer intrusions;

---

[277] See on this subject: MEDIATI, N. "The 17 Most Dangerous Places on the Web," PCWorld, September 26, 2010, online: https://www.pcworld.com/article/206107/most_dangerous_places_on_the_web.html
[278] See, for example, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Protecting your privacy online," August 2018, online: https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/online-privacy/social-media/02_05_d_74_sn/
[279] DEPARTMENT OF JUSTICE (STATE OF CALIFORNIA). "Protect Your Computer From Viruses, Hackers, and Spies," online: https://oag.ca.gov/privacy/facts/online-privacy/protect-your-computer (consulted on July 15, 2021).
[280] *Ibid.*
[281] TAYLOR, S. "Is Your Antivirus Software Spying on You?", Restore Privacy, February 4, 2019, online: https://restoreprivacy.com/antivirus-privacy/; TEMPERTON, J. "AVG can sell your browsing and search history to advertisers," Wired UK, September 18, 2015, online: https://www.wired.co.uk/article/avg-privacy-policy-browser-search-data; MIHALCIK, C. "Antivirus firm Avast is reportedly selling users' web browsing data," CNET, January 27, 2020, online: https://www.cnet.com/news/antivirus-firm-avast-is-reportedly-selling-users-web-browsing-data/

the fact that it then sells this data to companies such as L'Oréal, Home Depot and Pepsi is considerably less normal![282]

2.2.2.2. Software updates

It is also recommended to regularly update – manually, or automatically when possible – one's devices' software and operating systems. Those updates often serve to remedy a system flaw or vulnerability that could be exploited by a hacker and that has been discovered or reported to the company[283]. According to an article in the New York Times, "these security updates are typically far better at thwarting hackers than antivirus software[284]."

2.2.2.3. Customizing privacy settings

It is also recommended that the privacy settings of the various components involved in Internet use (operating systems of connection devices, connected objects, browsers, applications, firewalls, cloud services, etc.) be adapted to ensure that the maximum protection standards available[285] are applied. The Office of the Privacy Commissioner of Canada recommends that users regularly review the settings selected[286].

Tightening default settings is also of interest when it comes to social media, where public access to postings can be changed or adapted to the user's choice,[287] among other things.

---

[282] COX, J. "Leaked Documents Expose the Secretive Market for Your Web Browsing Data," Vice, January 27, 2020, online: https://www.vice.com/en_us/article/qjdkq7/avast-antivirus-sells-user-browsing-data-investigation
[283] GOSAFEONLINE (SINGAPORE GOVERNMENT AGENCY). "Cyber Tip - Update Your Software Promptly," September 4, 2019, online: https://www.csa.gov.sg/gosafeonline/go-safe-for-me/homeinternetusers/update-software-asap; IDENTITY THEFT RESOURCE CENTER. "What are security patches and why are they important?," June 17, 2012, online: https://www.idtheftcenter.org/what-are-security-patches-and-why-are-they-important/
[284] KLOSOWSKI, T. "How to Protect Your Digital Privacy, Privacy Project," New York Times, online: https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy
[285] *Ibid*; HODGE, R. "Browser privacy settings you need to change right away: Chrome, Firefox and more," CNET, June 6, 2021, online: https://www.cnet.com/tech/services-and-software/browser-privacy-settings-you-need-to-change-right-away-chrome-firefox-and-more/; OSBORNE, C. and WHITTAKER, Z. "Cybersecurity 101: Protect your privacy from hackers, spies, and the government," ZDNet, December 8, 2020, online: https://www.zdnet.com/article/online-security-101-how-to-protect-your-privacy-from-hackers-spies-and-the-government/; GERMAIN, T. "How to Use Google Privacy Settings," Consumer Reports, June 11, 2021, online: https://www.consumerreports.org/privacy/how-to-use-google-privacy-settings/
[286] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Tips for using privacy settings," March 2019, online: https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/online-privacy/gd_ps_201903/
[287] STERN, T. & KUMAR, N. "Improving privacy settings control in online social networks with a wheel interface," Journal of the Association for Information Science and Technology, vol. 65, No. 3, 2014, p. 525; GERMAIN. "How to Use Facebook Privacy Settings," *supra* note 285.

2.2.2.4. Deleting the browsing history and cookies

When people surf the Internet, their browsers usually store a lot of data, such as where they log in, what websites they visit, and what passwords and other information they enter on those websites. It is recommended that users regularly delete their browsing history, cache (a temporary memory system that facilitates the display of previously viewed Web pages) and cookies from their various devices.

It should also be noted that tracking Internet users remains possible despite the deletion of browsing cookies, particularly through device fingerprinting techniques (e.g., *canvas fingerprinting*)[288]. Those techniques were developed in response to the increasingly frequent rejection of cookies by Internet users and the cookies' inaccuracy[289].

2.2.2.5. The variety of passwords used and regular change

The majority of Internet users reuse the same passwords for several accounts or use passwords considered "weak" or insecure[290]. According to a NordPass analysis of hundreds of thousands of Internet users' passwords, the most common password is still "123456[291]." The password "password" is also among the favourites.

Using simple and predictable passwords exposes Internet users to the risk of having their account (easily) hacked and their personal data stolen and used without their knowledge. Using the same password for several accounts amplifies this risk, given *credential stuffing* cyberattacks. They involve making large-scale login requests on the Web after obtaining an individual's online account username and password. If the individual reuses the username and password for several accounts, the latter may be compromised[292].

---

[288] TANNER, A. "The creepy web tracking technology that will replace cookies," Globe & Mail, June 18, 2013, online: https://www.theglobeandmail.com/technology/business-technology/the-creepier-web-tracking-technology-that-will-replace-cookies/article12632904/
[289] *Ibid.*
[290] See on this subject: WASH, R. *et al.* "Understanding Password Choices: How Frequently Entered Passwords Are Re-used across websites," Symposium on Usable Privacy and Security, 12th ed,, 2016, online: https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-wash.pdf
[291] HO, S. "If your password is on this list, you should change it," CTV News, November 18, 2020, online: https://www.ctvnews.ca/sci-tech/if-your-password-is-on-this-list-you-should-change-it-1.5193720
[292] *Ibid*; MUELLER, N. "Credential stuffing, Open Web Application Security Project," online: https://owasp.org/www-community/attacks/Credential_stuffing# (consulted on June 15, 2021).

In addition to recommending the selection of a separate complex password for each account[293], some experts encourage the regular updating of passwords[294]. However, this last proposal is not unanimous, since for several years there have been recommendations against changing passwords unless they are compromised[295]. Internet users would indeed be inclined to opt for less secure passwords after a few changes, for lack of ideas.

Using a password manager

Many Internet users use password managers to ensure the diversification and complexity of their passwords[296]. Those tools can generate multiple secure passwords (combinations of numbers, letters and symbols) for the Internet user and store them in one place. A user will therefore have only one password to remember, that of the application, whose access is encrypted. Some password managers also offer automatic password changes on certain websites after a predetermined period[297]. In 2019, the four most popular password managers, 1Password, Dashlane, KeePass and LastPass, had some 61.5 million individual users worldwide[298].

While using those tools is generally recommended by experts, it is not entirely without risk; if the application's password is compromised, then so are all the user's passwords! In fact, several studies, including one published in 2020 and produced by researchers at York University, have found a series of security flaws that can be exploited by hackers, especially in this type of applications intended for the Windows 10 operating system and

---

[293] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Be privacy powerful: Use strong passwords," July 29, 2019, online: https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/online-privacy/video_pw/; LORD, N. "101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Safe in 2019," Digital Guardian, July 15, 2019, online: https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe; ELLIOTT, M. "7 Common Security Mistakes You're Probably Making," CNET, July 9, 2017, online: https://www.cnet.com/how-to/online-security-mistakes-youre-probably-making/; POLK, R. "The Lazy Person's Guide to Better Online Privacy," Internet Society, January 28, 2018, online: https://www.internetsociety.org/blog/2018/01/lazy-persons-guide-better-online-privacy/

[294] FOWLER, B. "Tips for Better Passwords," Consumer Report, May 2, 2019, online: https://www.consumerreports.org/digital-security/tips-for-better-passwords/; COMMISSION D'ACCÈS À L'INFORMATION. "Le courrier électronique," online: http://www.cai.gouv.qc.ca/documents/CAI_FI_courrier_electronique.pdf (consulted on June 15, 2021).

[295] EVANS, J. "Password expiration is dead, long live your passwords," Techncrunch, June 2, 2019, online: https://techcrunch.com/2019/06/02/password-expiration-is-dead-long-live-your-passwords/; CRANOR, L. "Time to rethink mandatory password changes," FTC, March 2, 2016, online: https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes; HOFFMAN, C. "Should You Change Your Passwords Regularly?," How-to-Geek, September 22, 2016, online: https://www.howtogeek.com/187645/htg-explains-should-you-regularly-change-your-passwords/

[296] CHAIKIVSKY, A. "Everything You Need to Know About Password Managers," Consumer Report, February 7, 2017, online: https://www.consumerreports.org/digital-security/everything-you-need-to-know-about-password-managers/

[297] *Ibid.*

[298] That statistic does not include companies that use those password managers. ISE. "Password Managers: Under the Hood of Secrets Management," February 19, 2019, online: https://www.ise.io/casestudies/password-manager-hacking/

smartphones[299]. However, it should be noted that after being notified by the researchers concerned, several password managers quickly corrected some of the problems found[300].

2.2.2.6. Using two-factor authentication

Another measure to protect the security of online devices and accounts, and indirectly the privacy of Internet users, involves two-factor authentication (2FA). This measure was notably promoted by the White House in 2016 as part of a campaign to educate Americans about cybersecurity[301].

This measure is complementary to choosing and updating a secure password, in that it adds a layer of security when accessing a device or online account[302]. After entering the password correctly, the user will need to validate his identity by using a second "authentication factor." There are three types of possible factors[303]:

- Knowledge factors (e.g., security question)
- Possession factors (e.g., security code received via SMS on a mobile device and used as a security key)
- Inherence factors (e.g., fingerprints, facial recognition)

Two-factor authentication can be enabled (directly or through apps) on most smartphones, social media accounts, email boxes, major transactional websites, etc.[304]

Note that two-factor authentication improves the user's privacy from a cybersecurity perspective, but unfortunately can be harmful with respect to other aspects of online privacy. It is, after all, the disclosure of additional (and generally very private) data to an entity. For example, it is possible to authenticate to Facebook by using a security code received via SMS on a mobile device in addition to a password. Facebook thus acquires its

---

[299] UNIVERSITY OF YORK. "Researchers expose vulnerabilities of password managers," March 16, 2020, online: https://www.york.ac.uk/news-and-events/news/2020/research/expose-vulnerabilities-password-managers/

[300] OWAIDA, A. "Security flaws found in popular password managers," We live security - ESET, March 19, 2020, online: https://www.welivesecurity.com/2020/03/19/security-flaws-found-in-popular-password-managers/

[301] WHITE HOUSE – OFFICE OF THE PRESS SECRETARY. "Fact sheet: Cybersecurity National Action Plan," February 9, 2016, online: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

[302] RONFAUT, L. and FERRAN, B. " La double authentification, un geste simple pour se protéger du piratage," Le Figaro, June 9, 2016, online: https://www.lefigaro.fr/secteur/high-tech/pratique/2016/06/09/32002-20160609ARTFIG00117-la-double-authentification-un-geste-simple-pour-se-proteger-du-piratage.php

[303] "T]here are three generally recognized factors for authentication: something you know (such as a password), something you have (such as a hardware token or cell phone), and something you are (such as your fingerprint). Two-factor means the system is using two of these options.": GRIFFITH, E. "Two-Factor Authentication: Who Has It and How to Set It Up," PCMag, March 11, 2019, online: https://www.pcmag.com/feature/358289/two-factor-authentication-who-has-it-and-how-to-set-it-up; HIGGINS, P. "How to Enable Two-Factor Authentication on Twitter (And Everywhere Else)," Electronic Frontier Foundation, May 28, 2013, online: https://www.eff.org/deeplinks/2013/05/howto-two-factor-authentication-twitter-and-around-web

[304] GARUN, N. "How to set up two-factor authentication on all your online accounts," The Verge, March 27, 2019, online: https://www.theverge.com/2017/6/17/15772142/how-to-set-up-two-factor-authentication; KLOSOWSKI, T. "How to Protect Your Digital Privacy," New York Times, online: https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy

users' phone numbers. And it acknowledged in 2018 – after being exposed by a group of researchers[305] – that it uses those numbers as part of its targeted advertising program[306].

2.2.3. Online privacy enhancing technologies

Another active privacy measure is the use of a commercially available privacy enhancing technology. There are several types of such technologies, as discussed in the next section.

The term "privacy enhancing technologies" was first used in 1995 as part of a joint report by the Information and Privacy Commissioner of Ontario and the Dutch privacy authority (then called *Registratiekamer*). The report explored privacy technologies, particularly those related to online anonymity[307].

In light of the various existing definitions[308], we formulate the following definition of online privacy enhancing technologies:

> A set of technical tools, applications and mechanisms built into Internet connection devices, online services or platforms and designed to mitigate security and privacy risks to Internet users.

It should be noted that privacy enhancing technologies are sometimes seen as substitutes for the adoption of legislative or regulatory instruments[309]. We think that on the contrary, they are a complementary protection that in no way diminishes the importance of a solid privacy framework.

---

[305] VENKATADRI, G *et al.* "Investigating sources of PII used in Facebook's targeted advertising," Proceedings on Privacy Enhancing Technologies, April 19, 2018, online: https://mislove.org/publications/PII-PETS.pdf; The researchers' findings were later echoed in HILL, K. "Facebook Is Giving Advertisers Access to Your Shadow Contact Information," Gizmodo, September 26, 2018, online: https://gizmodo.com/facebook-is-giving-advertisers-access-to-your-shadow-co-1828476051

[306] LOMAS, N. "Yes Facebook is using your 2FA phone number to target you with ads," Techcrunch, September 27, 2018, online: https://techcrunch.com/2018/09/27/yes-facebook-is-using-your-2fa-phone-number-to-target-you-with-ads/

[307] INFORMATION AND PRIVACY COMMISSIONER FOR THE PROVINCE OF ONTARIO and REGISTRATIEKAMER. "Privacy-Enhancing Technologies: The Path to Anonymity," Vol 1, August 1995, online: http://www.ontla.on.ca/library/repository/mon/10000/184530.pdf

[308] *Ibid.,* Section 1.3; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Privacy Enhancing Technologies – A Review of Tools and Techniques," November 2017, online: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/; COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES. "Usage de Privacy-Enhancing Technologies (PETS)," online: https://cnpd.public.lu/fr/dossiers-thematiques/nouvelles-tech-communication/privacy-by-design/Usage-de-Privacy-enhancing-Technologies-_PETs_.html (consulted on April 10, 2021); THE ROYAL SOCIETY. "Protecting privacy in practice," March 2019, p.14, online: https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf; DENMARK. Ministry of Science Technology and Innovation, "Privacy Enhancing Technologies," META Group Report v 1.1, 28 March 2005, p. 4, online: https://danskprivacynet.files.wordpress.com/2008/07/rapportvedrprivacyenhancingtechlologies.pdf; COMMISSION OF THE EUROPEAN COMMUNITIES. "Communication from the Commission to the European Parliament and the Council," COM(2007) 228, 2007, p. 3, online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52007DC0228&from=EN

[309] PISA CONSORTIUM. "Handbook of Privacy and Privacy-Enhancing Technologies The case of Intelligent Software Agents," 2003, p. 34, online: https://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf

2.2.3.1. Anonymization tools

Anonymization tools are designed to allow Internet users not to be identified while browsing. They are used for masking a user's online identity[310]. Data are collected (websites visited, visit times, preferences, etc.), but ultimately cannot be linked to the individual.

There are several ways to identify an Internet user, for example by means of his email address or his IP address (unique identification number of his Internet connection[311]). Tools are available to anonymize those elements.

Note that some private browsers also act as anonymizers. They are discussed below as data limiting tools.

Virtual private networks

There are many virtual private network (VPN) services that allow Internet users to hide their IP address. A VPN works like this: All the traffic of an Internet user using a VPN is done via a "secure tunnel" (encrypted) toward the Internet network[312]. Visited websites cannot identify where the connection actually comes from, and the Internet user's service provider will not know what the Internet user has visited.

There are also proxy services that, similarly to VPNs, allow users to access websites using an IP address that is not their own but the third-party server's, which acts as an intermediary between the different networks[313]. Unlike VPNs, proxy servers do not encrypt the data transmitted between the connecting device and the server[314].

It should be noted that virtual private networks and proxy servers are sometimes better known for their use by certain organizations to allow their employees to access the organization's server remotely. These tools are also used by some to access content that is not accessible from their geographical location, but accessible elsewhere in the world (access to content blocked by certain states, access to geolocated entertainment content, etc.).

Unfortunately, these tools occasionally fail to function as intended and ultimately violate the user's privacy. The most common vulnerability is the occasional disclosure of the IP

---

310 OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Privacy Enhancing Technologies," *supra* note 308.
311 A name and address of an individual or company are linked to the IP address. This is normally the person responsible for paying the subscription to the Internet access service.
312 EUROPEAN UNION AGENCY FOR CYBERSECURITY. "PETs controls matrix – A systematic approach for assessing online and mobile privacy tools," December 20, 2016, pp. 35-36, online: https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-controls-matrix-a-systematic-approach-for-assessing-online-and-mobile-privacy-tools
313 FITZPATRICK, J. "What's the Difference Between a VPN and a Proxy?", How To Geek, June 18, 2019, online: https://www.howtogeek.com/247190/whats-the-difference-between-a-vpn-and-a-proxy/; KURNIADI, D. "The Difference Between Using Proxy Server and VPN," 2015, online: https://www.howtogeek.com/247190/whats-the-difference-between-a-vpn-and-a-proxy/
314 *Ibid.*

address by the tool itself due to a vulnerability in the computer system or to an interruption of the connection to the tool[315].

Disposable email addresses

Another online anonymization tool is the disposable or temporary email address. This type of tool allows users to create a new email address and access it for a short period of time (usually a few minutes). Those email addresses can be used when a user needs to fill out an online form or provide an email address to access specific content online; a temporary address eliminates the risk of receiving unwanted email (spam) in the real mailbox afterward[316].

2.2.3.2. Data limiting tools

As the name implies, the purpose of data limiting tools is to reduce the amount of data collected by a website visited or by an application used. Those tools ensure that only minimal data, necessary for navigation or use, are collected[317].

Private browsers

Generally speaking, the most popular browsers (Chrome, Explorer/Edge, Safari, Firefox, etc.) record data on their users' browsing activities (websites visited, date and time of each visit, etc.)[318] . There are so-called private browsers that make it possible to avoid such data collection and storage.

The most famous private browser is Tor, whose development was partially funded by the Electronic Frontier Foundation[319]. Tor is actually an acronym for *The Onion Router*, referring to its "onion routing" operation. Communication transmitted over the Internet is embedded with layers of data encryption and flows through various random intermediary relays (on different servers), thus ensuring, among other things, that the IP address at the communication's origin is not disclosed[320].

---

[315] A 2015 study concluded that 10 of the 14 popular VPNs studied were likely to leak a user's IPv6 address. See on this topic: "Researchers Reveal Top VPN Services Leak IP Data, Vulnerable to DNS Hijacking," TripWire, June 30, 2015, online: https://www.tripwire.com/state-of-security/latest-security-news/researchers-reveal-top-vpn-services-leak-ip-data-vulnerable-to-dns-hijacking/; See similarly: VIJAYAN, J. "Port Fail Vulnerability Exposes Real IP Addresses of VPN Users," Security Intelligence, December 1, 2015, online: https://securityintelligence.com/news/port-fail-vulnerability-exposes-real-ip-addresses-of-vpn-users/

[316] TUFNELL, N. "21 tips, tricks and shortcuts to help you stay anonymous online," The Guardian, March 6, 2015, online: https://www.theguardian.com/technology/2015/mar/06/tips-tricks-anonymous-privacy

[317] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Privacy Enhancing Technologies," *supra* note 308.

[318] *Ibid.*

[319] TOR. "History," online: https://www.torproject.org/about/history/

[320] ALQAHTANI, A. A. and EL-ALFY, E-S. M. "Anonymous Connections Based on Onion Routing: A Review and a Visualization Tool," Procedia Computer Science, vol. 52, 2015, pp. 123 and fol.

Private browsing mode

Even in browsers that are not private, it is possible to use a private mode (sometimes called *incognito* or *inPrivate mode*)[321] . Those modes are primarily intended to prevent data such as browsing history or cookies from being automatically saved on the user's device[322]. They act as temporary browsing sessions that are distinct from a user's regular browsing. Note that simply enabling private browsing mode is generally considered insufficient – and provides less protection than private browsers – because it still allows some servers to track a user's online activity[323].

Private search engines

There are several search engines that advertise themselves as "private," meaning that they collect very little data when a user searches online. For example, they generally do not collect users' IP addresses and do not store any information about the searches performed (keywords, date and time, etc.)[324]. And since they don't "profile" users, they neither filter search results according to users nor present behavioural advertising[325]. They are usually contrasted with the Google, Bing or Yahoo search engines, which track their users and adapt the search engine accordingly[326].

The best known private search engine is DuckDuckGo, which is automatically linked to by the Tor browser mentioned above[327].

---

321 OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Privacy Enhancing Technologies," *supra* note 308.
322 JOHANSEN, A. G. "Is Private Browsing Really Private? Short answer: No," Norton, online: https://us.norton.com/internetsecurity-privacy-your-private-browser-is-not-so-private-after-all.html; DICKSON, B. "Private Browsing Won't Protect You from Everything," PC Magazine, September 16, 2019, online: https://www.pcmag.com/news/370703/private-browsing-wont-protect-you-from-everything
323 DELEON, N. "What Your Web Browser's Incognito Mode Really Does," Consumer Reports, June 19, 2018, online: https://www.consumerreports.org/internet/incognito-mode-web-browser-what-it-really-does/; MATHEWS, L. "What Is Private Browsing and Why Should You Use It?", Forbes, January 27, 2017, online: https://www.forbes.com/sites/leemathews/2017/01/27/what-is-private-browsing-and-why-should-you-use-it/#53e0308325b1; AGGARWAL, G *et al.* "An Analysis of Private Browsing Modes in Modern Browsers." Proceedings of Usenix Security, 2010, online: https://crypto.stanford.edu/~dabo/pubs/papers/privatebrowsing.pdf
324 CRAWFORD, D. "The Best Private Search Engines That Respect Your Privacy," ProPrivacy, May 13, 2020, online: https://proprivacy.com/cloud/private-search-engines; MORRIS, J. "DuckDuckGo: The search engine taking on Google and making the internet 'less creepy' with its privacy mission," Evening Standard, May 12, 2019, online: https://www.standard.co.uk/news/world/duckduckgo-the-search-engine-taking-on-google-and-making-the-internet-less-creepy-with-its-privacy-a4138911.html; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Privacy Enhancing Technologies," *supra* note 308.
325 CHAN, K. "European privacy search engines aim to challenge Google," Associated Press, November 21, 2018, online: https://www.apnews.com/dd8824e6f9424439b66e3992882b5c0b
326 TENE, O. "What Google Knows: Privacy and Internet Search Engines," Utah Law Review, online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1021490
327 LOMAS, N. "Tor switches to DuckDuckGo search results by default," Techcrunch, May 31, 2016, online: https://techcrunch.com/2016/05/31/tor-switches-to-duckduckgo-search-results-by-default/

Cookie blockers

Other tools can also block the installation of cookies on a browser and thus reduce the amount of data collected about an Internet user. This is the case, for example, with certain content filtering tools that we will discuss later[328].

2.2.3.3. Data and communication encryption tools

Today, many software programs and applications are designed to encrypt the data of Internet users on their connection devices (computer, smartphone, etc.). Similarly, some email services or online content sharing services offer automatic encryption of communications[329], and browser extensions compatible with major providers' email boxes are easily accessible[330].

Experts also recommend more broadly the use of encryption tools when browsing the Internet itself, such as *HTTPS Everywhere*, which secures unsecured websites[331].

2.2.3.4. Data deletion tools

There are tools that, rather than preventing the collection of data during browsing, eliminate its effects after the fact, at the end of the browsing session for example. Those tools erase the browsing history and/or eliminate cookies that may have been installed during the browsing session[332], thus making it more difficult to profile the Internet user (and ultimately to expose him to behavioural advertising). Examples include *CCleaner*[333] and the *Cookie AutoDelete* browser extension[334].

2.2.3.5. Data obfuscation tools

There are tools designed to "obfuscate" Internet users' data by creating parallel inaccurate data in which the Internet user's real data are "drowned." The tools aim at making it more

---

328 Section 2.2.3.7.
329 For a review of existing services, see the Electronic Frontier Foundation scorecard: ELECTRONIC FRONTIER FOUNDATION. "Secure Messaging Scorecard," online: https://www.eff.org/fr/pages/secure-messaging-scorecard (consulted on June 13, 2021).
330 VINCENTE, M. "How to encrypt emails?", TechAdvisor, April 21, 2020, online: https://www.techadvisor.fr/tutoriel/ordinateurs/crypter-emails-3689941/
331 LAWRENCE, J. and RINTEL, S. "Eight ways to protect your privacy online," The Guardian, December 3, 2013, online: https://www.theguardian.com/commentisfree/2013/dec/03/eight-ways-to-protect-your-privacy-online
332 DENMARK. "Privacy Enhancing Technologies," *supra* note 308, p. 17.
333 CCleaner, online: https://www.ccleaner.com/fr-fr/
334 Cookie AutoDelete, online: https://chrome.google.com/webstore/detail/cookie-autodelete/fhcgjolkccmbidfldomjliifgaodjagh?hl=en

difficult to create a profile of the Internet user or at making that profile totally inaccurate and, therefore, unusable[335]:

> This signal-jamming offers just one modest example of the larger theory of obfuscation, the idea that if you can't disappear online at least you can hide yourself in a miasma of noise[336].

Those tools, which do not influence the user's navigation – their actions are generally invisible to him – offer several possibilities:

- Simulating clicks on available ads (e.g. the *AdNauseam*[337] browser extension);
- Simulating continuous random Web searches (e.g. the *TrackMeNot*[338] application);
- Simulating continuous random website visits (e.g. the *Noise*[339] application);
- Reporting multiple geographic locations (e.g. the *CacheCloak*[340] application).

It should be noted that some browsers regularly try to block the use of obfuscation tools because the latter not only increase online traffic, but also harm the browsers' targeted advertising accuracy and *de facto* their advertising revenues[341].

2.2.3.6. Data tagging tools

Another type of privacy enhancing technology involves the tagging of users' personal data. Data submitted online "is labeled or tagged with instructions or preferences specifying how the data should be treated by service providers[342]." For example, Internet users indicate whether they agree to the data being treated for research purposes, financial transactions, etc. Those instructions are provided in a computer-readable format[343] (e.g., the E-P3P language previously supported by Windows) and are thus processed automatically[344].

---

335 POWLES, J. "Obfuscation: how leaving a trail of confusion can beat online surveillance," The Guardian, October 24, 2015, online: https://www.theguardian.com/technology/2015/oct/24/obfuscation-users-guide-for-privacy-and-protest-online-surveillance
336 DREYFUSS, E. "Wanna Protect Your Online Privacy? Open a Tab and Make Some Noise," Wired, March 29, 2017, online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1021490
337 ADNAUSEAM. Online: https://adnauseam.io/
338 TRACKMENOT. Online: https://trackmenot.io/
339 INTERNET NOISE. Online: http://makeinternetnoise.com/index.html
340 CACHECLOAK. Online: https://dl.acm.org/doi/pdf/10.1145/1710130.1710138
341 CIMPANU, C. "Google to no longer allow Chrome extensions that use obfuscated code," ZDNet, October 1, 2018, online: https://www.zdnet.com/article/google-to-no-longer-allow-chrome-extensions-that-use-obfuscated-code/; CIMPANU, C. "Mozilla announces ban on Firefox extensions containing obfuscated code," ZDNet, May 2, 2019, online: https://www.zdnet.com/article/mozilla-announces-ban-on-firefox-extensions-containing-obfuscated-code/
342 OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Privacy Enhancing Technologies," *supra* note 308.
343 PEARSON, S. *et al.* "Sticky Policies: An Approach for Managing Privacy across Multiple Parties," Computer, vol. 44 , No. 9, Sept. 2011, p. 61.
344 OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Privacy Enhancing Technologies," *supra* note 308.

Although this technology is very interesting, it is admittedly present mainly in the scientific literature, and has had little concrete impact so far, not having been adopted by consumers.

2.2.3.7. Online content filtering tools

Lastly, we identify content filtering tools, which indirectly protect Internet users' privacy.

Spam blockers

Some mailbox providers offer a spam filtering feature; there are also third-party spam blockers that can be added to users' mailboxes. Those tools use a variety of techniques to identify and filter out unwanted email (analysis of email content, listed senders, etc.)[345].

Ad blockers and pop-up windows

Internet users also have access to ad blockers, which are usually browser extensions (*Adblock Plus*[346], *Privacy Badger*[347], *Ghostery*[348], *uBlock Origin*[349], etc.). Some block all ads identified on the Web page the user is viewing, as well as pop-up windows associated with the page, while other tools limit filtering to ads that may run malware (*malicious software, spyware*) or track users[350].

Unfortunately, the various ad blockers offer uneven and generally incomplete protection, since many of the most widely used tools have commercial agreements with certain advertisers who want to avoid filtering of their ads[351]. The effectiveness of ad blockers is also undermined by the policies of some browsers and websites, which block or greatly complicate the operation of ad blockers or deny access to them, in order to secure their advertising revenues[352].

---

[345] DENMARK. "Privacy Enhancing Technologies, *supra* note 308, p. 16.
[346] ADBLOCK PLUS. Online: https://adblockplus.org/en/
[347] PRIVACY BADGER. Online: https://privacybadger.org/
[348] GHOSTERY. Online : https://www.ghostery.com/
[349] UBLOCK ORIGIN. Online: https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm?hl=en
[350] BISCHOFF, P. "75+ free tools to protect your privacy online," Comparitech, January 26, 2016, online: https://www.comparitech.com/blog/vpn-privacy/75-free-tools-to-protect-your-privacy-online/#Ad_Blockers; CHAIKIVSKY, A. "Want to Protect Against websites That Spy on You? Get an Ad Blocker," Consumer Report, February 15, 2018, online: https://www.consumerreports.org/digital-security/to-protect-against-websites-that-spy-on-you-get-an-adblocker/; HENRY, AL. "The Best Browser Extensions that Protect Your Privacy," Lifehacker, August 31, 2015, online: https://lifehacker.com/the-best-browser-extensions-that-protect-your-privacy-479408034
[351] COOKSON, R. "Google, Microsoft and Amazon pay to get around ad blocking tool," Financial Times, February 1, 2015, online: https://www.ft.com/content/80a8ce54-a61d-11e4-9bd3-00144feab7de; NATEOG. "Google reportedly paid Adblock Plus not to block its ads," The Verge, July 5, 2013, online: https://www.theverge.com/2013/7/5/4496852/adblock-plus-eye-google-whitelist
[352] HAY NEWMAN, L. "Google Says It Isn't Killing Ad Blockers. Ad Blockers Disagree," Wired, June 12, 2019, online: https://www.wired.com/story/google-chrome-ad-blockers-extensions-api/; ROGERS, K. "Why Your Ad Blocker

Social Media Widget Blockers

Lastly, there are also browser extensions *(*e.g. *Facebook Container*) designed to block social media *widgets.*

Many websites allow users to directly share the Web page they are viewing on social media, by using Facebook's "Like" and Twitter's "Tweet" buttons embedded in the interface of third-party Web pages. While those buttons may seem convenient, they unfortunately enable the social media concerned to track their online followers. The social media are notified of every website visited by the user that includes one of their widgets, even if he doesn't click on the button[353].

2.3. What Is the Privacy Paradox?

A review of the scientific literature on consumer privacy identifies a phenomenon that is regularly raised by authors, namely the online privacy paradox.

This phenomenon was identified in the scientific literature at the turn of the 2000s. In 2001, Barry Brown was the first author to address the subject, in examining the privacy concerns of certain consumers and their use of loyalty cards in grocery stores. He concludes that the situation "presents something of a paradox, in that while our participants seemed to be willing to volunteer general worries about privacy, in turn they were also willing to lose that privacy for very little gain[354]."

The potential existence of a privacy paradox was subsequently taken up by several authors who in turn conducted tests with consumers, particularly Internet users. The contradictory results of some studies are reviewed in the following pages.

The privacy paradox is generally described as a mismatch between consumers' concerns about privacy and their actual behaviour in this regard[355]. While it is not exclusive to the Internet, manifestations of the paradox are more prevalent[356] on the Internet, particularly because access to many online services requires the disclosure of personal information.

Doesn't Block Those 'Please Turn Off Your Ad Blocker' Popups," Vice, December 12, 2018, online: https://www.vice.com/en_us/article/j5zk8y/why-your-ad-blocker-doesnt-block-those-please-turn-off-your-ad-blocker-popups

[353] EFRATI, A. "'Like' Button Follows Web Users," Wall Street Journal, May 18, 2011, online: https://www.wsj.com/articles/SB10001424052748704281504576329441432995616

[354] BROWN, B. "Studying the Internet Experience," Hewlett Packard, March 26, 2001, pp. 17-18, online: https://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf

[355] HALLAM, C. and ZANELLA, G. "Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards," Computers in Human Behavior, vol. 68, 2017, p. 217.

[356] CHEN, H-T. "Revisiting the Privacy Paradox on Social Media With an Extended Privacy Calculus Model: The Effect of Privacy Concerns, Privacy Self-Efficacy, and Social Capital on Privacy Management," American Behavioral Scientist, vol. 62, No. 10, 2018, p. 1395.

The phenomenon is sometimes referred to as the online privacy dilemma, because of the "choice" that Internet users regularly face[357].

Regardless of what it is called, several types of online user behaviour have been identified to support the phenomenon's existence:

- Engaging in risky behaviours, including disclosing (voluntarily or recklessly) a lot of personal information on social media[358]
- A total lack of measures taken to protect one's privacy online[359]
- Weak or inadequate measures to protect one's online privacy[360]

2.3.1. A variety of studies on the subject

Nevertheless, an overview of the studies conducted on the online privacy paradox since 2006 shows that the existence of the online phenomenon is still far from unanimous.

Table 4
Summary presentation of some studies on the online privacy paradox

Studies that reject or strongly qualify the existence of the paradox	Studies that recognize the existence of the paradox
The study by Dienlin *et al* from the Universities of Mainz and Hohenheim[361]	The study by Oomen and Leenes from Tilburg University[363]

[357] GOULDING, A. "The identity and privacy dilemma," Newsroom, August 26, 2019, online: https://www.newsroom.co.nz/@ideasroom/2019/08/26/770241/the-identity-and-privacy-dilemma#; BURKHARDT, K. "The privacy paradox is a privacy dilemma," Mozilla Firefox, August 24, 2018, online: https://blog.mozilla.org/internetcitizen/2018/08/24/the-privacy-paradox-is-a-privacy-dilemma/
[358] NORBERG, P. A., HORNE, D. R. and HORNE, D. A. "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," Journal of Consumer Affairs, vol. 41, No. 1, 2007, p. 101; XIE, W., FOWLER-DAWSON, A. and TVAURI, A. "Revealing the relationship between rational fatalism and the online privacy paradox," Behaviour & Information Technology, vol. 38, No. 7, 2019, p. 744; BAEK, Y., KIM, E., and BAE, Y. "My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns," Computers in Human Behavior, vol. 31, No. 1, 2014, p. 49.
[359] BAEK, Y. "Solving the privacy paradox: A counter-argument experimental approach," Computers in Human Behavior, vol. 38, 2014, p. 34.
[360] GERBER, N., GERBER, P. and VOLKAMER, M. "Explaining the Privacy Paradox - A systematic review of literature investigating privacy attitude and behavior," Computers & Security, vol. 77, 2018, p. 227.
[361] DIENLIN, T., MASUR, P. K. and TREPTE, S. "A Longitudinal Analysis of the Privacy Paradox," September 2019, online: https://www.researchgate.net/publication/335948948_A_Longitudinal_Analysis_of_the_Privacy_Paradox
[363] OOMEN, I. and LEENES, R. " Privacy risk perceptions and privacy protection strategies" in LEEUW E, FISCHER-HÜBNER S, TSENG J, BORKING J, eds. Policies and research in identity management, Springer, 2008, pp. 121-138.

More than 1,400 German Internet users were surveyed in 2014 and 2015 in a longitudinal study (6 months between question periods) regarding their habits and perceptions of personal information disclosure online. The researchers observed that changes in the level of concern for their online privacy partially correlated with changes in online disclosure behaviours. For example, Internet users whose level of concern increased shared slightly less information than before (quantity and frequency) and vice versa[362].	Just over 5,500 Dutch students were surveyed in 2006 and 2007 about their online privacy strategies. Both researchers conclude that the adoption of protective behaviours and tools is rarely higher among those who perceive more risk to their online privacy. There are some exceptions, including the use of encryption technologies and disposable email addresses, which are associated with a higher level of concern among those Internet users[364].
<u>The study by Joinson *et al* from the Universities of Zurich, Westminster and Bath and the Hult International Business School</u>[365] Approximately 750 students from an online research panel at the Open University (from the U.K.) were asked about their privacy concerns and online behaviours in two surveys six weeks apart. The researchers conclude that the overall level of privacy concern reported by respondents predicts their willingness to disclose personal information online in the following weeks[366]. The study finds that the impact of concern on online disclosure is modest, but does exist[367].	<u>The study by Acquisti and Gross of Carnegie Mellon University</u>[368] More than 500 U.S. students who use the Facebook platform were surveyed about their privacy concerns, their use of the platform, and the visibility of their online profile in 2006. The researchers conclude that while Internet users' privacy concerns may influence their choice of whether or not to join social networks, once they have signed up, those concerns have no real impact on the amount of information that is disclosed by individuals[369].

362 *Ibid.,* p.22.
364 *Ibid.,* pp. 129-132.
365 JOINSON, A. N., REIPS, U.-D., BUCHANAN, T., and PAINE SCHOFIELD, C. B. "Privacy, trust, and self-disclosure online," Human-Computer Interaction, vol. 25, No. 1, 2010.
366 *Ibid.,* p. 12.
367 *Ibid.,* p. 18.
368 ACQUISTI, A. and GROSS, R. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," Lecture Notes in Computer Science book series, vol. 4258, 2006.
369 *Ibid.,* p. 51.

The study by Krasnova *et al* from Humboldt University Berlin and the European School of Management and Technology[370]	The study by Zafreiropoulou *et al* from the University of Southampton[371]
Some 250 German users of the social media platforms StudiVZ and Facebook were surveyed in 2008 about the platforms (usage, concerns, trust, etc.).	Approximately 150 Internet users of mobile applications (Foursquare, IMDB, Facebook, etc.) were surveyed in 2013 by means of various scenarios regarding disclosure of their geolocation data.
The study found that respondents adjust the information they disclose online based on their perceived privacy risks. The authors note that the level of trust in social media indirectly influences the extent of personal information disclosure, by affecting the platform users' perception of privacy risks.	The researchers conclude that there is no significant correlation between the level of concern and the willingness to share one's geolocation data, although there is a correlation between the general level of concern for privacy and the specific level of concern about geolocation data[372].

Thus, there are conflicting results regarding the existence of a privacy paradox among American and European Internet users. As mentioned above, this study includes the results of our 2020 survey of Canadian Internet users. We will discuss those results in detail, as well as the indications of the presence or absence of a privacy paradox among our respondents (section 3.3.5).

2.3.2. Some possible explanations

Since a number of studies support the existence of a privacy paradox, it is relevant to look at the various possible explanations of this phenomenon. We will briefly discuss those most likely to apply to Canadian Internet users.

Generally speaking, the theoretical models are based on the premise that an Internet user who transmits personal information online does so following a rational choice, i.e. that he makes this decision following an evaluation of the risks and benefits of such a transmission (referred to as a *privacy calculus*)[373]. As we know, the consumer is more often impulsive

[370] KRASNOVA, H. *et al.* "Online social networks: Why we disclose," Journal of Information Technology, vol. 25, No. 2, 2010.
[371] ZAFEIROPOULOU, A. M. *et al.* "Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions?," 2013, online: https://www.researchgate.net/publication/266653696_Unpicking_the_privacy_paradox_Can_structuration_theory_help_to_explain_location-based_privacy_decisions
[372] *Ibid.,* p. 469.
[373] According to some economic theories, consumers' decisions are all motivated by a desire to maximize their profits. *Homo oeconomicus* theory. GERBER. "Explaining the Privacy Paradox," *supra* note 360, p. 229.

than coldly calculating[374]. That being said, even within the framework of a rational evaluation, certain factors likely affect choices and lead to an erroneous or distorted evaluation of the risks or benefits, hence the potential presence of a paradox.

2.3.2.1. A lack of knowledge?

The privacy paradox could be explained firstly by a poor assessment of the risks and benefits of the disclosure of personal information, because of the Internet user's lack of information or knowledge.

It should be kept in mind that there is a significant information asymmetry between consumers and the businesses that seek to collect and handle their personal information[375]. Consumers know little or nothing about the practices of the companies that solicit them. They also know very little about the legislative and regulatory framework in place and their rights with respect to the protection of personal information.

That significant lack of information is highly likely to mislead the consumer when he assesses the risks and benefits of disclosing his personal information to a private entity[376].

2.3.2.2. Psychological reasons?

The psychological distance

The divide between consumers' fears and their behaviours may also be explained by the different ways in which individuals conceive the risks and benefits regarding the protection of their privacy online.

The potential benefits of disclosing personal information to a company are usually much more tangible than the potential risks. Access to discounts or improved services or socialization tools through personalization are much easier for individuals to perceive or conceive than the negative (and sometimes highly technical) situations of computer security breaches, third-party access to data or online profiling, for example[377]. Moreover, the risks that an individual has to take into account are perceived as uncertain and

---

[374] Quebec courts have repeatedly defined the average consumer as someone who is hasty, gullible and inexperienced as opposed to careful and diligent. The Supreme Court of Canada has upheld this approach. *Richard* v. *Time* Inc., 2012 SCC 8, [2012] 1 S.C.R. 265.
[375] BANDARA, R., FERNANDO, F., and AKTER, S. "The Privacy Paradox in the Data-Driven Marketplace: The Role of Knowledge Deficiency and Psychological Distance." Procedia Computer Science, vol. 121, 2017, pp. 564-565.
[376] *Ibid.* TREPTE, S. *et al.* "Do people know about privacy and data protection strategies? Towards the 'online privacy literacy scale' (OPLIS)" in GUTWIRTH, S., LEENES, R. and DE HERT, P., eds., Reforming European Data Protection Law, Springer, lines 491 and fol.
[377] GERBER. "Explaining the Privacy Paradox," *supra* note 360, p. 229.

hypothetical and sometimes only identifiable after a privacy breach has occurred[378], whereas the benefits are often guaranteed and immediate[379].

Those distinctions are important because consumers naturally place greater importance on tangible aspects and maintain a certain psychological distance from more abstract aspects[380]. They also prioritize near-future consequences (positive or negative), as Hallam and Zanella report:

> [...] the privacy risk associated with information self-disclosure is perceived as abstract and psychologically distant, more related to distant-future intentions, while the social rewards are perceived as psychologically near and more concrete, related to short-term intentions. Our model shows that the near-future intentions are significantly related to the self-disclosure behavior, while the distant-future ones are not[381].

Optimism bias

The underestimation of online privacy risks could also be explained by the presence of an optimism bias, sometimes referred to as comparative optimism or described as the "it won't happen to me[382]" attitude.

For example, studies show that individuals distinguish between risks to themselves and risks to other members of their society. And they tend to perceive their level of risk to their online privacy as lower than that of others[383].

Social norms

The paradox of online privacy could also be explained by the social pressure on Internet users to participate in the digital social environment[384]. According to researchers, many Internet users use social media and share information about themselves in order to meet their peers' expectations and thus become part of an online community, to the detriment

---

[378] HALLAM. "Online self-disclosure," *supra* note 355, p. 219; ACQUISTI, A. and GROSSKLAGS, J. "Privacy and rationality in individual decision making," IEEE Security & Privacy, vol. 3, No. 1, 2005, p. 26.
[379] BANDARA. "The Privacy Paradox," *supra* note 375, p. 565.
[380] *Ibid*; HALLAM. "Online self-disclosure," *supra* note 355, p. 219.
[381] *Ibid.,* p. 223.
[382] GILLESPIE, K. "It Won't Happen to Me: The Psychology Behind Optimism Bias," Vice, October 16, 2018, online: https://www.vice.com/en/article/a3an4a/it-wont-happen-to-me-the-psychology-behind-optimism-bias
[383] See for example: CHO, H., LEE, J. S. and CHUNG, S. "Optimistic Bias About Online Privacy Risks: Testing the Moderating Effects of Perceived Controllability and Prior Experience," Computers in Human Behavior, vol. 26, No. 5, 2010, p. 990; CAMPBELL, J. *et al.* "Unrealistic optimism in internet events," Computers in Human Behavior, vol. 23, No. 3, 2007, pp. 1280-1281; BANDARA. "The Privacy Paradox," *supra* note 375, p. 565.
[384] BANDARA. "The Privacy Paradox," *supra* note 375, p. 563.

of their privacy concerns[385]. The Internet user thus discloses personal information not as the result of a rational choice, but of peer pressure.

> It has been found that social norms and social rewards more often overwhelm consumers to undermine their privacy[386].
>
> Members of social groups using social networks as their primary communication medium put pressure on their peer group members to do likewise, i.e. share information and conform to social norms. Peer group members not conforming to communication and information sharing rituals are sanctioned with attention deprivation and exclusion from the social group. Opting out (…) becomes increasingly difficult the more group members agree on information sharing as a basic principle constituting their affiliation[387].

Online privacy fatigue

Researchers also point to the phenomenon of privacy fatigue or apathy to explain the existence of the online privacy paradox. Privacy fatigue can occur when Internet users are continually challenged by requests for consent to disclose personal information and are unable to respond as they would like (either because they have no real choice or because they cannot realistically read their information in order to make an informed decision)[388]. An Internet user who is overwhelmed (and desensitized) by this situation may then adopt a strategy of "disengagement" from protection of his online privacy in order to reduce the stress he feels[389].

> […] consent overload, information overload, and the absence of meaningful choice leads to 'consent desensitisation'. Users no longer make active, informed choices when confronted with a consent situation, but instead simply provide consent when consent is asked[390].

---

385 GERBER. "Explaining the Privacy Paradox," *supra* note 360, p. 230; HALLAM. "Online self-disclosure," *supra* note 355, p. 219.
386 BANDARA. "The Privacy Paradox," *supra* note 375, pp. 562-567.
387 FLENDER, C. and MÜLLER, G. "Type Indeterminacy in Privacy Decisions: The Privacy Paradox Revisited" in BUSEMEVER, J. R. *et al,* eds., QI 2012: Quantum Interaction, Conference proceedings, 2012, pp. 153-154.
388 CHOI, H., PARK, J., and JUNG, Y. "The role of privacy fatigue in online privacy behavior," Computers in Human Behavior, vol. 81, April 2018, p. 43; SCHERMER, B. W., CUSTERS, B., and VAN DER HOF, S. "The crisis of consent: How stronger legal protection may lead to weaker consent in data protection," Ethics and Information Technology, vol. 16, No. 2, 2014, p. 176.
389 *Ibid.,* p. 43; WIRTH, J., MAIER, C. and LAUMER, S. "The Influence of Resignation on the Privacy Calculus in the Context of Social Networking Sites: An Empirical Analysis," research Papers. 161, 2018, p. 5.
390 SCHERMER. "The crisis of consent," *supra* note 388, p. 178.

Cynicism about online privacy

Lastly, some researchers suggest that a certain cynicism may be responsible for what is perceived as a privacy paradox. The sense of powerlessness or resignation felt by many Internet users in the face of risks to their personal information online may have the ultimate effect of rendering any attempt to protect it futile in their eyes[391].

> Privacy cynicism allows users to take advantage of online services without trusting providers while aware of privacy threats by forming the conviction that effective privacy protection is out of their hands[392].

This explanation is supported, among other things, by the results of a survey of several thousand American and British Internet users: Two thirds of respondents felt that it was impossible to protect their privacy online in 2019, a figure that was up sharply from the previous year[393]. It is also worth noting that this helplessness-based explanation of the privacy paradox is consistent with one of the major concerns of Internet users, outlined in section 2.1.1, i.e. the feeling of having lost control over their personal information online.

Xie *et al* refer to a "rational fatalism" on the part of Internet users, and associate it mainly with the (perceived) inability of the law, companies and technological tools to provide real protection for their personal information online[394].

---

[391] XIE. "Revealing the relationship," *supra* note 358, p. 745.
[392] HOFFMANN, C., LUTZ, C., and RANZINI, G. "Privacy cynicism: A new approach to the privacy paradox," Cyberpsychology: Journal of Psychosocial Research on Cyberspace, vol. 10, 2016, p. 7.
[393] STERLING, G. "Most consumers believe online privacy is impossible, survey finds," MarTech, July 10, 2019, online: https://marketingland.com/most-consumers-believe-online-privacy-is-impossible-survey-finds-263538; a similar study (but limited to online personal information marketing) was conducted in 2015 by researchers at the University of Pennsylvania and arrives at very similar results: "When we investigated the overlap that designates resignation, we found that a majority of the population-58%-is resigned.": TUROW, J., HENNESSY, M. and DRAPER, N. "The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them up to Exploitation," Communication, University of Pennsylvania, 2015, p. 14.
[394] XIE. "Revealing the relationship," *supra* note 358, p. 754.

WHAT CANADIAN CONSUMERS SAY

3.1 Canada-wide Survey

We commissioned a specialized firm to conduct a survey of Canadian respondents during the month of January 2020. The sample, comprised of 1,519 Canadian residents aged 18 to 97, is representative of the population and has a margin of error of 2.5% 19 times out of 20.

The representation of the different generations to which the respondents belong is detailed as follows[395]:

- 12% of respondents are from Generation Z
- 26.7% of respondents are from Generation Y or Z
- 28.8% of respondents are from Generation X
- 29.3% of respondents are baby boomers
- 3.3% of respondents are from the silent or previous generation

Let's mention at the outset some limitations of the survey and the pool of respondents.

Since the survey was conducted online, the results may paint a picture that somewhat over-represents the opinions and behaviours of more experienced Internet users[396]. Canadians who don't use the Internet could not be surveyed. This exclusion, while regrettable, seems acceptable given that this is a study (and a survey) about online privacy and that other studies tend to show that non-adoption of the Internet is not generally due to privacy considerations[397].

As well, the results may somewhat underestimate Canadians' level of concern, because survey participants are generally less concerned about their privacy than non-participants[398]. It should be noted, however, that this does not appear to be true in this case, given the very high levels of concern revealed by the survey.

---

[395] Silent Generation (those born between 1928-1945), Boomer Generation (1946-1964), Generation X (1965-1980), Generation Y (1981-1996) and Generation Z (1997-2012). According to the Pew Research Center categorization: DIMOCK, M. "Defining generations: Where Millennials end and Generation Z begins," Pew Research Center, January 17, 2019, online: https://www.pewresearch.org/fact-tank/2019/01/17/where-millennials-end-and-generation-z-begins/

[396] HONG. "Drivers and Inhibitors," *supra* note 98, p. 3.

[397] Generally, Internet non-use is reportedly related to the cost and unavailability of telecommunications services: STATISTICS CANADA. "Canadian Internet Use Survey, 10-29-2019," online: https://www150.statcan.gc.ca/n1/daily-quotidien/191029/dq191029a-fra.htm; HORRIGAN, J. B. and DUGGAN, M. "Home Broadband 2015," Pew Research Center, December 31, 2015, online: https://www.pewresearch.org/internet/2015/12/21/home-broadband-2015/

[398] ACQUISTI. "Imagined Communities," *supra* note 368, p. 50.

3.1.1 Background: the *Desjardins* and *Capital One* cases

Before discussing the survey results, it is also important to briefly summarize two major events that occurred in the months leading up to the survey. The case involving Desjardins seems to have particularly struck Quebec and French-speaking respondents, who stand out from other respondents on several issues. Indeed, Desjardins is one of the most influential brands in the province[399].

In July 2019, the U.S. bank Capital One publicly revealed that it was the victim of a massive data theft. That data leak occurred in March and April 2019, affecting approximately 100 million American and 6 million Canadian consumers. The personal information disclosed pertained to credit card applications received between 2005 and 2019 and included consumers' names, contact information, credit scores and credit history, among other things. One million Canadian social insurance numbers were also reportedly hacked[400]. A hacker nicknamed "Erratic," who allegedly exploited the company's misconfigured firewall, has since been arrested and charged by the U.S. justice system[401].

Around the same time, in June 2019, a Quebec police force discovered that a former employee of the Desjardins Group had illicitly obtained and transmitted personal information about all 4.2 million of the company's individual customers (date of birth, social insurance number, phone number, email address, etc.)[402]. Those affected were contacted in July or November 2019, just a few months before our survey was conducted.

3.1.2 Highlights

3.1.2.1 What is privacy?

To better understand the privacy concerns of Canadian Internet users, we must first understand the meaning they attach to this concept. To that effect, we offered respondents five definitions that relate to the major themes identified in the literature (control, access,

---

399 DALLAIRE, S. "Indice Ipsos-Infopresse: Hydro-Québec en 3e place, juste derrière Google et Facebook," Infopresse, March 25, 2019, online: https://www.infopresse.com/article/2019/3/25/indice-ipsos-infopresse-hydro-quebec-en-3e-place-juste-derriere-les-geants-google-et-facebook

400 ABEDI, M. "Capital One data breach: here's what Canadians need to know," Global News, July 30, 2019, online: https://globalnews.ca/news/5702026/capital-one-data-breach-what-to-know/; MCLEAN, R. "A hacker gained access to 100 million Capital One credit card applications and accounts," CNN, July 30, 2019, online: https://www.cnn.com/2019/07/29/business/capital-one-data-breach/index.html; BENNARDO, M. "Everything Canadians need to know about the Capital One data breach," CBC, July 30, 2019, online: https://www.cbc.ca/news/business/capital-one-data-breach-1.5230287

401 HAY NEWMAN, L. "Everything We Know About the Capital One Hacking Case So Far," Wired, August 29, 2019, online: https://www.wired.com/story/capital-one-paige-thompson-case-hacking-spree/

402 "Data theft at Desjardins: all individual members affected, Radio-Canada," November 1, 2019, online: https://ici.radio-canada.ca/nouvelle/1371366/vol-de-donnees-desjardins-cormier-point-presse

secrecy, dignity, etc.[403]). Respondents were given the opportunity to select one or two definitions that resonated with them.

We find that the definitions of privacy that pertain to personal information are by far the most popular among the Internet users surveyed, regardless of their socio-demographic characteristics. Without really standing out from each other, the following three definitions all get the endorsement of more than half of the respondents:

- Controlling the sharing and use of personal information (58.8%)
- The ability to determine the use of home, body and personal information (56.2%)
- The ability to keep personal information secret (53.3%)

The other two proposed definitions of privacy that relate to isolation and image control are not very popular, with support rates of only 10% and 4% respectively. It should be noted that the privacy definition related to the possibility of isolating oneself from the public space still appeals to a portion of the youngest respondents. It corresponds to the privacy definition of 14.9% of the 18-34 year old Internet users surveyed, compared to only 6.2% of those aged 55 and over. It is also more favoured by Quebec residents than by those in other regions of the country.

3.1.2.2 What is private information?

The majority of respondents associate privacy with control or protection of their personal information. It is therefore important to define what they consider to be personal or private information. To that effect, we provided respondents with a list of 22 types of information that they were asked to classify as private or public. The information that was considered private by the greatest number of respondents was the following:

- Passwords (98%)
- Banking information (97%)
- Credit card number (97%)
- Credit report (92%)
- Annual income level (91%)
- Email content (91%)
- Sources of income (87%)
- Photographs or videos of them (80%)

We observe that without being exclusive to social media, the information about which opinions are divided regarding its private or public nature is likely to be available on those platforms. For example, name, age, location, or political affiliations and opinions are perceived as private by only 43%, 57%, 55% and 64% of respondents, respectively.

[403] See section 1.2.1.

Moreover, social media profiles rank last in the survey. Barely 2 in 5 respondents believe those profiles are private information, regardless of the privacy settings users have in place.

The types of information most commonly available on social media, with the exception of photographs and geographic location, are in fact the only ones for which we find significant differences by age group of respondents. For example, less than 35% of Internet users under the age of 34 believe that a user's name is private information, compared to nearly 50% of those 55 and older. The same is true for age, which is perceived as private by 45% of younger people, but by 60% of older people. According to Statistics Canada, 90% of Canadians aged 15 to 34 regularly use at least one social media platform, compared to 60% of Canadians aged 64 and over[404].

There are no similar age differences regarding perceptions of financial information (credit card number, credit report, income level, etc.).

3.1.2.3 What are respondents concerned about?

On average, respondents rate their level of concern for their online privacy at 7 out of 10. Note that respondents aged 55 and older are much more likely to rate their level of concern above the 9 out of 10 mark than their younger counterparts (34.4% vs. 17.7% among 18-35-year-olds and 24.4% among 35-54-year-olds).

In addition to the age of respondents, the level of concern also varies considerably depending on where they live. While almost half of Quebec respondents rate their level of concern at 9 or 10 out of 10, only one in five respondents in Ontario or the West do so. This particularly high level of concern among Quebecers is reflected throughout the survey results. We will see later that among the Quebec respondents interviewed for this study, the name Desjardins was on everyone's lips...

Table 5
Respondents' overall level of concern about online privacy

Not at all concerned — Extremely concerned

1	2	3	4	5	6	7	8	9	10
1.6%	0.7%	3.2%	4.2%	11.1%	12.5%	21.6%	19.5%	10.9%	14.7%
9.7%				23.6%		41,1%		25.6%	

[404] SCHIMMELE, C., FONBERG, J. and SCHELLENBERG, G. "Canadians' assessments of social media in their lives, Economic and Social Reports," Statistics Canada, 24 March 2021, online: https://www150.statcan.gc.ca/n1/pub/36-28-0001/2021003/article/00004-eng.htm

None of the three broad categories of concern according to Malhotra *et al* stands out. Respondents show a similar level of concern (about 7 out of 10 on average) about the extent to which personal information is collected online, the loss of control over that information, and the state of their knowledge on the subject. A higher level of concern is again observed among respondents aged 55 and over and Quebec residents.

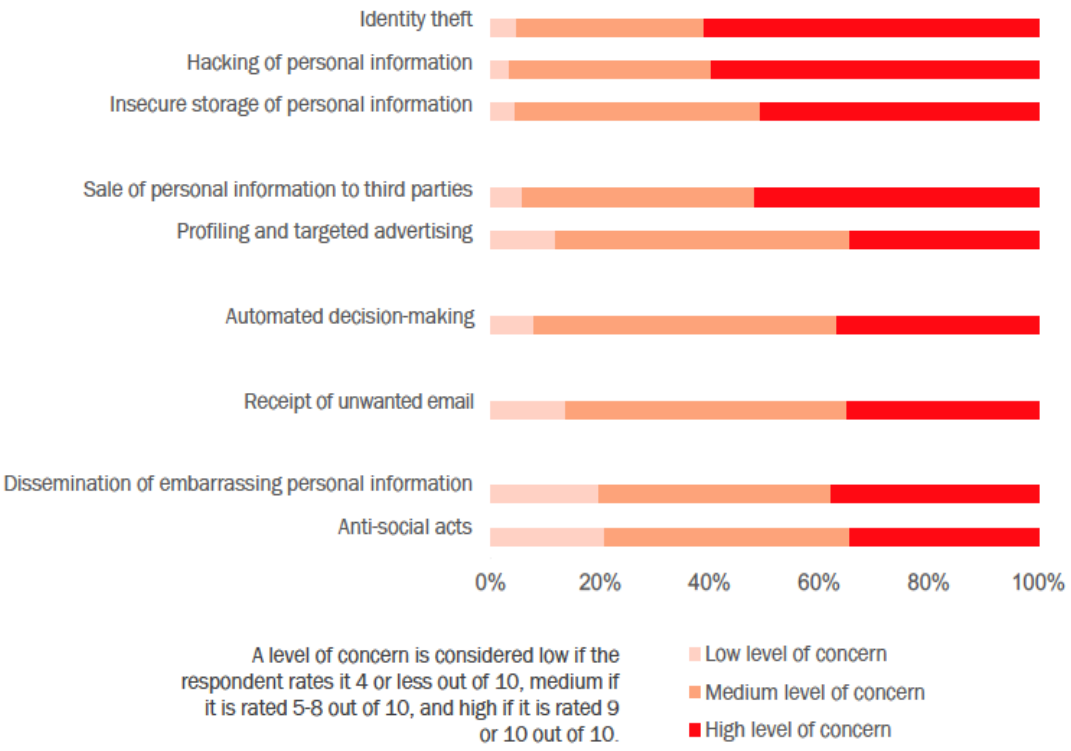
Identity theft above all

Not surprisingly, risks related to identity theft and personal information hacking are of the greatest concern to Canadian respondents. Both types of risks score an average level of concern of about 8.5 out of 10. In fact, none of the risks that respondents were questioned about scored lower than 6 out of 10.

The risks that respondents were least concerned about were those related to the perpetration of anti-social acts (threats, harassment, bullying) using an individual's personal information, the dissemination of embarrassing or compromising personal audio and video information or content, and the receipt of unwanted email. Those risks are more in line with the literature's privacy definitions that received little support from respondents, namely isolation from the public space and control of image (and reputation).

The two risks that are more related to relationships with others (dissemination of embarrassing content, perpetration of anti-social acts) still present interesting results. Those risks divide respondents more. Respondents who are concerned are very concerned and conversely, the others are particularly unconcerned. Fewer respondents are moderately concerned about this risk than about many other risks (e.g., targeted advertising, automated decision-making, etc.).

Table 6
Respondents' level of concern about certain online privacy risks

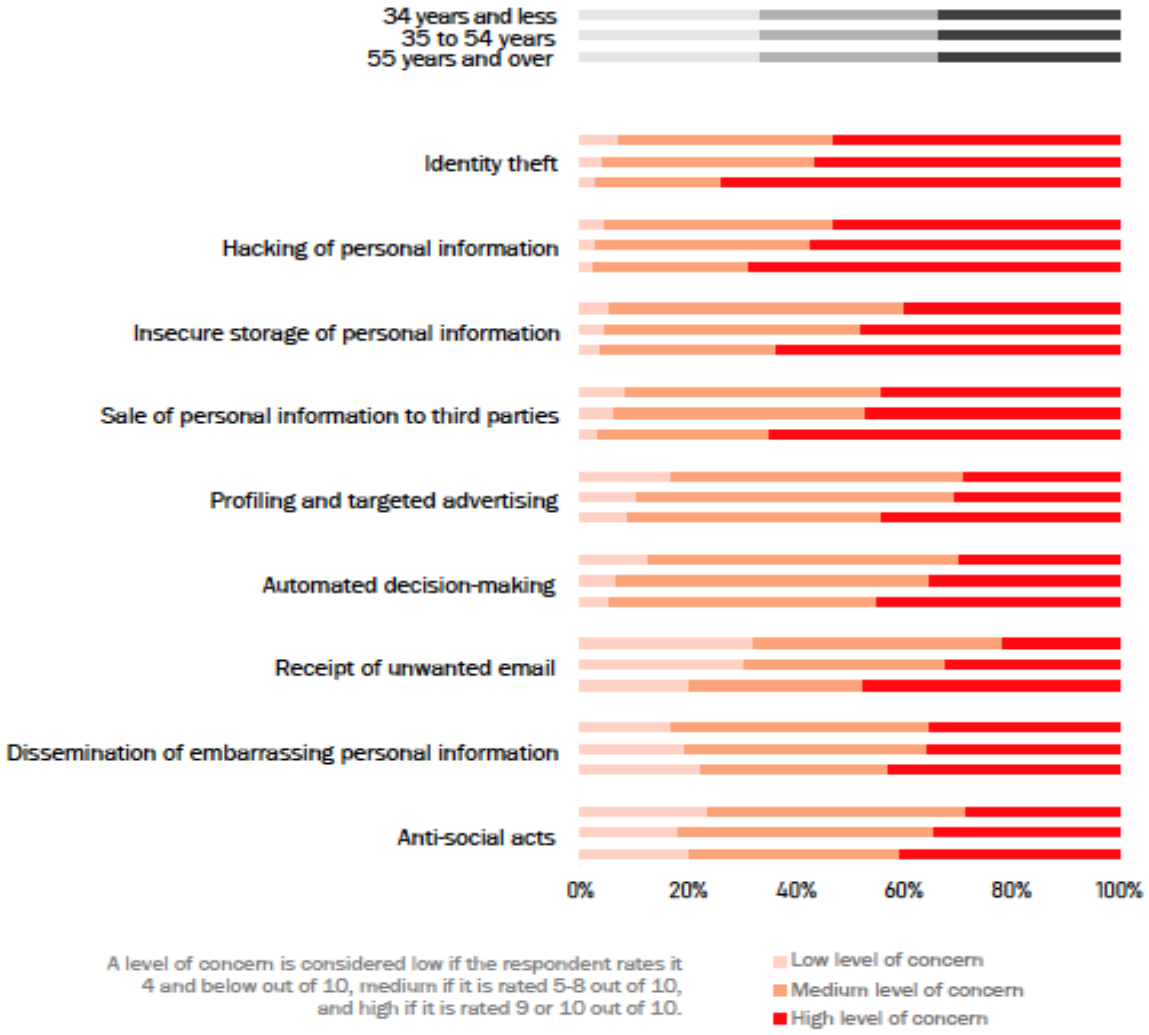


As with the overall level of concern for their online privacy, respondents aged 55 and over are generally more concerned about the various risks than their younger counterparts.

Thus, for all the risks presented, with the exception of the risk of disseminating embarrassing or compromising content, respondents aged 55 and over express more concern than the average respondent. For this last risk, we note this surprising result: We find in this age group both the highest percentages of those who are most concerned and those who are least concerned![405]

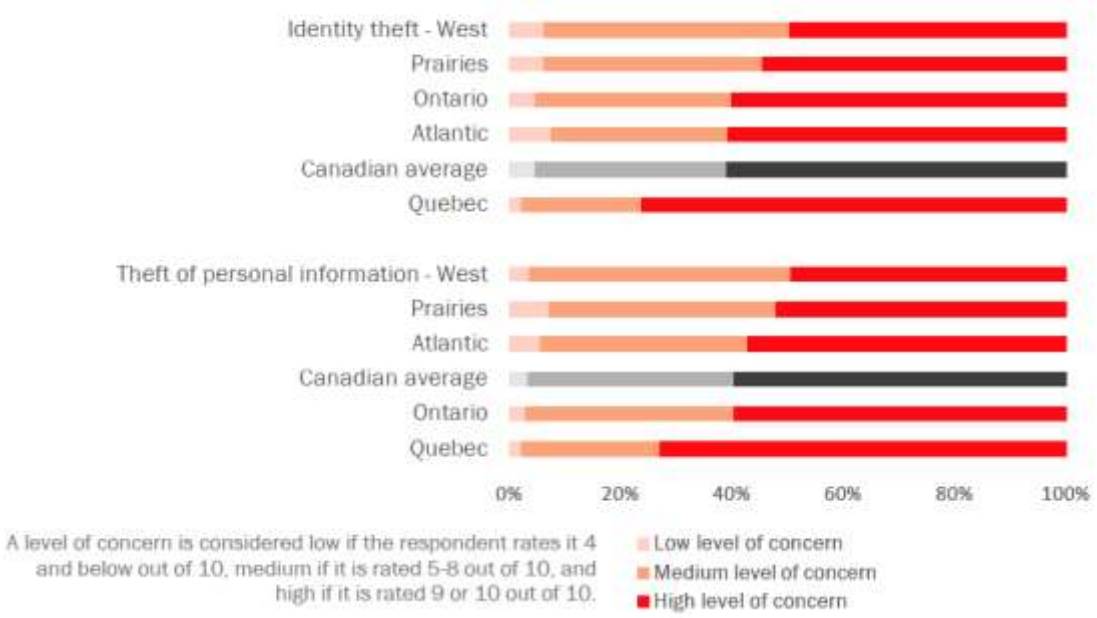
[405] 42.9% were very concerned (compared to 34.9% and 35.7% among respondents aged 18-34 and 35-54, respectively) and 22.4% were somewhat concerned (compared to 17.1% and 19.5% among respondents aged 18-34 and 35-54, respectively).

Table 7
Respondents' level of concern for certain online privacy risks, by age group



The differences identified previously according to the region in which respondents reside (Quebec, Ontario, Prairies, West or Atlantic) are maintained. Quebec respondents consistently express more concern about the various risks presented to them than respondents from other regions. And consistently, those from the Western provinces (and sometimes the Prairies) report the lowest average level of concern for those same risks. The gap is marked, averaging almost 15%. Even for risks associated with the security of personal information, which are certainly less divisive, there are significant differences between Canadian regions.

Table 8
Respondents' level of concern for certain online privacy risks, by region



As with their overall level of concern for their online privacy, women have a higher average level of concern than men for each of the risks presented. For example, women are 23% more likely to say they are very concerned about their personal information being hacked. The gap rises to 32% when it comes to the release of embarrassing or compromising audio and video content or information. It's hard not to make the connection to the disproportionate effect of revenge porn[406] or deepfakes[407] on women online[408].

[406] Sometimes called "Pornodivulgation" in French; it is the dissemination of a video or image of a sexual nature without the consent of the person presented, for the purpose of revenge or harassment: OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE. "Pornodivulgation," online: http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26552451 (consulted on July 15, 2021); MERRIAM WEBTERS. "Revenge porn," online: https://www.merriam-webster.com/dictionary/revenge%20porn (consulted on July 15, 2021).

[407] Sometimes called "Hypertrucage" in French; it is a process of ultra-credible manipulation of an audio and/or video recording that makes it appear that a person or persons are doing or saying things they did not actually do or say: OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE. "Hypertrucage," online: http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26552557 (consulted on July 15, 2021); MERRIAM WEBSTER. "Deepfake," online: https://www.merriam-webster.com/dictionary/deepfake (consulted on July 15, 2021).

[408] WANG, C. "Deepfakes, Revenge Porn, And The Impact On Women," Forbes, November 1, 2019, online: https://www.forbes.com/sites/chenxiwang/2019/11/01/deepfakes-revenge-porn-and-the-impact-on-women/?sh=552560191f53; SHARRATT, E. "Intimate image abuse in adults and under 18s," University of Exeter and Economic and Social Research Council, 2019, online: https://swgfl.org.uk/assets/documents/intimate-image-abuse-in-adults-and-under-18s.pdf

Increased fear associated with smartphones

Half of the respondents felt that their level of concern varied depending on the device they use to connect to the Internet. Not surprisingly, the gap is smaller among respondents who are not very concerned about their online privacy.

Three out of five respondents are more concerned about accessing the Internet from a smartphone than from a personal computer. This trend may be due to the greater security risks of smartphones, as described by the Electronic Frontier Foundation:

> Unfortunately, cell phones were not designed for privacy and security. Not only do they do a poor job of protecting your communications, they also expose you to new kinds of surveillance risks-especially location tracking. Most cell phones give the user much less control than a personal desktop or laptop computer would; it's harder to replace the operating system, harder to investigate malware attacks, harder to remove or replace undesirable bundled software, and harder to prevent parties like the mobile operator from monitoring how you use the device[409].

Opinions are mixed when it comes to tablets and other connected objects (smart speakers, smart watches, etc.). A similar percentage of respondents believe that their use is more of a concern and less of a concern than a computer for online privacy.

3.1.2.4 What are respondents doing to protect their online privacy?

When asked about the strategies they have adopted to protect their online privacy, respondents first point to the following:

- Using antivirus software and/or a firewall (69% of respondents)
- Using a spam blocker (66%)
- Reducing the amount of personal information provided or shared online (62%)
- Using different passwords for the majority of online accounts (61%)
- Using an online ad blocker (60%)
- Manually deleting the browsing history and cookies (54%)
- Adjusting privacy settings on devices, websites and apps (54%)

Of the 23 behaviours and tools we suggested in the survey, respondents said they each took, on average, just over 5 different steps to protect their online privacy.

Internet users aged 55 and over are particularly different from younger users when it comes to withdrawal from the digital sphere. They are more likely to reduce the amount of information they share online (73% vs. 57% for those under 55) and avoid certain online

[409] ELECTRONIC FRONTIER FOUNDATION. "The Problem with Mobile Phones," October 30, 2018, online: https://ssd.eff.org/en/module/problem-mobile-phones

content they find risky (56% vs. 45%). They are also more likely to limit or entirely avoid purchases or other financial transactions online (39% vs. 25%).

But the use of online privacy tools appears to be inversely proportional to the respondents' age. Younger Internet users, those under the age of 34 and in some cases those between 35 and 54, are more aware of those tools and use them more. Men also stand out for their use of the tools and technologies presented in the survey.

Table 9
Respondents' awareness and use of online privacy tools

Tools	% of respondents who are **aware of** the tool				%of respondents who have **used** the tool			
	Average	By age group			Average	By age group		
		18-34	18-34	55 and over		18-34	35-54	55 and over
Spam Blocker	83%	85%	87%	77%	66%	65%	71%	62%
Ad blocker	83%	90%	85%	75%	60%	71%	59%	52%
Password manager	73%	75%	77%	66%	50%	75%	49%	29%
Private browsing feature or mode	69%	89%	72%	47%	35%	36%	41%	28%
Virtual private network (VPN)	64%	78%	68%	47%	35%	38%	37%	30%
Browser history and cookie blocker or eraser	62%	71%	66%	51%	32%	43%	35%	19%
Encrypted email	59%	64%	64%	48%	24%	27%	27%	18%
Data encryption services	53%	60%	57%	42%	20%	26%	20%	14%
Temporary email address	51%	58%	53%	41%	19%	21%	21%	15%
Private Browser	38%	50%	40%	23%	17%	20%	19%	12%
Private search engine	36%	47%	40%	22%	16%	22%	17%	8%

* Percentages have been rounded to the nearest whole number.

3.1.2.5 What is Internet users' state of knowledge?

81% of respondents say they have already informed themselves about their online privacy. They learn from a variety of sources about the risks to their privacy and the behaviours and tools they can use to protect themselves. In fact, none of the sources suggested to them really stood out:

- Families and relatives: 38.5% of respondents

- Traditional media (newspapers, television, radio, etc.): 33%
- Digital media (blogs, podcasts, etc.): 30.5%

- Internet service providers: 31%
- Internet companies (Google, Yahoo, Facebook, etc.): 29.5%

- Government agencies: 24%

A modest level of knowledge

Respondents were asked to rate their knowledge of corporate practices regarding the collection and handling of personal information online.

About one in two respondents thinks he has a good knowledge of those practices. This is more the case among men, anglophones and consumers aged 18 to 34. Quebecers again stand out as they rate their knowledge much more pessimistically than the average.

We also note that this picture of respondents' knowledge is not as clear-cut as it might appear. In fact, very few respondents say they are "very well informed" or "very poorly informed" (7% and 10% respectively). The vast majority of respondents are moderately confident in their knowledge (42% say they are "somewhat knowledgeable" and 41% say they are "somewhat uninformed").

While this study is not intended as an assessment of Canadians' privacy literacy, we thought that respondents' self-assessment alone was insufficient and would have painted too inaccurate a picture. In order to test respondents' actual level of knowledge, we asked them to rate five statements as "true" or "false." The test was very brief and the level of difficulty was relatively low. All of the statements submitted were false.

We're surprised that respondents who say they are well or very well informed about companies' practices regarding the online collection and use of personal information generally score lower than others, as Table 10 shows! Similarly, while women, Quebecers and consumers over 55 years of age rate their knowledge much more harshly than their respective counterparts, they score about the same on the test and even do better on some statements.

In general, this "true or false" test reveals that the majority of respondents, regardless of the degree of knowledge they believe they have, are aware of the possibility of being identified and tracked online, despite certain precautions. But the situations presented to respondents were quite simple, and there is still cause for concern that between 19% and 31% of respondents were unaware of that possibility. One can easily imagine that this percentage increases dramatically when it comes to more subtle or complex collection practices (e.g. *browser fingerprinting, canvas fingerprinting, zombie cookies, supercookies, evercookies*, etc.[410]). Especially since the level of distrust among survey respondents may have been artificially exaggerated due to their exposure to several prior questions about online privacy.

Table 10

Respondents' answers according to their level of knowledge (self-assessed)

Assertions	**% of respondents believe this is not true**	% of "well informed" respondents believe this is not true [411]	% of "uninformed" respondents believe this is not true	**% of respondents believe this to be true**
"If you do not disclose your name, contact information or image online, it is impossible to identify you when you're browsing."	**84%**	81%	86%	16%
"Data collected by an Internet-connected object (such as a watch, fridge or smart TV) are transmitted only to the object's manufacturer. "	**75%**	74%	77%	25%
"The presence of a privacy policy on a website ensures that personal information collected will not be shared with other companies."	**73%**	71%	74%	27%
"Social media platforms only collect personal information from users who are members of their website."	**70%**	68%	72%	30%
"It is impossible to geolocate an Internet user when he has disabled the location feature on his Internet-connected device. "	**69%**	69%	69%	31%

[410] For a description of those technologies: GHOSTERY. "Cookies and fingerprinting: tracking methods clearly explained," March 6, 2018, online: https://www.ghostery.com/cookies-fingerprinting-co-tracking-methods-clearly-explained/; AVAST. "What Is Browser Fingerprinting and How Can You Prevent It?", online: https://www.avast.com/c-what-is-browser-fingerprinting (consulted on May 15, 2021).

[411] "Well-informed" respondents are those who said, in answer to another survey question, that they were "very" or "somewhat" familiar with companies' practices regarding the collection and use of personal information online. 48.8% of all respondents said that. "Uninformed" respondents are those who said they were "very" or "somewhat" unaware of companies' practices regarding the collection and use of personal information online. 51.2% of all respondents said that.

3.1.2.6 What is the state of respondents' confidence?

Respondents' perception of their current protection

56% of respondents feel they don't protect their privacy enough online and want to do more. This is particularly true of Quebecers and women. Conversely, 43% of respondents feel they are doing enough to protect their privacy online. This time, residents of the Atlantic provinces and Alberta stand out. Unlike many of the other topics in the survey, there are no significant age differences.

Respondents who feel they are not doing enough to protect their privacy online were asked to choose from a list of possible explanations. More than half feel that their lack of knowledge about what to do and what tools or technologies to use is preventing them from doing more. Some tools, such as private search engines and private browsers, were known by barely a third of respondents. A similar proportion of respondents feel that the technologies and tools available are too complex.

Other reasons suggested to respondents as to why they feel they do not adequately protect their privacy online were selected in the following proportions:

- Feeling powerless over the collection and use of their personal information: 38%
- Lack of time or motivation to learn about the privacy practices of websites and apps used: 35%
- Difficulty in identifying and understanding the risks: 21%
- A desire not to change one's routine or daily life online: 18%

Note that the feeling of powerlessness affects more than 50% of respondents residing in Quebec, a statistic that can probably be explained in part by the data leak scandal at Desjardins, which surprised many. Similarly, lack of time or motivation affects over 50% of respondents aged 34 and under.

Acceptable risks

We also asked respondents about the situations in which they agree to provide personal information online. Over 50% of respondents, regardless of age, agree to do so in order to complete online transactions, such as the purchase of goods. The other situations in which respondents are willing to provide personal information are all related to potential financial or material gain: participation in contests (44%), free service (29%) and discounts on online products and services (27%).

Personalization of the online experience is much less persuasive (personalized customer service, personalized recommendations for goods and services, etc.). Just over 5% of respondents would agree to provide personal information online to personalize the advertising they are exposed to, yet most actually provide that information online every day...

It is worth noting that almost a quarter of respondents would not agree to provide personal information in any of the circumstances described above. Again, this result is at odds with the reality of today's Internet users.

3.2 Semi-structured Interviews with Selected Respondents

We conducted approximately 25-minute interviews with 30 survey participants. Those interviews, in both French and English, were conducted within days of the survey, January 23-30, 2020, to ensure good participation by respondents. Interviewees were contacted only after they responded affirmatively to a survey question soliciting their interest in participating in a follow-up interview. They received a $50 thank you for participating in the telephone interview.

3.2.1 Profile of respondents

We interviewed almost as many women (14) as men (16), although many more men indicated an interest in participating in the interviews (27% more). The individuals interviewed ranged in age from 23 to 77, representing generations Z, Y, X, and Boomers. Some demographic information about the respondents is provided in the following table:

Age group	Gender	Region	Language
29 and -	♀	Atlantic	En
	♀	West	Fr
	♂	Quebec	En
	♀	Atlantic	En
	♀	Ontario	Fr
	♂	Quebec	En
40-49	♂	Quebec	En
	♂	Quebec	En
	♀	Ontario	Fr
	♂	Quebec	En
	♂	Ontario	Fr
	♀	Ontario	Fr
	♂	West	Fr
50-59	♂	Prairie	En
	♂	Ontario	Fr
30-39	♂	Atlantic	En
	♀	Ontario	Fr
	♀	West	Fr
	♀	Quebec	En
	♂	Ontario	Fr
	♀	Atlantic	Fr
60-69	♂	Quebec	En
	♂	Quebec	En
	♀	Atlantic	Fr
	♂	Ontario	Fr
	♂	Quebec	En
	♂	Quebec	En
	♀	Ontario	Fr
70 and over	♀	Quebec	En
	♀	Quebec	En

3.2.2 Highlights

At the outset, we asked respondents to rate (again) their overall level of concern for their privacy on a scale of 1 to 10. The average response was slightly higher than in the survey (almost 8 out of 10), perhaps due to the voluntary nature of the interviews; those who chose to participate as a result of the survey may have had a greater than average interest in the topic. It should be noted that two of the respondents indicated that they had studied in the field of new technologies and/or computers, and several others said that they had learned about the subject on their own.

We find no correlation between the amount of time spent on the Internet by the consumers interviewed (from 1.5 hour to more than 12 hours per day, depending on the respondents)

and their level of concern for their online privacy. Note that a 2007 study by Paine Schofield *et al* also concludes that there is no correlation between those aspects[412].

For the most part, the consumers we interviewed access the Internet with several devices – computer, smartphone and tablet. In the interviews, we did not note any impact of the type of device used on the overall level of concern for their Internet privacy. It should be kept in mind, however, that the survey results indicated a higher level of concern when using smartphones. None of the respondents used only his smartphone to access the Internet. Moreover, the behaviours and actions reported by the consumers surveyed to protect their online privacy are more related to their computer. They seem less equipped or inclined to adopt privacy protection measures for their tablets or smartphones. We'll come back to that later.

None of the thirty respondents spontaneously mentioned their connected objects or any particular concern about them.

3.2.2.1 Recent data leaks increase the level of concern

Just over half of consumers surveyed say they are more concerned about their online privacy than at this time last year.

Only one person reported being less concerned than before. He actually had a very low overall level of concern (2 out of 10). It became clear in a discussion with him that he had gained this sense of confidence online, not because he no longer saw/did not see a risk to his privacy, but because he had adopted more online safeguards in recent years and felt more able to deal with the risks.

Those who say they are more concerned about their online privacy than in the previous year point to their increased awareness of the risks. A few participants refer to problems experienced by people close to them, but the vast majority mention more generally the most recent data leaks reported in the media: Desjardins, Capital One and to a lesser extent, Cambridge Analytica and Equifax. The perception that the media are focusing more on the issue of personal information handling online is widespread among participants. There were mixed views on whether there are more risks than before, or whether they are simply more known and publicized.

We observe that the respondents are relatively uncritical of the "Web giants," although the latter's handling of personal information is severely criticized by some experts and media outlets[413]. Similarly, despite the association some make between online privacy issues and

---

412 PAINE SCHOFIELD. "Internet users' perceptions," *supra* note 153, p. 530.
413 See, for example, AMNESTY INTERNATIONAL. "Surveillance giants: how the business model of Google and Facebook threatens human rights," 2019, online: https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF; KAKAES, K. "Zuckerberg's new privacy essay shows why Facebook needs to be broken up," MIT Technology Review, March 7, 2019, online: https://www.technologyreview.com/2019/03/07/1248/zuckerbergs-new-privacy-essay-shows-why-facebook-

social media, few participants mention Facebook, Instagram, Twitter or TikTok without the topic being directly raised by the interviewer. And Amazon and Google receive surprisingly positive comments in the context of an interview about online privacy and raise very few concerns among respondents[414]. We'll come back to that.

3.2.2.2 Financial risks first and foremost

As in the survey, identity theft is the number one risk for the vast majority of respondents. We note that almost all Quebec respondents mention the Desjardins situation. And when respondents do not mention the risk of identity theft first, it's because they mention a situation that could result from this theft, such as a stain on their credit report or a fraudulent transaction in their name.

Only two respondents are exceptions to this rule and express relatively little concern about identity theft and its potential financial and other impacts. Both are among the youngest of the interview participants. One of them explained that he was not very concerned about the issue because "at his age" he would not "really" have a credit record to protect.

When asked about what they fear from identity theft, participants primarily point to the following consequences:

- Fraudulent use of their banking or credit information (opening accounts, applying for credit, making purchases, etc.)
- Financial losses
- The "destruction" of their credit report
- Liability for loans taken out in their name
- The loss of time or the need to take countless steps to restore their financial situation

A few respondents also raised more general concerns about their place in society. One worried that he would have to "rename" himself after identity theft, while another suggested that he might simply "not exist anymore."

---

needs-to-be-broken-up/; CAMERON, D. "Amazon's Favorite New Word Is 'Privacy,' But Does It Even Know the Meaning?," Gizmodo, September 25, 2019, online: https://gizmodo.com/amazons-favorite-new-word-is-privacy-but-does-it-even-1838460901

[414] Google and Amazon even top the list of tech brands that Canadians trust the most according to the 2020 CanTrust Index (58% and 53% trust rates respectively): SHANKAR, B. "Google and Amazon are the most trusted tech brands in Canada: study," Mobilesyrup, April 23, 2020, online: https://mobilesyrup.com/2020/04/23/2020-proof-cantrust-index/

3.2.2.3 Targeted advertising and spam divide respondents

As soon as respondents are asked about perceived risks to their online privacy that are not directly related to the use of their financial information, the answers become vaguer. Many respondents openly say they don't care about those "other risks," as in the case of this participant:

> "It's mostly identity theft. Apart from that, I'm not that worried about it. Except for anything financial, anything else I'm not worried about!"
> *Participant - 40 to 50 years of age*

Those responses contrast with the survey results, which still show a high level of concern about the risks associated with targeted advertising, profiling and automated decision-making online.

Moreover, many respondents naturally bring the discussion of other risks raised by the interviewer back to identity theft and its potential financial consequences. When asked about online profiling and the sale of collected personal information to third-party companies, one respondent expressed concern that her information might also be mistakenly sold to "criminals" who would use it to steal her identity. Another respondent was concerned about the security of the servers containing the data processed for profiling purposes and the risk that it could be stolen and used by a hacker… to steal her identity. When it comes to receiving unwanted email, many point to the risk of phishing. Regarding harassment on social media, many mention scams on those platforms.

Targeted advertising

Targeted advertising bothers a majority of respondents. The expressions "annoying," "tiresome" and "irritating" are regularly used in the discussions. However, opinions diverge, beyond the initial discomfort.

Only a few respondents expressed concern about the practice because it exposes the extent to which their personal information is collected and processed and/or because their interests and buying habits are private information that should not be so widely known and used without their knowledge.

The others are rather resigned. "It's more annoying than concerning," says one. Targeted advertising is annoying, just like any other advertising, but it's considered harmless. Many point out that it's easy to ignore (or even block). Others defend the companies that use this commercial practice because it's logical in a capitalist society that favours maximizing profits and exploiting available data to that end.

Lastly, a few respondents even see benefits to targeted advertising, in that it would make their online shopping easier and occasionally save them money. One respondent noted that

he feels much less "aggressed" by a personalized ad than by an ad for a product or service that is not at all suitable for him (and that he describes as unnecessary).

Table 12
Excerpts from interviews about targeted advertising

DISCOMFORT	INDIFFERENCE	ACCEPTANCE	INTEREST
"It gets a little bit too personal sometimes… Too much information that they know." "It's like they are spying on you or something. It makes me uncomfortable." "Ce n'est pas nécessairement terrible qu'ils sachent ce que j'achète, mais ça remet en question le concept même de vie privée. C'est à moi, ces renseignements-là." "It's kind of creepy!"	"Je comprends que ça peut en déranger certains, mais moi, je n'ai pas de problème avec ça." "Le fait qu'ils sachent que j'aime quelque chose en particulier : ils ne feront pas grand-chose avec cette information-là !" "It's annoying, but it's not a major concern. I'm not upset that they know what I like to buy." "C'est fatigant parce que tu te sens écouté, mais je ne pense pas qu'avec ça ils peuvent vraiment faire de quoi de malin. Ce ne sont pas des données importantes, des données sensibles."	"If you're going to use Facebook or Snapchat, you go to a website that is provided for free, then they are going to use your data. If you don't want them to use tour data, don't use their services." "I think that's just them advertising to the best of their abilities. It doesn't mean you have to buy it. It doesn't hurt anyone in any way. You can just ignore it super easily." "Quand on s'amuse sur Internet, il faut s'attendre à ça."	"It's kind of good in a way. You see ads that you might be interested in. it's an advantage actually." "Je pourrais même avoir un spécial." "Parfois, ça peut être bénéfique pour moi. Je fais le choix d'embarquer ou non."

On the subject of the acceptability of targeted advertising among Canadian consumers, we note that a 2015 study by Option consommateurs reached a similar general conclusion[415]. That in-depth study on behavioural advertising (which included focus groups in Montreal and Toronto) nevertheless provides some nuances regarding the relatively favourable position of many consumers, particularly when certain information deemed more private is used.

[415] "Despite their concerns, consumers also seem to find value in the business model of online companies, which are financed in part by BPA [behavioural online advertising]. (…) A few add that this form of advertising can even be beneficial, allowing them to learn about relevant discounts, discover new buying ideas or compare products": CONSUMER OPTION. "The Price of Free, *supra* note 594, p. 33.

Lastly, many respondents also seem to believe they are immune to online profiling as they would not shop or buy online. Respondents show a very similar detachment regarding spam and anti-social behaviour on social media.

Spam

As with exposure to targeted advertising, respondents are annoyed by the receipt of unwanted email. All of them, however, seem to be resigned and underline the effectiveness of mechanisms put in place by email providers to mitigate the inconvenience.

> "It bothers me, but not to a great extent because I have mechanisms to filter that away."
> *Participant - 60 to 70 years of age*

> "It takes exactly a second and a half to hit delete. No big deal."
> *Participant - 40 to 50 years of age*

But is spam still an invasion of their privacy online? Respondents are divided on that question, but a majority answer no, it's simply an annoying marketing practice – like many others – but nothing more. A few are more troubled by the practice and see it as evidence of the sale of their email address to third parties without their consent.

3.2.2.4 Social media: a risk for others only

Interview participants are even more nonchalant about the risks of anti-social behaviour online (threats, harassment, or bullying based on Internet users' personal information). Only one respondent mentions this spontaneously (when discussing the specific risk of *catfishing* on social media) and few express concern when asked directly about the topic.

Those who are sensitive to this risk are most critical about the amount of personal information voluntarily disclosed by social media subscribers and collected in other ways by the platforms, and about the ease with which this information can then be used.

> "Strangers know too much information about your private life."
> *Participant - 20 to 30 years of age*

> "I just don't want people to know what I'm doing or where I am."
> *Participant - 30 to 40 years of age*

The differences in views and experiences on this topic are interesting. While one respondent doubts that these situations actually occur, another says he "sees them regularly on Facebook."

We find that, with few exceptions, participants don't feel at risk for anti-social behaviour online, whether because they don't have social media accounts, or because they think they share little personal information, or because they have tightened their privacy settings.

However, many fear for the "younger" generations and their loved ones (children, grandchildren), which is reminiscent of the phenomenon of optimism bias (described briefly in Section 2.3.2.2).

> "I am not concerned on a personal level, but I could see the danger, how it could affect others."
> *Participant - 30 to 40 years of age*

3.2.2.5 Protective behaviours that are difficult to explain

Many participants readily admit that they have not adopted many behaviours specifically to protect their privacy or personal information online.

According to the survey results, Canadians take just over 5 steps to protect their privacy online. When asked to identify the measures (behaviours or tools) that they take, without any suggestions or choices, interview participants name an average of 2 to 3. The use of antivirus software is almost always mentioned.

Thus, there is an apparent discrepancy between the survey and interview results as to the extent of privacy behaviours actually adopted by Canadian Internet users. It's not possible for us to determine whether respondents have "embellished" their online habits (by checking off behaviours that they don't actually engage in or do so infrequently), or whether those behaviours are so embedded in their online routines that they are not always able to distinguish and identify them as specific to protecting their online privacy.

In addition, there is significant confusion between some online privacy enhancement tools. This is particularly true between private browsers, private browsing modes, and private search engines. Participants who are familiar with or use them mix up the terms regularly. Password managers are sometimes confused with antivirus software, presumably because some antivirus software now offers password management capabilities. The survey results regarding knowledge and use of these tools should therefore be viewed with caution. The general awareness of the tools was moderate and their use was rather low.

Aside from antivirus software, the benefits of which seem to be universally recognized by now, participants regularly have difficulty explaining the usefulness of a behaviour or tool they have adopted to protect their privacy. Many "know" that they should do this online, but don't really know why.

> "I'm not technically savvy. I go with these things, because I believe they're gonna protect my online privacy"
> *Participant - 60 to 70 years of age*

> "I don't know the details of how it works. I just know I use it to protect my computer. (…) I don't know a lot about the cyberworld. I just know I use all these tools to protect myself."
> *Participant - 70 years and older*

Many older participants say they rely heavily on family and friends to keep their electronic devices safe. The "contacts" identified by participants are more comfortable with

technology (daughter, husband, grandson) or have specific knowledge of it (a co-worker who works in the computer field, for example).

> "Vous savez on n'est pas tous des cracks de l'informatique. Mon petit-fils de 16 ans nous en montre des fois et on dit « oh je ne savais pas ça ! ». Ils sont venus au monde avec un ordinateur dans les mains, eux !"
> *Participant - 60 to 70 years of age*

3.2.2.6 Their views on…

Passwords

We find that difficulty remembering multiple passwords is an almost unanimous problem among interview participants. Most admit – for that reason – that they don't change their online passwords on a regular basis (and without being forced to do so). Many report, as if to justify themselves to the interviewer, that they do try to vary the passwords they create. We note that the use of a variety of complex passwords for the majority of online accounts is much less reported in the interviews than in the survey.

> "C'est peut-être mon seul défaut. J'ai souvent les mêmes mots de passe. J'ai 3-4 mots de passe pour tous les sites et je réussis quand même à les oublier !"
> *Participant - 30 to 40 years of age*

> "Ça fait quelques années que j'ai les mêmes mots de passe sur Internet. Tu es bien dans tes pantoufles. Tu ne veux rien changer. Tout va bien. Mais je sais quand même que ça peut être dangereux…"
> *Participant - 30 to 40 years of age*

Cookies and browsing history

Many admit they don't delete cookies and browsing histories on their devices often enough. And many do so without being able to explain how this helps protect their online privacy.

> "I don't really know what the purpose, the benefit of deleting your browsing history is. Maybe there is one, I'm not sure."
> *Participant - 30 to 40 years of age*

Their level of concern about targeted advertising is quite modest; similarly, respondents associate only to a small extent the deletion of cookies and browsing histories with online profiling. In fact, we find that many see this behaviour as a way to protect their personal information (especially passwords) in case of theft or unauthorized physical access to their devices and seem to have little interest/concern regarding the use that can be made of cookies and their browsing history directly online. For example, no less than three respondents insist that they don't have to delete them since they're the only ones using their login device.

> "The two computers that I use most of the time, I'm the only one that uses them, so I'm not worried about anyone looking at my browsing history."
> *Participant - 40 to 50 years of age*

A few participants delete cookies and browsing histories for reasons other than protecting their online privacy. Two respondents have at times deleted their browsing history so that their employers or other members of their household don't know what they've been viewing. Another respondent regularly deletes browser cookies so as not to slow down his computer unnecessarily. He doesn't see how this practice would help protect his online privacy.

Online transactions

A few respondents make very few or no purchases or transactions online, either because of a lack of interest, ease and confidence in using e-commerce or due to a fear of providing their financial information to dishonest companies. In fact, privacy concerns seem to be generally subordinate to the uncertain nature of online purchases (will they actually receive the product? Will it be in good condition? Etc.).

For the other respondents, banking and shopping are part of their daily online life, but the watchword is caution. And all methods are good: visiting only large company websites, HTTPS websites or websites recommended by relatives or that have positive online reviews, using *PayPal*, providing only required information, etc. Many respondents identify Amazon as a trusted website where they feel comfortable shopping without fearing for their personal information. At first glance, this is surprising given past allegations against the company[416]...

3.2.2.7 Privacy enhancing technologies: moderate interest and distrust

Based on participants' reported concerns and previously mentioned protective behaviours, we presented a few privacy enhancing tools (other ones, in some cases) to better understand participants' potential interest or fears regarding their use. Our questions about those tools were preceded by a brief description of how they work and their potential privacy benefits.

---

[416] See, for example, MANANCOURT, V. "'Millions of people's data is at risk' - Amazon insiders sound alarm over security," Politico, February 24, 2021, online: https://www.politico.eu/article/data-at-risk-amazon-security-threat/; LYNKSEY, D. "'Alexa, are you invading my privacy?' - the dark side of our voice assistants," The Guardian, October 9, 2019, online: https://www.theguardian.com/technology/2019/oct/09/alexa-are-you-invading-my-privacy-the-dark-side-of-our-voice-assistants; HAY NEWMAN, L. "Amazon's Latest Gimmicks Are Pushing the Limits of Privacy," Wired, October 11, 2020, online: https://www.wired.com/story/amazon-drone-camera-go-palm-data-privacy/

It should be noted that several participants of various ages seemed uncomfortable discussing "more technical" tools, while stating they were not familiar with those tools, had not used them, and were not sure they could use them.

> "C'est plus pour les personnes qui travaillent dans l'informatique, qui sont douées (...) Moi, je ne sais pas le faire."
> *Participant - 30 to 40 years of age*

> "I'm just not really familiar with them. It's not that I would never use them, but I don't know enough about it to download one and use it "
> *Participant - 30 to 40 years of age*

Generally, we were surprised by the low level of interest among participants in the tools presented to them, with the exception of the ad blocker. We note a high level of distrust in the operation of the other tools presented and their ability to protect users' personal information. We will discuss in more detail the participants' criticisms of some of the tools presented. Indeed, the expression "if it's free, you're the product" seems to have left its mark. Many questioned the funding of the free tools' providers. Others did not understand the companies' choice and almost seemed to criticize them for not fully exploiting their personal information as all the others do, thus unintentionally revealing how fully they have internalized industry practices.

The example of private search engines

Only a few participants know about private search engines. Many confuse them with private browsers or with the latter's private browsing mode.

Two participants initially said they had never used a private search engine, before changing their minds and pointing to their past use of *DuckDuckGo* and *Ecosia*. Those engines had not been chosen (and used) for reasons related to personal information protection. In one case, the participant had turned to *DuckDuckGo*, one of those suggested by her browser, on a day when she found Google too slow. In the other case, the participant turned to *Ecosia* for environmental reasons (the company helps plant trees around the world). Although she didn't know it was a private search engine, she was able to provide a lot of details about the German company's environmental efforts.

A brief description of private search engines was given to participants, who immediately drew a parallel with Google. One participant asked if those engines are available... on Google!

In general, participants showed little interest in using private search engines. Some who had already used them said they're less effective and offer worse search results than Google.

> "I feel it brings up a lot of irrelevant search results. So, it's a little bit of extra work."
> *Participant - 30 to 40 years of age*

Those who have never used private search engines also had questions about their effectiveness – a factor that seems to determine whether or not they will adopt this type of tool.

> "I might be interested in using those, as long as they're effective. I mean it would depend on if they can give me the proper results."
> *Participant - 60 to 70 years of age*

> "I don't think I would use the private search engines, mostly because I find that even Yahoo or Bing aren't as efficient as Google."
> *Participant - 30 to 40 years of age*

Beyond the effectiveness of private search engines, some question the description of their practices in handling users' personal information.

> "Est-ce que vraiment ça va me protéger ou on nous dit que ça va nous protéger, mais en arrière-plan, non?"
> *Participant - 30 to 40 years of age*

> "They have to make money somehow! I'm just wondering how they are doing it."
> *Participant - 40 to 50 years of age*

Some participants concluded the discussion by acknowledging that they are too used to their current search engine (especially Google) and can't imagine changing it, even if it would improve their online privacy.

The example of password managers

Most of the participants who are presented with a password manager don't seem particularly interested in using the tool. This reaction is somewhat surprising given the widespread feeling that it's difficult to remember all the passwords required online today.

Some would like to use a password manager, but fear forgetting its own password. Others are strongly opposed to using the tool because of another fear: What happens if the manager's password is hacked on the user's device or with the company? This concern is shared by consulted consumers of all age groups.

> "I would be wary about that. Passwords are the biggest things. To have a system that keeps them all in one place. I'm very wary of that."
> *Participant - 30 to 40 years of age*

> "Si tu mets ces mots de passe là dans le gestionnaire, il y a un tiers qui va le connaître. C'est mieux de les garder pour soi. Il y a une personne quelque part qui pourrait y accéder sinon."
> *Participant - 40 to 50 years of age*

> "Je ne suis pas certain de vouloir utiliser ça parce que si eux autres me donnent un mot de passe, ils vont connaitre le mot passe eux aussi. Qu'est-ce qui me dit que ce mot de passe là, il n'est pas revendu à d'autres après ? Je ne sais pas."
> *Participant - 60 to 70 years of age*

One participant proposed the following solution to use the tool, which he sees as useful despite that fear: Putting all of one's passwords in the tool, except those for one's most important accounts (e.g., bank accounts).

Among the few participants who had already used or regularly use a password manager, the opinions are positive, but some limitations of the tools are criticized, such as their cost and their incompatibility with certain websites and platforms.

The example of disposable email addresses

Disposable email addresses were neither of interest nor concern to the consumers interviewed. Very few participants were aware of them. None use them. And hardly any see any potential use for them.

In fact, many participants believe they're already doing something similar to what the tool would do, i.e., they have multiple email addresses, some of which are intended for websites and contests that may flood them with spam later on.

> "I wouldn't say it's disposable, but I have one email that I use for those things, as opposed to my primary email."
> *Participant - 50 to 60 years of age*

> "Moi, j'ai créé une adresse courriel justement pour quand il me demande une adresse, et que je n'ai pas le choix, pour visiter le site. (...) Et quand je reçois trop de courriels indésirables sur celle-là, je la ferme et j'en fais une autre (...) le moindrement qu'on me demande une adresse courriel pour rentrer sur un site, je donne une adresse que je sais qu'à un moment je vais fermer."
> *Participant - 60 to 70 years of age*

One participant also noted that those temporary email addresses are sometimes identified and blocked by websites when he tries to use them.

The example of ad blockers

Ad blockers differ from the other tools presented to the consumers interviewed in that the latter are more familiar with ad blockers and use them regularly. On the other hand, most users don't see them as helping to protect their online privacy, thus again highlighting the mixed views on whether or not targeted advertising intrudes into Internet users' privacy. Respondents mostly see ad blockers as a way to deal with the inconvenience of advertising.

> "Ça protège ta vie privée, oui et non. C'est juste des publicités. C'est juste fatigant. C'est juste agaçant. Dans mon cas, c'est surtout pour ça que je l'utilise... Comme ça il n'y a pas de *pop-up* ou de publicités qui apparaissent."
> *Participant - 30 to 40 years of age*

> "Je ne pense pas du tout que ça protège ma vie privée. Je pense juste que ça empêche les publicités d'apparaitre."
> *Participant - 40 to 50 years of age*

3.2.2.8 A surprising level of confidence

The vast majority of respondents are confident and satisfied with how they currently protect their privacy online.

Only six out of 30 participants were clearly dissatisfied and five others were reluctant to say they were fully satisfied ("somewhat satisfied"), knowing they could theoretically do more.

> "I'm doing as much as I could. I'm sure there are more ways I could be safer, but with the time commitment and financial situation, I feel I'm doing as much as I could."
> *Participant - 40 to 50 years of age*

This result is surprising considering that more than half of survey respondents felt they were not doing enough to protect their privacy online.

We don't observe a correlation between participants' satisfaction and their overall level of concern for their online privacy. In fact, several respondents who expressed satisfaction with their current online privacy made surprisingly cynical comments about the state of their online privacy during the interview.

It's not possible for us to determine whether participants are satisfied because they believe they are adequately/sufficiently protecting their information online or because they have not yet experienced an incident involving their personal information online.

Perhaps they're also satisfied because they believe they're doing everything they're capable of doing in practice. This is what emerges from the explanations of dissatisfied consumers: They would like to do more, but don't think they can. This inability stems from a multitude of factors:

> "I haven't implemented more, better protection measures, because I don't know what is available to me and I'm not that computer-savvy. I'm not as knowledgeable as I wish I would be. I know that the basics are not enough. "
> *Participant - 30 to 40 years of age*

> "There are always more expensive antivirus, anti-phishing, software, upgrades to get by. I don't want to spend hundreds of dollars every year to do that."
> *Participant - 40 to 50 years of age*

> "I only have a limited data plan. So, if I keep downloading new apps, that wipes out all my monthly data. "
> *Participant - 40 to 50 years of age*

> "My whole day would be spent reading privacy policies. "

Participant - 30 to 40 years of age

"Dans la vie, être protégé à 100 %, c'est impossible. C'est sûr que quelqu'un qui est malveillant et qui est un pro va pouvoir me retracer quand même. Ces outils-là, c'est juste une parure. Vaut mieux le faire que ne pas le faire, mais…"
Participant - 30 to 40 years of age

3.2.2.9. A wide variety of solutions

All respondents were asked about the best way to help consumers better protect their privacy online. The answers concerned three types of stakeholders.

Consumers

Respondents appear to think Internet users themselves are primarily responsible for protecting their privacy online. In this view, Internet users should become better informed about the risks and, after doing the necessary research, should adopt more protective behaviours online. While respondents were lenient regarding their own behaviour's limitations (e.g., justifications based on lack of time or knowledge), they appear to be harsher toward those of others.

"An attitude shift is needed. Understanding what really needs to be private and what doesn't. […] Basically, people are lazy. They don't think about this stuff. "
Participant - 40 to 50 years of age

Governments

The majority of respondents advocated the awareness-raising and education of Internet users. Some saw this as a task for Internet users alone, but others felt that government and its agencies should be involved, including through classroom training and widely distributed videos or explanatory materials.

Respondents gave surprisingly little mention to the need for improved privacy laws, perhaps due to unawareness of the laws' contents or to doubts about the laws' effectiveness.

"Legislations have loopholes and most corporations are very savvy to finding those loopholes. Even if there are no loopholes, we, as citizens, don't know if the rules are being followed. So I don't think legislation really helps."
Participant - 30 to 40 years of age

Companies

Respondents made few suggestions for improving online privacy that are related to private companies. Yet large Web companies, such as Apple and Google, have a major influence on the evolution of online privacy practices, through the companies' capacity to influence legislators and direct the practices of companies that rely heavily on them for data access and use. The American magazine Politico recently described large Web companies as "the world's biggest privacy regulators[417]."

The respondents don't necessarily seem to share this view (or be aware of it)! They did, however, point to some improvements they would like to see from the companies, such as more widespread use of dual authentication. Others would like to see, on the websites they visit, clearer disclaimers about personal information policies.

> "Not like in a tiny font in the terms and conditions that you don't read! Something kind of in your face: Ok, this is what we're using. This why we're using it. We won't sell it to any other company, if something happens we will…"
> *Participant - 30 to 40 years of age*

Others support the development of additional privacy enhancing tools, but at the same time acknowledge that a good variety already exist. The specific usefulness of the additional tools suggested remains unclear. Generally speaking, the missing tool would protect against everything, without any intervention from the Internet user…

> "A third party neutral type that would more or less kind of manage the privacy issues and not use it to their advantage"
> *Participant - 40 to 50 years of age*

> "Some type of app or something that you can search that has everything bundled into one."
> *Participant - 20 to 30 years of age*

3.3 Conclusions on the Survey and Interviews

3.3.1 A rising level of concern

Canadian Internet users' level of concern appears to be undeniably on the rise compared to previous years. The Internet users interviewed in 2020 for this study almost unanimously expressed this. And other surveys of Canadians appear to confirm this trend.

Surveys conducted by the Office of the Privacy Commissioner of Canada in recent years reveal that the level of concern for privacy (in general, but not specifically online) has been rising steadily since 2012. 25% of respondents said they were extremely concerned about

[417] SCOTT, M and MANANCOURT, V. "Google and Apple are the world's biggest privacy regulators," Politico, April 27 2021, online: https://www.politico.eu/article/google-apple-privacy-regulators-gdpr-floc/

the issue in 2012 versus 37% in 2018[418]. And the most recent survey from the Center for International Governance Innovation estimates that the level of concern about online privacy increased between 2018 and 2019 among nearly one in two Canadian respondents[419]. It will be interesting to analyze those organizations' future surveys, conducted during or possibly after the COVID-19 pandemic that contributed to increased internet use. Some experts have expressed particular concern that Internet users' privacy has been given little consideration by executives and businesses in managing the crisis[420]. Do consumers share this concern?

Given the data leaks that have occurred in Canada since the Center for International Governance innovation survey was conducted – including the Desjardins and Capital One leaks that affected many Canadians or their loved ones – it is plausible that no longer half, but now the vast majority of our interviewees rate their level of concern as higher than in the previous year.

Moreover, past surveys by Office of the Privacy Commissioner of Canada also show a divide in privacy concerns among residents of some Canadian provinces, notably among Quebecers and British Columbians[421]. Given that those surveys date from before the Desjardins leak that particularly affected Quebec, one must conclude that the particularly high level of concern among Quebecers cannot be explained by that fact alone.

3.3.2. Ambivalence about non-financial concerns

While the survey results indicate a high level of concern about receiving unwanted email and being exposed to targeted advertising and anti-social behaviour online, the interview results are less compelling. Very few interviewees mention those concerns spontaneously, and responses are rather nonchalant when the risks are directly presented to them. In general, consumers are annoyed, but appear relatively unconcerned. The only risks for which responses are consistent in the survey and interviews are those related to computer security and unauthorized access and use of Internet users' financial information. Identity

---

418 OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. 2018-2019 Survey, *supra* note 158, Figure 3.
419 Survey conducted from December 21, 2018 to February 10, 2019 among 25,229 Internet users from 25 countries. We will limit our analysis to the results obtained from the 1,000 Canadian respondents aged 18 to 64: CENTRE FOR INTERNATIONAL GOVERNANCE INNOVATION. "Global Survey," *supra* note 99.
420 MORISSON, S. "The year we gave up on privacy," Vox, December 23, 2020, online: https://www.vox.com/recode/22189727/2020-pandemic-ruined-digital-privacy; HO, S. "COVID-19 eroding global internet freedom, Canada among the most free, report says," CTV News, October 14, 2020, online: https://www.ctvnews.ca/sci-tech/covid-19-eroding-global-internet-freedom-canada-among-the-most-free-report-says-1.5145180; SINGER, N. and SANG-HUN, C. "As Coronavirus Surveillance Escalates, Personal Privacy Plummets," New York Times, March 23, 2020, online: https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html; VILLENEUVE, S. and ELIAS, D. "Surveillance Creep: Data collection and privacy in Canada during COVID-19," Brookfield Institute, September 2, 2020, online: https://brookfieldinstitute.ca/surveillance-creep-data-collection-and-privacy-in-canada-during-covid-19/
421 OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. 2018-2019 Survey, *supra* note 158: "Compared to respondents in British Columbia, those in the Atlantic region, Quebec and the Prairies are more likely to be concerned about their privacy."

theft and its consequences are undoubtedly the number one concern of Canadians when it comes to online privacy.

How do we reconcile the survey and interview results regarding other possible risks? We hypothesize that the term "concern" used in the survey is associated with both fear and annoyance for many respondents. The choice of term may have something to do with this, but so may the inquiry method. A study by Singleton and Harper of guided surveys regarding online privacy confirms that survey respondents tend to be more alarmist than interviews in which participants are asked to give spontaneous answers[422]. It's easier for respondents to dramatize their responses when presented with closed-ended questions and answer choices. The authors refer to the "talk is cheap" phenomenon.

3.3.3 Great ignorance and a certain wilful blindness

Many of the consumers surveyed said they were powerless to protect their privacy online because of a lack of knowledge about the risks and appropriate safeguards. And even when they say they "know" about a risk or an available tool, confusion regularly reigns in practice.

More than one fifth of consumers surveyed were unable to correctly answer very simple questions about companies' personal information collection and use practices. Rice and Bogdanov's 2019 study specific to Canadians' privacy literacy levels arrives at even more alarming results:

> Many Canadians lack a basic awareness and understanding of how companies collect and use their personal data. Specifically, on 10 of the 16 statements, more than 60% of the respondents could not correctly identify how their data were being collected and used[423].

Our consumer interviews also show significant ignorance about the various privacy enhancing tools available free online. What do they do? What risks can they help reduce or eliminate? How do they work? Few are able to answer those questions, which may explain, at least in part, the low use of those tools, despite expert recommendations.

But ignorance sometimes gives way to wilful blindness. While admitting to knowing too little about the risks to their online privacy, a surprisingly high proportion of interview participants not only are satisfied with the way they protect themselves against those risks, but also tend to view the risks as greater to others than to themselves. Younger respondents are concerned about older Internet users who may be less comfortable with technology. Older respondents express concern about younger Internet users disclosing too much personal information online. Many are aware of the risks to others and believe they themselves are safe, but don't seem to be taking any steps to justify that confidence.

---

[422] SINGLETON, S. M. and HARPER, J. "With a Grain of Salt: What Consumer Privacy Surveys Don't Tell Us," February 11, 2002, online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=299930

[423] RICE, M. D. and BOGDANOV, E. "Privacy in Doubt: An Empirical Investigation of Canadians' Knowledge of Corporate Data Collection and Usage Practices," Canadian Journal of Administrative Sciences, vol. 36, No. 2, 2019, p. 166.

3.3.4 Behaviours that are difficult to change

Respondents identified a number of protective behaviours they have adopted over the years to protect their online privacy, including the use of antivirus software, which appears to be well integrated into the lifestyle of Canadian Internet users. However, the survey results paint a more positive picture of the adoption of protective behaviours by Canadian Internet users than do the interview results. It's difficult to determine what accounts for this discrepancy, but there is concern that some survey respondents may have embellished their situation, particularly just after answering a series of questions about the extent of risk to their personal information online.

In general, we find that Internet users engage in a fairly limited number of protective behaviours online. And they seem relatively uninterested in changing this, even though many feel they "should" do more. Beyond the lack of knowledge about those behaviours, the survey and interviews reveal a certain lack of will, a feeling of powerlessness and a certain cynicism among many respondents, which has the effect of reinforcing their current behaviour.

3.3.5 What about the privacy paradox?

We discussed above the debate surrounding the very existence of an online privacy paradox (section 2.3). We described this paradox as a mismatch between the concerns of Internet users and their behaviour with respect to online privacy issues.

But how can we determine whether this phenomenon is present among the Canadian Internet users surveyed? There seems to be no common methodology for the various studies conducted on the subject, and their conclusions are sometimes contradictory. Some of our survey's results, although not conclusive on their own, can nevertheless point us in the right direction. They will be presented briefly in the following pages.

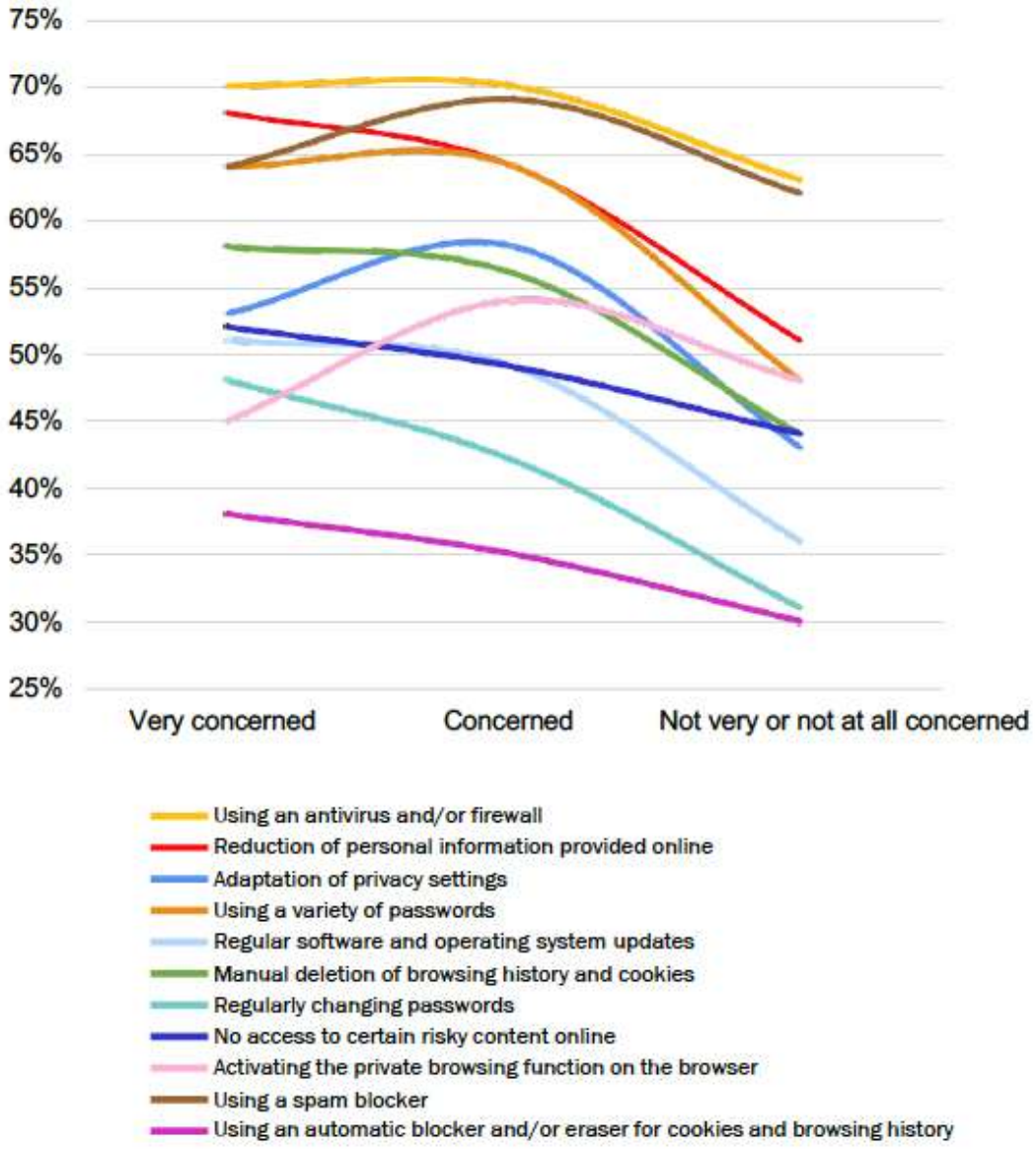
3.3.5.1 Overall level of concern and adoption of protective behaviours

We find that the level of concern about online privacy has relatively little influence on the adoption of behaviours to reduce the risk of online privacy breaches. In general, respondents who express a high level of concern about their online privacy do not engage in any more protective behaviours than those who express a moderate level of concern, and only slightly more than those who express little or no concern (less than a 10% difference on average).

The table below illustrates the percentage of respondents who engage in a behaviour based on their overall level of concern. It should be noted that this is not an analysis of the effectiveness of the protective behaviours adopted, but only of the number of behaviours adopted based on the overall level of concern expressed.

Curiously, we find that some safeguards are used more often by respondents who are not among the most concerned about their online privacy.

Table 13
Adoption of online privacy behaviours,
by overall level of concern



A respondent is considered "very concerned" about his online privacy if he expressed a concern level of 9 or 10 out of 10. A respondent is considered "concerned" if he expressed a level of concern of 6 to 8 out of 10. A respondent is rated as "not very or not at all concerned" if he expressed a level of concern of 5 or less out of 10.

3.3.5.2 Specific level of concern about certain risks and the adoption of specific protective behaviours

Antivirus, varied passwords, spam and advertising blockers, etc. We can see that the measures adopted in greater numbers by the Internet users surveyed respond to a variety of risks. But do they correspond to the risks specifically identified by the respondents who use them?

We compared the adoption of certain behaviours among respondents according to their level of concern about specific risks to their online privacy. From the list offered to respondents, the behaviours analyzed below are those most likely to reduce the identified risks.

We find that respondents who are more concerned about certain risks generally take more appropriate action to address those concerns, but again, the gap is relatively small by level of concern. The largest gaps pertain to concerns about hacking of personal information.

Table 14
The adoption of protective behaviours and tools
according to the specific level of concern for certain risks

Behaviours	% of respondents who adopt the behaviour based on their level of concern for specific risks to their online privacy*		
Risk of personal information hacking			
	Very concerned	Concerned	Not very or not at all concerned
Using an antivirus and/or firewall	73%	64%	53%
Regular software and operating system updates	51%	43%	37%
Avoiding certain online content (emails, hyperlinks, websites, etc.)	52%	53%	42%
Using different passwords for most online accounts	65%	57%	47%
Regularly changing passwords	43%	40%	35%
Using a password manager	37%	32%	28%
Using dual authentication	51%	45%	36%

Risk of profiling for the purpose of exposure to targeted advertising			
	Very concerned	Concerned	Not very or not at all concerned
Using an ad blocker	58%	62%	60%
Manual deletion of browsing history and cookies	59%	53%	49%
Using an automatic cookie and history blocker or eraser	40%	34%	29%
Activating the private browsing function on the browser	48%	52%	51%
Risk of receiving unwanted emails			
	Very concerned[424]	Concerned	Not very or not at all concerned
Using a spam blocker	67%	68%	65%
Using temporary email addresses	19%	21%	20%

Percentages are rounded to the nearest whole number.

We thus find that respondents' overall level of concern is not necessarily a determinant of protective online behaviour, except for Internet users who are not at all concerned about the issue. Those users consistently take fewer actions, although the differences remain surprisingly small. On the other hand, when unconcerned users do choose to adopt certain privacy protection behaviours, those choices are in response to specific fears and are thus influenced by their concerns. So we doubt there is a complete discordance between Internet users' concerns about their online privacy and their actual online behaviour, as opposed to what the privacy paradox theory holds.

[424] Respondents are considered "very concerned" if they expressed a level of concern of 9 or 10 out of 10 about this risk. Respondents are considered "concerned" if they expressed a level of concern of 6 to 8 out of 10. Respondents are considered "not or not very concerned" if they expressed a level of concern of 5 or less out of 10.

ACCESSIBILITY OF PRIVACY ENHANCING TECHNOLOGIES

One of the most disappointing results of the 2020 survey and interviews was the very low awareness and use of privacy enhancing tools by Canadian Internet users, even though those tools are highly recommended by experts. Less than a third of respondents have ever used a private virtual network, a private search engine or a private browser, for example. With the exception of spam and ad blockers, the various tools available remain unknown to a considerable portion of the population. And when the tools are discussed in interviews, interest is less than modest. Many doubt they're able to use them, because they're not comfortable with technology or because they're suspicious of the usefulness and effectiveness of those tools.

In light of these results, it seems relevant to analyze how the tools' providers present their products and how likely they are to respond to the concerns of Canadian Internet users, based solely on how the tools are presented. It should be noted that this is not a study of the tools' specific operation or actual usefulness in protecting their users' privacy.

We will focus on the presentations of seven types of tools and three popular providers for each tool, in order to develop a picture of existing types of presentations and what shortcomings if any the latter may have in addressing the fears consumers express about those tools.

It should be noted that a consumer who searches for tools on a search engine will also be offered a few specialized websites and blogs (e.g. *PCMag*[425], *TechRadar*[426], *CNET*[427], etc.) that offer explanations about the tools or comparisons of the different products offered. However, no resource stands out and it's highly likely that a consumer will eventually click on the website of a provider of the tool he is looking for, mainly because of the provider's search engine optimization (SEO) efforts. We therefore focus our analysis on the providers' presentation of the tools.

[425] PCMAG. Online: https://www.pcmag.com/
[426] TECHRADAR. Online: https://www.techradar.com/
[427] CNET. Online : https://www.cnet.com/

4.1 Methodological Summary

The providers' presentation of the tools' purpose and use was analysed using an analytical grid mainly modelled after the criteria used by the European Network and Information Security Agency (ENISA) in its assessment of the market for online privacy enhancing technologies[428].

We placed particular emphasis on the presentation and explanations offered by providers regarding online privacy risks, while taking into account the *PrimeLife* consortium's findings:

> Users often do not have a correct understanding of where (at what site) their personal data is stored and processed and to what entities their data is transferred. When designing and testing privacy-enhancing identity management systems, investigations are thus needed on how to evoke the correct mental models in users with regard to where what data are transmitted and under whose control the data are stored and processed. Having a comprehensive mental model will be essential for them to estimate privacy risks correctly, to understand better how far PETs can protect their online privacy[429].

With respect to the simplicity and clarity of the language used by providers, we have drawn on the Canadian government's work on "successful communications" between the state and its citizens, many of whom have low literacy levels[430]. In the case of software tools pertaining to online privacy, we think a relatively low level of digital literacy among the average Internet user should be assumed.

Data were collected at selected provider websites and analyzed during the winter of 2020-2021.

4.1.1 General comments on the accessibility of information

4.1.1.1 Very unequal access to French

Our overview of websites when searching for tools and information about them leads us to an initial observation: There are far fewer tools available for unilingual French-speaking Internet users. Several tools are presented exclusively in English – the private browser Epic

---

[428] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. "PETs controls matrix – A systematic approach for assessing online and mobile privacy tools," December 20, 2016, pp. 17 and 23-24, online: https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-controls-matrix-a-systematic-approach-for-assessing-online-and-mobile-privacy-tools; EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. "PETs control matrix," Annex 1, online: https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-control-matrix-annex-1-assessment-questionnaires (consulted on January 15, 2020).

[429] GRAF, C. *et al*, eds., "Towards Usable Privacy Enhancing Technologies: Lessons Learned from the PrimeLife Project," PrimeLife HCI, June 17, 2011, section 2.1.1.1.1, online: http://primelife.ercim.eu/images/stories/deliverables/d4.1.6-towards_usable_pets-public.pdf

[430] GOVERNMENT OF CANADA. "Successful Communication. Tool Kit, Literacy and You," May 2003, sections 1 and 5, online: https://publications.gc.ca/collections/Collection/PF4-16-2003E.pdf

and the tracking blocker Privacy Badger, for example – and others often have only partially bilingual websites. Unfortunately, the help sections on the secondary pages of those websites (pages that contain tutorials, FAQs, etc.) usually escape translation. This is information the consumer would have needed. It's on those pages that we most often find explanations that complement the catchy but vague phrases written on some providers' home pages. Many of the blogs provided on the tools' websites are also unilingual. The blogs are generally not directly related to the tool offered, but teach Internet users about issues that affect their online privacy (risks, legislative developments, etc.).

It should be kept in mind that a little less than a quarter of the Canadian population has French as its first language[431]. And a significant number don't know English. This is the case for nearly 60% of Quebecers. It is regrettable to see this language barrier in the introduction to online privacy enhancing technologies, especially since the results of our survey tend to demonstrate a generally lower level of knowledge of the tools among Francophone respondents.

With the exception of cookie and browser history blockers or erasers, all the other tools presented in the survey are less familiar to Francophone respondents than to Anglophone respondents. The difference is 10% on average.

4.1.1.2 Occasionally complex wording, despite undeniable efforts

Beyond the languages in which the information is disseminated, the complexity of the terms used varies greatly depending on the providers and the tools studied.

Some tool providers clearly pay special attention to the clarity of the information conveyed. They present the information with explanatory tables, visual aids or examples. They attempt to define the more technical terms used in the online documentation, by including, for example, a hyperlink to another page of the website or to an external resource (e.g., media article) or by means of a modal window the consumer can click on for a definition or explanation of the term in bold or underlined characters.

The number of defined terms varies considerably from one provider to another; however, private search engines and antivirus software stand out by the simplicity of their wording. Other providers' choice of defined terms, if any, is sometimes perplexing. Yopmail, a provider of disposable email addresses, for example, defines what "spam" is, but not what "search plugins" or "widgets" that the Internet user could download are. We would think that the opposite would have been more useful to the average consumer, who is probably aware of the spam phenomenon, but less comfortable with the more technical elements of his browser.

---

[431] GOVERNMENT OF CANADA. "Statistics on official languages in Canada," online: https://www.canada.ca/en/canadian-heritage/services/official-languages-bilingualism/publications/statistics.html (consulted on March 14, 2021).

4.1.1.3 A variety of support resources

The efforts of some providers to provide clear and simple information about online tools and privacy are also reflected in the variety of help and information services available to users. Automated chat services, newsletters, discussion forums, podcasts, shows[432], etc.: Providers are creative in disseminating information. This is particularly true for providers of services for which the consumer will generally have to pay (antivirus, VPN and password managers).

Table 16
The types of support resources available from providers
by type of online privacy enhancing tools offered

Types of online privacy enhancing tools	Types of support and information resources available on the websites studied				
	Frequently asked questions	Virtual assistant or individual help service	Forum or community	Blog	Newsletter
Antivirus	✓✓✓	✓✓	✓✓✓	✓✓✓	✓✓✓
Virtual private networks (VPN)	✓✓✓	✓✓✓	✓	✓✓✓	✓
Password managers	✓	✓✓	✓✓	✓✓✓	✓✓
Private browsers	✓✓✓		✓✓	✓✓✓	✓
Private search engines	✓✓		✓	✓✓✓	✓✓
Ad and tracking blockers	✓✓✓		✓	✓✓	
Disposable email addresses	✓			✓	

* A total of 21 providers' websites were reviewed, three for each type of online privacy enhancing tool selected.

It should be noted, however, that in some cases those services were difficult to find on the websites. Similarly, the table does not distinguish between the quality and quantity of information available on the blogs and FAQs. Some blogs, for example, contain more than 100 posts, while others contain only a few useful links. The same is true for the FAQs on the websites studied; some cover very few aspects (installation or privacy policy, for example).

[432] See for example: MCAFEE. "Hackable? Podcast," online: https://hackablepodcast.com/episodes; AVAST. "Garry on lockdown, online: https://blog.avast.com/garry-on-lockdown-episode-1-avast

4.1.1.4 Some inconsistency

On a less positive note, we're disappointed that the collection and use of Internet users' personal information on the tools' websites are widespread. Many, for example, display browser cookie notices with non-essential cookies pre-checked for approval. Ironically, this is especially true of Adblock Plus, an online tracking blocker! While this practice is not necessarily prohibited in Canada (unlike in the European Union[433]), it still seems difficult to reconcile with the tools' mission to improve their users' online privacy protection. The privacy policies of some websites also raise eyebrows.

4.2 Private Search Engines

To study the presentation of private search engines, we selected the three major providers DuckDuckGo, StartPage and Qwant[434]. Note that DuckDuckGo is undoubtedly the most popular private search engine. In 2019, it performed 50 million searches every day[435]. It is now one of the search engines available by default on the Chrome browser[436]. Qwant, meanwhile, has received a serious boost from the French government; since 2019, it has been the default search engine on all government employees' devices[437].

4.2.1 Presentation of usefulness

Two of the three search engines studied provided information about the tool's privacy benefits directly on their home Web page, below the search box.

Take the example of the DuckDuckGo website's home page, which states:

> Your data should not be sold.
> [...] No tracking, no ad targeting, just search.

It clearly and simply mentions the risks avoided, namely the sale of information to third parties, profiling and exposure to behavioural advertising. There are also several references

---

433 LOMAS, N. "Europe's top court says active consent is needed for tracking cookies," Techcrunch, October 1, 2019, online: https://techcrunch.com/2019/10/01/europes-top-court-says-active-consent-is-needed-for-tracking-cookies/
434 STEWART, C. "The Best Private Search Engines - Alternatives to Google," Hackernoon, February 8, 2018, online: https://hackernoon.com/untraceable-search-engines-alternatives-to-google-811b09d5a873
435 DUCKDUCKGO. Posted on Twitter, November 06, 2019, online: https://twitter.com/DuckDuckGo/status/1192079712379494406
436 ZHOU, M. "DuckDuckGo is now a default search engine option in Chrome," CNET, March 14, 2019, online: https://www.cnet.com/news/duckduckgo-is-now-a-default-search-engine-option-in-chrome/; LOMAS, N. "Google has quietly added DuckDuckGo as a search engine option for Chrome users in ~60 markets," Techcrunch, March 13, 2019, online: https://techcrunch.com/2019/03/13/google-has-quietly-added-duckduckgo-as-a-search-engine-option-for-chrome-users-in-60-markets/
437 "France is bidding adieu to Google in favor of a more private search engine," ExpressVPN, August 7, 2019, online: https://www.expressvpn.com/blog/google-france-qwant-privacy/

to search history, i.e. the personal information that the tool protects. By consulting – even briefly – the provider's website, a user would easily find answers to the *who*, *what* and *why* questions.

Qwant is in a class of its own by not offering any details on its home page about the usefulness of its service. Only the slogan "The search engine that respects your privacy" appears under the search engine's logo. In order to find out what the tool actually does for privacy, a user will have to click on the relatively inconspicuous "About" heading on the right-hand corner of the page next to the music and geographic search services. Even on its "About" page, there is relatively little information about the usefulness of Qwant or, more generally, of a private search engine.

It's unfortunate that an Internet user has to click on two other links[438] in order to access a real explanation of the risks of "commercial" search engines for his online privacy. Qwant's excellent explanation, which he is unlikely to read, would have deserved a much higher profile:

> You tell your search engine everything about yourself, when you ask it questions every day: where you want to go, what you want to cook, the symptoms or treatments of your eventual illness, your sexuality, your religion, your investment plans, your income level, your profession, your favorite sports, the movies you are going to see… the list of intimate and commercially exploitable questions is endless, and often these searches are stored, analyzed, and sold directly or indirectly.
>
> […you can use Qwant with confidence, we will never attempt to build a psychological or commercial profile of you for resale to advertisers, here or elsewhere.

We also note with interest the StartPage website's warning about the limits of a private search engine for online privacy protection. On the home page of the provider's website, the following warning is found:

> By clicking on the search results, you leave the protection of Startpage.com, which results in a barrage of cookies being installed on your device.

While this warning is primarily intended to direct consumers to Startpage's other service, its "anonymous browsing mode," this important clarification highlighted by the provider is commendable. Consumers should be informed about the tool's limitations and not mistakenly believe that there is no longer any risk of tracking and profiling or exposure to behavioural advertising when browsing online. In the absence of explanations on the subject, the catchy phrases of the providers studied could mislead some: "no tracking, no ad targeting," "a search engine […] that respects users' rights and freedoms," etc.

[438] After accessing the "About" page of the Qwant website, the user will have to click on the title "Help Center" and finally on the title "Our philosophy" at the bottom of that page.

4.2.2 Presentation of usage

Few Canadian Internet users have never used Google, Yahoo or another search engine. Therefore, explanations of the basic features of this type of tool are less necessary.

The only obvious reference to how the search engine works is on the home page of the StartPage website, which mentions using Google's search results, for a fee, and removing all "trackers" from the search results before passing them on to its own users.

4.3 Virtual private networks

In order to study the presentation that virtual private networks make, we selected the following three providers: NordVPN, ExpressVPN and Hide.me. Commonly named among the most popular providers[439], NordVPN and ExpressVPN offer a paid service, ranging from US$8 to US$13 per month depending on the package, while Hide.me offers a free version of the service (2GB download limit) in addition to its paid version.

4.3.1 Presentation of usefulness

In general, we find that two purposes are put forward by the providers on the home page of their respective websites: protection of personal information online and circumvention of geoblocking (i.e. regional restrictions on access to certain content).

ExpressVPN puts more emphasis on circumventing censorship and content restrictions than its competitors. In fact, the provider doesn't even specifically mention data protection in the description of the tool's basic features that appears on the Web page dedicated to this topic. It mentions anonymous browsing and IP address masking, but never explains how these processes help protect online privacy. Consumers can find the answer to this question on another page dedicated entirely to privacy issues. It's unfortunate that the information has been split up in this way.

More easily understood by the average Internet user, Hide.me addresses IP address anonymization by directly describing the vulnerability that the tool aims to fix. The user is presented with his IP address, followed by the following statements:

> If we can see your true identity and location, everyone can see it too.

---

[439] GROM, E. "The Popularity Of VPNs Is On The Rise," VPNBase, April 9, 2019, online: https://vpnbase.com/blog/popularity-of-vpns-is-on-rise/; SIMMONS, J. H. "Most Downloaded VPN Apps for Android (Big List Inside!)," VPNCrew, data as of January 15, 2019, online: https://www.vpncrew.com/most-downloaded-vpn-apps-for-android/; RIVINGTON, J. "The Best VPN Service 2019," Tom's Guide, October 2, 2019, online: https://www.tomsguide.com/best-picks/best-vpn; LAUKKONEN, J. "The 8 Best Free VPN Services of 2019," Lifewire, October 23, 2019, online: https://www.lifewire.com/best-free-vpn-services-818192

> You are being monitored. Without a VPN, the sites you visit have access to your real IP and location. Your ISP [Internet Service Provider] knows what sites you visit, who you email, and what you download. Not only is your online activity tracked, but it is tracked under your name.

In contrast to the other tools studied, VPN providers focus on the privacy risks posed by the ISPs themselves. In addition to browsing activity information stored and sometimes sold by ISPs, their lack of transparency and copyright obligations are highlighted. Hide.me, for example, accompanies its tool's presentation with a table listing the laws of a few countries, including Canada, regarding the retention of activity logs by Internet service providers.

4.3.2 Presentation of usage

The operation of virtual private networks is technically more complex than that of many of the other tools studied. The clarity of the explanations provided is therefore all the more important.

Each provider has a website section dedicated to explaining what a virtual private network is and to popularizing complex concepts such as encryption and the VPN protocol. They all use the image of a tunnel and use illustrations that build on this analogy.

But despite undeniable efforts to simplify the explanations, the presentations of the operation of this type of tool remain a bit technical and the content is complex. And it's unlikely that the average Internet user will understand all the subtleties. NordVPN's explanation is the most complete, but also the least easily understood:

> When you connect to a VPN service, it creates an encrypted "tunnel" across the Internet. This secures the data flowing between you and your destination, whether it's a search engine or an online bank account.
>
> This tunnel is created by first authenticating your client to a VPN server. The server then applies an encryption protocol to all data you send and receive.
>
> To ensure the security of each data packet, a VPN wraps it in an external packet, which is then encrypted by encapsulation. It protects the data during transfer and is the core element of the VPN tunnel. When the data arrives at the server, the outer packet is removed via a decryption process.

Figure 1
ExpressVPN's schematic illustration of how a virtual private network works

https://www.expressvpn.com/what-is-vpn

Two providers also present videos that both promote their products and explain how they work[440]. The websites studied also present usage diagrams in three steps, which roughly consist of installing the application, activating the protection and choosing a particular server, if desired. The explanations on how an Internet user can use the tool are particularly well done, although simpler.

A visitor to a VPN provider's website should therefore come away from the experience with a modest general understanding of how the tool works, but a good idea of how the tool can be used and who and what it protects.

[440] ExpressVPN also has a YouTube channel that contains several popular videos: https://www.youtube.com/channel/UCFzUH6rnGYqJD6EexQSdVhw (visited on March 2, 2021).

4.4 Private Browsers

We chose to study the three free private browsers Tor, Brave and Epic because of their popularity and distinct approach to anonymization.

4.4.1 Presentation of usefulness

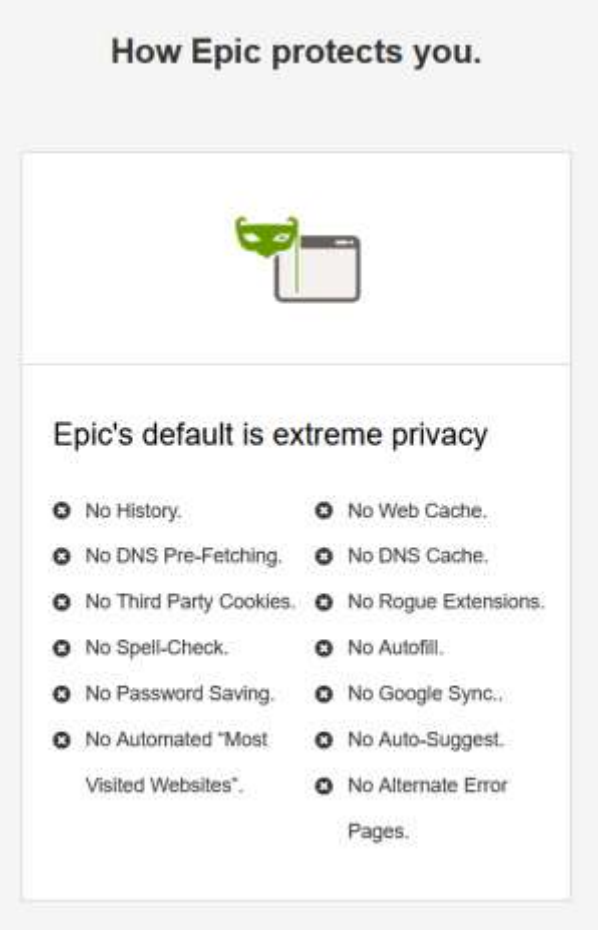
Within this category of tools, the consumer experience varies greatly from website to website. Tor's and Epic's presentations, for example, focus on online privacy, while Brave's tempers that goal with other considerations such as browsing speed.

For example, Brave's home page does not put a particular emphasis on privacy. There are catchy phrases such as "a better Internet" and a "reimagining" of the Web browser. In trying to present its product as an improved version of traditional browsers, Brave relegates privacy to the back burner, alongside speed and security, and nothing more.

In order to obtain an explanation of the tool's added value in terms of online privacy, the consumer must go to a secondary page that details the tool's features. But again, those explanations are found under those related to download speed and the *Brave Rewards* loyalty program. There is a very complete, if somewhat technical, list of the tool's features, which mentions the following, among others: *fingerprint prevention, cookie control, HTTPS upgrade, erasing browsing data, private windows*, etc. The features mentioned are not accompanied by explanations or definitions, which makes them quite difficult to understand. It's unrealistic to think the average consumer knows what script blocking or global shield configuration is!

Epic's website has a similar problem, although it places more emphasis on online privacy on its home page. The examples on the home page are not defined (e.g., *fingerprinting, ultrasound signaling,* etc.). The Web page that specifically addresses the tool's features provides more detail, but unfortunately no further explanation, as the following excerpt shows:

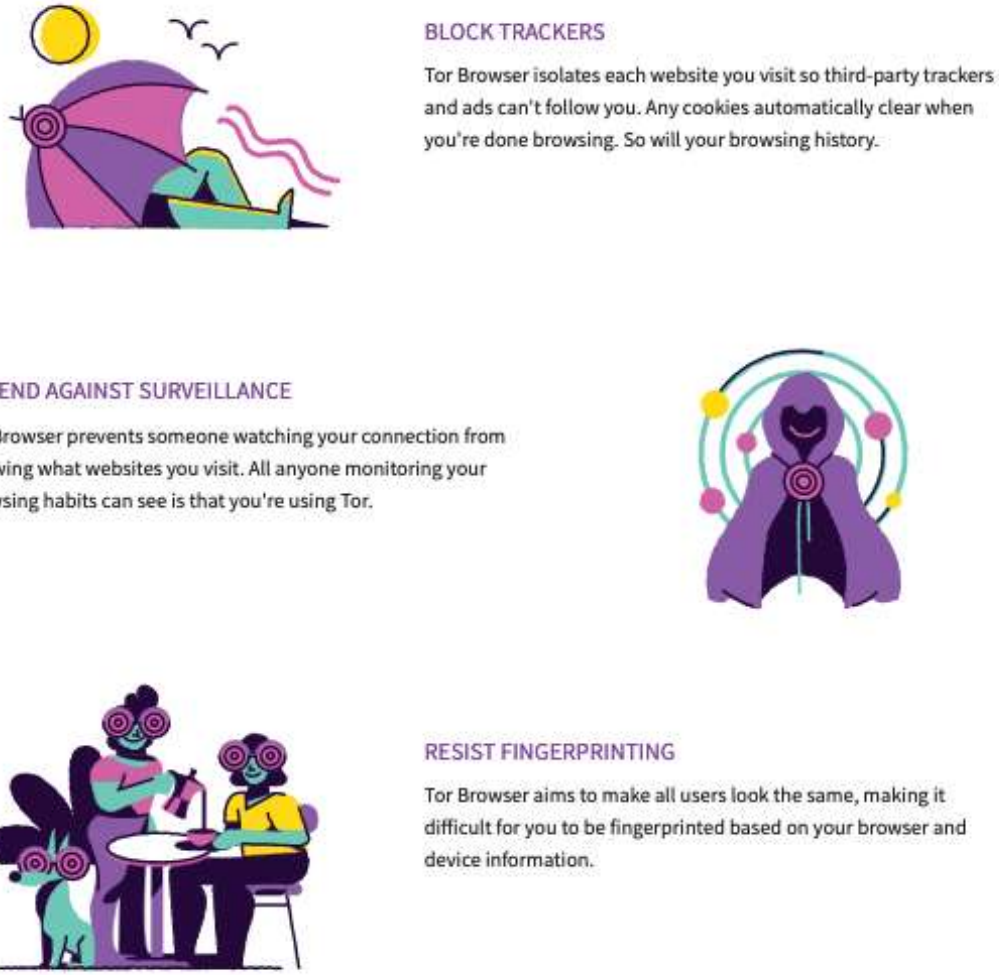
Figure 2
Excerpt from an Epic website page about the tool's features



Source: https://www.epicbrowser.com/our-key-features.html

The Tor private browser's Web page differs from the others studied in that the reader has access to relatively simple explanations of the tool's usefulness in protecting personal information, right on the home page. Under the catchy phrase "Defend yourself against tracking and surveillance," there are short paragraphs that address various key elements of the protection offered by the tool, all accompanied by playful images.

Figure 3
Excerpt from the Tor website's home page



Source: https://www.torproject.org/

A tech-savvy consumer who is disappointed by the lack of detail at first glance can turn to other sections of the Tor website, which offers an impressive amount of explanations, hyperlinks, and other useful resources.

The Epic home page also points out the risks of online tracking that remain when a virtual private network is used or the incognito browsing mode is activated on traditional browsers. While this warning is primarily aimed at converting users to using its tool, it's interesting to see this type of warning so visibly communicated to consumers, who often don't fully discern the usefulness (and limitations) of different privacy enhancing technologies.

4.4.2 Presentation of usage

The observed browsers' websites are not very descriptive about the basic features of their products, which is justified by Internet users' familiarity with using a browser, an essential component in any online navigation…

4.5 Ad Blockers and Online Tracking

We chose three of the most popular ad blockers, Adblock Plus, Privacy Badger and Ghostery. All of them come in the form of a browser extension and are available at least for the Firefox, Chrome and Opera browsers.

4.5.1 Presentation of usefulness

From the outset, we see that Adblock Plus puts very little emphasis on online privacy on its website. That's because it's primarily an ad blocking tool, whose online tracking blocking features appear secondary. We assume that, like many Canadians surveyed in our study, the tool's creators see personalized online advertising as more of an inconvenience than an invasion of privacy.

Adblock Plus thus explicitly emphasizes the annoying nature of ads and their effect on users' browsing speed (who are promised a cleaner, faster Web experience). The references to tracking blocking, which are only found on the "About" page, would have deserved a little more visibility, including this remark about the relevance of blocking online ads to privacy protection:

> Many ads have built-in tracking devices and some may even contain malware.

Online privacy is more of a focus for the other two providers. There is a mention of blocking tracking devices on the home page of both tools.

The fuller explanation of how Privacy Badger works is particularly easy to grasp for the less digitally savvy:

> When you view a webpage, that page will often be made up of content from many different sources. (For example, a news webpage might load the actual article from the news company, ads from an ad company, and the comments section from a different company that's been contracted out to provide that service.) Privacy Badger keeps track of all of this. If as you browse the web, the same source seems to be tracking your browser across different websites, then Privacy Badger springs into action, telling your browser not to load any more content from that source. And when your browser stops loading content from a source, that source can no longer track you. That's it!

Unlike the other two tools studied, Privacy Badger makes no mention of other considerations, such as browsing speed or the visual aspect of ad-filled Web pages. The

only purpose mentioned is to protect online privacy. It also distinguishes the tool from a simple ad blocker:

> Because Privacy Badger is primarily a privacy tool, not an ad blocker. Our aim is not to block ads, but to prevent non-consensual invasions of people's privacy because we believe they are inherently objectionable. We also want to create incentives for advertising companies to do the right thing.

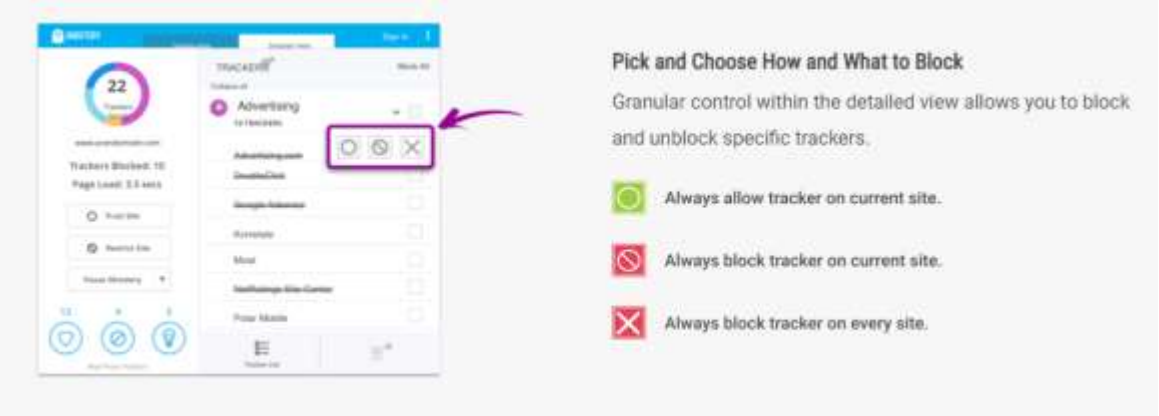
The absence of those "selling points" may be explained by the non-profit nature of the tool's developer, the Electronic Frontier Foundation. The organization's mission also explains the very educational aspect of the Privacy Badger website, which presents, on its home page, a long series of questions and answers about how the tool works and how it protects personal information online: "Does Privacy Badger prevent fingerprinting?"; "Does Privacy Badger still work when blocking third-party cookies in the browser?"; "Why does Privacy Badger block ads?"; etc. The explanations provided are simple and easy to understand for a non-technical Internet user, especially because the more technical elements are all defined and often even accompanied by hyperlinks for additional explanations.

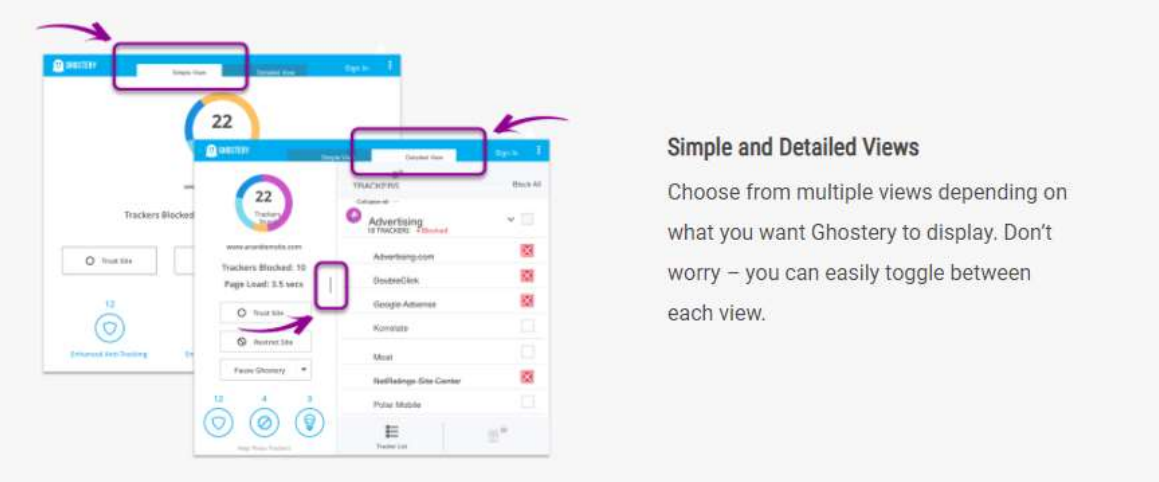
4.5.2 Presentation of usage

With the exception of Privacy Badger, the websites of the tools studied explain their usage in a simple way, with useful visual aids. The help section of the Adblock Plus website, for example, contains several illustrated tutorials that adapt to the browser used (by recognizing the browser used)[441]. The presentation of how Ghostery works is more minimal, but still clear, with a secondary Web page that includes a carousel of images representing the use of five features of the tool[442].

[441] ADBLOCK PLUS. Online: https://help.eyeo.com/fr/adblockplus/ (consulted on March 12, 2021).
[442] GHOSTERY. Online: https://www.ghostery.com/ghostery-browser-extension/ (consulted on March 15, 2021).

Figure 4
Excerpts from a Ghostery website page about the tool's features





Source: https://www.ghostery.com/ghostery-browser-extension/

The usage presentations of Adblock Plus and Ghostery put a lot of emphasis on the control that users will be able to exercise; for example, the presentations underline the multiplicity of possible settings. However, there are few explanations for Internet users as to the elements to take into account in this choice. A consumer looking for an ad blocker is likely to wonder why he should filter one tracker rather than another. And he may ultimately make choices that don't promote optimal online privacy, due to lack of knowledge and support.

Unfortunately, Privacy Badger, which stood out for its presentation of the tool's usefulness, is rather disappointing when it comes to the presentation of its usage. All the information is available, but the presentation is surprisingly unattractive for a provider that makes an undeniable effort to help the reader understand. And the user will have to go through a long list of Questions and Answers in order to understand how the tool works, since no section of the website is specifically dedicated to that.

There is also the particular situation in which Adblock Plus finds itself: The tool provides a list of "acceptable ads" that it does not block outright. This practice has been the subject of several criticisms and controversies, especially because advertisers sometimes pay to have their ads added to this "white list" of ads that will continue to be presented to the user despite the ad blocker's activation[443].

Insofar as many of the Canadian Internet users surveyed had doubts about the business model of the free tools offered and, incidentally, about the extent of the protection actually offered by TAQs, it's interesting how Adblock Plus explains the operation of its acceptable ads program, which very likely feeds that skepticism. Statements to the effect that "not all ads are bad" and that "websites need money to stay free" are present on the website's home page, with no additional details other than a hyperlink to a page that explains how to opt out of ads accepted by the tool. From that last page only, an Internet user will eventually be able to access explanations of the criteria for analyzing ads and on the tool's funding by the acceptable advertising program.

4.6 Antivirus Software

Among the most popular antivirus providers[444], we have chosen to study the presentations made by Avast, McAfee and Eset on their respective websites.

The websites visited are generally larger than those of other (usually free) tool categories, possibly because the price of the services offered can reach $240/year. All offer a range of products with various features and levels of functionality. We therefore focused our observations on each company's flagship product for individual Canadian customers, namely "Avast Free Antivirus," "McAfee Total Protection" and "Eset Internet Security."

4.6.1 Presentation of usefulness

The websites of the surveyed antivirus products are straightforward in terms of their main functions. The consumer quickly gets a good idea of the threats they aim to protect against. Protection against hackers, detection of threats such as viruses, malware and spyware, analysis of unknown files, etc.: Those functions are clearly visible on the home page of the various providers studied.

Other Web pages detail the coverage offered (and the threats addressed) by each service, usually in table form. The presentations are very complete and intelligible; undeniably, the

---

[443] MAHESHWARIA, S. "Adblock Plus, Created to Protect Users From Ads, Instead Opens the Door," New York Times, September 18, 2016, online: https://www.nytimes.com/2016/09/19/business/media/adblock-plus-created-to-protect-users-from-ads-opens-the-door.html

[444] OPSWAT. "Windows Anti-malware Market Share Report," online: https://metadefender.opswat.com/reports/anti-malware-market-share# (consulted on March 10, 2021).

providers have paid special attention to the language used. This is particularly true of McAfee, which offers the following description of a computer virus, for example:

> A computer virus is code that, once executed, is designed to enter a computer and replicate itself. Viruses designed to damage a computer are classified as a type of "malware". The harmful purposes of different types of malware are very diverse. For example, they can take the following forms:
>
> 1 Ransomware, which encrypts your sensitive files, photos and documents as well as your computer, and forces you to make a payment (often through bitcoins) in exchange for a password that allows you to decrypt and unlock these files
> 2 Trojans, which allow a hacker to take complete control of your computer and run programs as if they were actually using your keyboard and mouse
> 3 Spyware, which "extracts" personal information from your computer and sells it to the highest bidder
> 4 Adware, which generates unwanted pop-ups from questionable advertisers

It's also worth noting that this provider chooses to present, on its home page, statistics on the threats discovered and dealt with every day ("480 threats discovered every minute"). Even if this type of presentation is primarily aimed at selling a product, we still find it helps less informed Internet users become aware of the online risk to the security and confidentiality of their personal information.

4.6.2 Presentation of usage

Each provider studied provides a help portal with extensive documentation and sections dedicated to product installation and activation. Little product usage information is integrated into the main websites.

Perhaps because of the complexity and variety of possible features, there are no illustrations of the interfaces on the websites, unlike what we have seen for other types of tools, to explain the features' operation. However, in the providers' website sections, there are clear instructions, occasionally accompanied by visual support, on how to download, install or activate the tools.

Figure 5
Excerpts from the Eset website page on installing the antivirus software

Source : https://support.eset.com/en/kb3640-install-and-activate-eset-file-security-for-microsoft-windows-server-6x

4.7 Disposable Email Addresses

Based on our research, there are no publicly available data on the popularity of different disposable or temporary email address providers. So we simply selected three providers for this study that are regularly mentioned in the lists available online about this type of privacy tool[445]. The providers selected are Tempmail, Mohmal and YOPmail.

4.7.1 Presentation of usefulness

In general, websites for this type of tools are fairly sparse in terms of information. Tempmail stands out by its website, which includes a blog and a question and answer section.

A visitor to Mohmal's website, for example, should already know what disposable email addresses are, since the home page contains only a rather inconspicuous mention of email messages.

In contrast, the Tempmail website offers a fairly comprehensive presentation of the tool's usefulness:

[445] "10 Free Temporary Disposable Email Services To Fight Spam," GeckoandFly, June 9, 2019, online: https://www.geckoandfly.com/7782/how-to-create-temporary-email-and-gmail-forwarding-service/; "10 Best Disposable Email Services for a Temporary Email Address," MashTips, April 15, 2018, online: https://mashtips.com/disposable-email-services/; "Best Free Disposable Email Address Services," Technogadge, April 4, 2016, online: http://www.technogadge.com/best-free-temporary-email-providers/

> Forget about spam, advertising mailings, hacking and attacking robots[446], Temp Mail provides temporary, secure, anonymous, free, disposable email address[447].

A little further down, a section entitled "What is a temporary disposable email?" mentions the most common use – providing an email address to register on a website and access content, send comments or download. Another of the provider's Web pages notes that online store databases are sometimes hacked, resulting in their users' email addresses ending up on spam lists[448].

The provider also attempts to dispel some myths, including that the use of online privacy-enhancing technologies is "immoral" – not unlike the "I have nothing to hide" comments of some interview respondents:

> Technically, the idea of a temporary email address conjures up with black hat hackers and underworld Internet, but there are convincing reasons to use fake email services[449].

While many Canadians surveyed raised this concern, unfortunately none of the websites we visited addressed the issue of potential blocking of disposable email addresses by various Web services.

4.7.2 Presentation of usage

Unlike other tools studied, disposable email addresses can be used directly from the provider's website. There is no need to explain the installation procedure or to discuss compatibility with different browsers or operating systems.

YOPmail's operation is clearly explained on the home page and on the short FAQ page.

> Do I need to create an account to use YopMail?
> No! Nothing to do! All the accounts already exist, but none of them really belong to you. Just send an email to any address on YopMail and check the corresponding box.
>
> How to access an inbox?
> On the home page, you enter any account name in the input field provided. For example, to access the account "nimportekoi@yopmail.com" you enter "nimportekoi".

The other two providers are less descriptive about how to use the tool, but they have the advantage of a relatively intuitive interface and simpler usage (e.g., randomly assigning an email address).

---

[446] No additional information is available about "robot attacks."
[447] TEMPMAIL. Online: https://temp-mail.org/en/
[448] TEMPMAIL. "The tech behind Disposable Email Addresses," June 7, 2021, online: https://temp-mail.org/blog/the-tech-behind-disposable-email-addresses/
[449] *Ibid.*

4.8 Password Managers

According to ISE data, 1Password, Dashlane and LastPass are the 1st, 2nd and 4th most popular password managers, respectively[450]. The third-most popular provider, Keepass, was not included in this study because its website is exclusively in English. The three providers selected offer packages at prices ranging from US$36 to US$60 per year. Dashlane also offers a free option that includes storage for up to 50 accounts.

4.8.1 Presentation of usefulness

In general, the presentation of password managers focuses on ease of use and simplifying the online experience by supporting password storage and automatic password entry.

> Go ahead, forget your passwords - 1Password remembers them all for you. [1Password]

Explanations about privacy are present (especially in terms of computer security), but give way to practical aspects. Privacy protection is addressed more fully on secondary pages.

Data leakage and theft, especially due to insecure passwords, are the main threats that password manager providers refer to on their websites, and those threats are highlighted on every website visited. Based on a report from Verizon[451], LastPass states, for example:

> Passwords are a real security issue. According to a recent report, over 80% of hacking-related security leaks are due to weak or stolen passwords.

There are also several references to some large companies' data leaks that have resulted in millions of people having their logins and passwords compromised. A page on the 1Password website titled "security" lists different types of security breaches involving, for example, phishing and unauthorized keyloggers.

Compared to its competitors, Dashlane gives more space to security on its home page, which is titled "The more random your password, the stronger your security." The website takes an interactive approach to presenting its purpose: A section titled "Why did you choose Dashlane?" asks the user to answer a few questions to demonstrate the tool's value. Regardless of the answers, the consumer is of course taken to a page that recommends downloading the tool; this questionnaire nevertheless forces the consumer to reflect on his fears and needs regarding the protection of his privacy online, which is desirable.

---

[450] ISE. "Password Managers: Under the Hood of Secrets Management," February 19, 2019, online: https://www.ise.io/casestudies/password-manager-hacking/; FOWLER, G. A. "Password managers have a security flaw. But you should still use one," Washington Post, February 19, 2019, online: https://www.washingtonpost.com/technology/2019/02/19/password-managers-have-security-flaw-you-should-still-use-one/

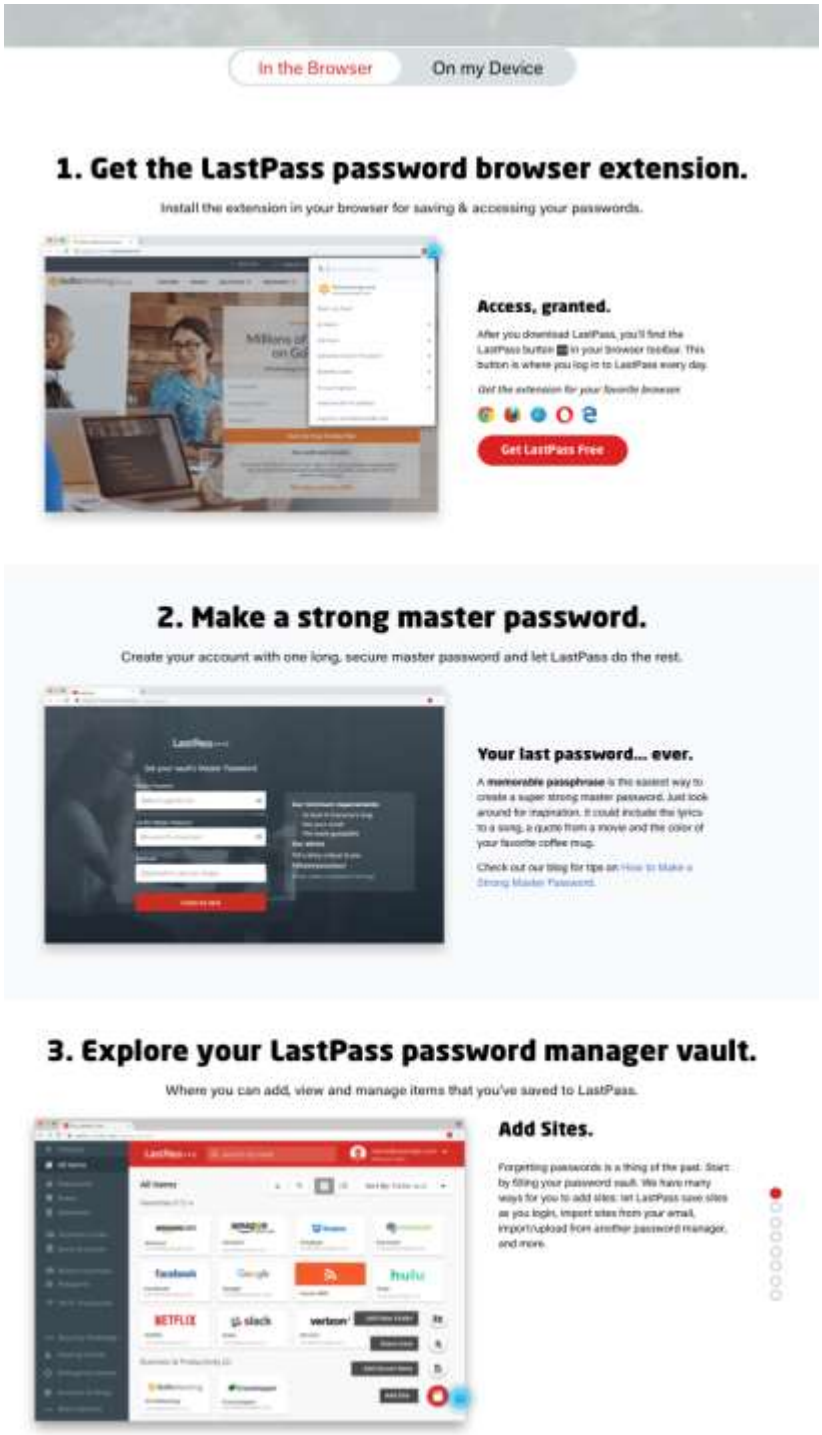
[451] VERIZON. "2021 Data Breach Investigations Report," online: https://enterprise.verizon.com/resources/reports/dbir/

Lastly, the providers all address a common fear among consumers, namely the risk that the service itself will be hacked. The providers all clearly explain that they don't have access to their customers' data, which is encrypted with a master password specific to each user.

4.8.2 Presentation of usage

The websites of the three providers studied clearly explain the usage of the password managers offered. Ease of use is one of the main selling points. The websites provide screenshots of the tool to explain how it works and its benefits. For example, the "How it works" page on the LastPass website, which can be accessed directly from the main navigation menu, shows the following steps:

Figure 6
Excerpt from a page on the LastPass website regarding the tool's installation



Source: https://www.lastpass.com/how-lastpass-works

All three providers discuss the encryption processes used, presumably to reinforce their selling point about the security of the tools offered. However, the evidence is so technical that it is unlikely to help the average Internet user. LastPass, for example, points out that it implements "256-bit AES encryption with SHA-256 PBKDF2 and salted hashes to ensure complete security in the cloud[452]." Very reassuring.

Dashlane at least specifies that AES 256-bit encryption is "the most secure method available today[453]." In the absence of this information, the consumer is unfortunately faced with a series of symbols and numbers with no particular meaning!

Other sections of the password manager providers' websites are also clearly dedicated to a more technophile audience. For example, there is an 80+ page document that describes 1Password's approach to computer security[454].

[452] LASTPASS. Online: https://www.lastpass.com/how-lastpass-works (consulted on April 15, 2021).
[453] DASHLANE. Online: https://www.lastpass.com/how-lastpass-works (consulted on April 15, 2021).
[454] 1PASSWORD. Online: https://1password.com/security/ (consulted on April 15, 2021).

IS CANADIAN LEGISLATION IN LINE WITH THE CONSUMER PERSPECTIVE?

5.1. Overview of the Applicable Canadian Federal and Provincial Framework

Canada's legal framework for privacy protection consists of legislation enacted by the federal Parliament and by some provincial jurisdictions. The federal Parliament's powers in this area derive from its jurisdiction over traffic and commerce[455], while those of the provincial legislatures derive from their jurisdiction over property and civil rights and matters of a purely local or private nature[456].

With respect to privacy protection in the private sector, the federal government exercised its authority by adopting *PIPEDA*[457] in April 2000. Three provinces have chosen to do the same: Quebec with the adoption of *APPIPS*[458] in June 1993 (and the inclusion of certain privacy provisions in the *Civil Code*[459] and the *Charter of Human Rights and Freedoms*[460]), Alberta with the adoption of *APIPA*[461] in 2003 and British Columbia with the adoption of *BCPIPA*[462] in 2003. Manitoba also passed legislation in this area, the *Personal Information Protection and Identity Theft Prevention Act* (*PIPITPA*)[463] in 2014, but never brought it into force. Ontario conducted a consultation in fall 2020 to develop its own provincial legislation on the subject[464], but no bill has yet been introduced in the Ontario legislature. Several provinces have legislation that specifically addresses the handling of personal information in the health care sector. We will not address those specific statutes in this report.

---

[455] CANADA. Constitution Act, 1867, 30 & 31 Victoria, c 3, s. 91(2).
[456] *Ibid.*, arts. 92(13) and (16).
[457] PIPEDA, *supra* note 77.
[458] APPIPS, *supra* note 78.
[459] QUEBEC. Civil Code of Québec, RSQ c CCQ-1991.
[460] QUEBEC. Charter of Human Rights and Freedoms, *supra* note 79.
[461] APIPA, *supra* note 78.
[462] BCPIPA, *supra* note 78.
[463] MANITOBA. The Personal Information Protection and Identity Theft Prevention Act, CCSM c P33.7.
[464] GOVERNMENT OF ONTARIO. "Ontario's Regulatory Registry, Public Consultation – Modernizing Privacy in Ontario," 2021, online: https://www.ontariocanada.com/registry/view.do?language=en&postingId=37468 (consulted on June 10, 2021).

5.1.1.The federal Act: a document with complex origins

PIPEDA is largely modelled on a self-regulatory initiative developed by industry in the mid-1990s[465]. The resulting legislation has a surprising structure: Many company obligations are found in Schedule 1 of the Act, in the form of principles, rather than in the sections that make up the body of the Act.

The legislation's surprising form and sometimes unclear content can be explained, according to Justice Décary of the Federal Court of Appeal, by the provisions' particular history:

> The PIPED *Act* is also a compromise as to form, as is amply demonstrated by the recital of its historical background. Schedule 1 is an exact replica of Part 4 of the CSA Standard adopted in 1995, which Standard in turn was based on the OECD Guidelines adopted in 1980 and to which Canada had adhered in 1984. Both the CSA Standard and the OECD Guidelines are the product of intense negotiations between competing interests, which proceeded on the basis of self-regulation and which did not use nor purport to use legal drafting[466].

Those repeated attempts to reconcile competing interests have resulted in a law whose objectives and approaches sometimes appear contradictory and that ultimately proves fundamentally unsatisfactory. *PIPEDA has* been amended a few times since 2000, with the addition in 2018, for example, of a duty to notify individuals following a confidentiality incident, but has not been subject to any major reform or substantive rewrite since its adoption.

The federal legislation also includes (as its name suggests) a series of provisions relating to electronic documentation, whose linkage to privacy appears weak at best. This will further confuse consumers and even lawyers trying to clearly understand the applicable legal framework!

5.1.2. Similar but distinct provincial laws

In principle, federal law applies to the entire private sector in Canada. But how does federal law coexist with existing provincial laws?

In practice, an organization will only be subject to one of the laws at a time, depending on where it operates and what activity it carries out. *PIPEDA* provides for the possibility of excluding from the Act's application certain organizations, activities or classes of activities where they are subject to a "substantially similar" provincial law[467]. This qualification, which is made by the Governor in Council by way of an order in council, may apply to the entire Act or to certain aspects only (for example, the processing of personal health information).

---

[465] LEVIN. "Privacy Law in the United States," *supra* note 64, p. 380.
[466] *Englander* v *Telus Communications Inc.*, 2004 FCA 387, para. 43.
[467] PIPEDA, *supra* note 77, s. 26.

The provincial laws for the protection of personal information in force in Canada have all been found to be sufficiently similar to the federal law.

For example, in Quebec, Alberta and British Columbia, private businesses are subject to provincial law, except in the case of federally regulated businesses (banking, telecommunications, aviation, etc.) or commercial activities that require the transfer of personal information across provincial boundaries[468].

Table 15
The application of Canadian laws for the protection of personal information in the private sector, by province

<table>
<tr><td rowspan="2">Location</td><td colspan="2">Applicable laws depending on the status of the company handling the personal information</td></tr>
<tr><td>Businesses under provincial jurisdiction</td><td>Businesses under federal jurisdiction</td></tr>
<tr><td>Alberta</td><td>Alberta Personal Information Protection Act (APIPA)</td><td rowspan="3">Personal Information Protection and Electronic Documents Act (PIPEDA)</td></tr>
<tr><td>British Columbia</td><td>British Columbia Personal Information Protection Act (BCPIPA)</td></tr>
<tr><td>Quebec</td><td>Act respecting the protection of personal information in the private sector (APPIPS)

* Reform of the law is underway (since June 2020)</td></tr>
<tr><td>Other provinces and territories</td><td>Personal Information Protection and Electronic Documents Act (PIPEDA)</td><td>* Reform of the law is underway (since November 2020)</td></tr>
</table>

Even if they are perceived as similar here, the different laws applicable in Canada may not be perceived as such by foreign entities. The European Commission's assessments of the adequacy of legal frameworks for the protection of personal information (adequacy determinations) are a good example.

[468] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Provincial laws that may apply instead of PIPEDA," May 2020, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/

The regulatory framework applicable within the European Union limits the transfer of personal information to a country or organization that does not respect the level of protection offered within the European Union. In order to facilitate the analysis and to avoid companies having to put in place specific guarantees for each transfer, there is a mechanism for recognizing the adequacy of foreign frameworks with the European framework[469]. Transfers to a third country deemed "adequate" by the European Commission are then assimilated to data transfers within the European Union. The Canadian federal framework has benefited from such an adequacy decision since December 20, 2001[470] (reaffirmed in 2006[471]). However, analysis of the Quebec framework – qualified here as essentially similar to the one provided for in the federal law – led to a recommendation not to declare the framework adequate for the European Union![472]

It should be noted that both the federal and provincial laws will eventually need to be reassessed by the European Commission, as the European Union changed its regulatory framework in 2016 with the adoption of the *General Data Protection Regulation* (*GDPR)* (which came into force in 2018).

5.1.3. Long-awaited reforms

In fact, it's partly because of the upcoming European assessments[473] that several Canadian legislatures are currently making significant reforms to their respective laws for the protection of personal information in the private sector.

On June 12, 2020, Bill 64 was tabled in the Quebec National Assembly[474], proposing changes to some 21 laws in the province as well as a significant reform of *APPIPS*.

A few months later, on November 17, 2020, Bill C-11 was introduced in the House of Commons in Ottawa[475]. It proposed a complete rewrite of *PIPEDA* (now called the *Consumer Privacy Protection Act*) and the creation of a personal information and data protection tribunal. The bill was part of the implementation of the *Canadian Digital Charter*, a

---

469 GDPR, *supra* note 55, art 45. Formerly EUROPEAN UNION. Directive 95|46|EC, *supra* note 85, art. 25.
470 COMMISSION OF THE EUROPEAN COMMUNITIES. Decision 2002/2/EC, *supra* note 87.
471 CANADA. "Third Progress Report on Developments in Data Protection Legislation in Canada," Report to the European Commission, June 2018, p.3, online: https://www.ic.gc.ca/eic/site/113.nsf/fra/h_07662.html
472 ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 7/2014 on the protection of personal data in Quebec, 1443/15/FR WP 219, June 4, 2014, online: https://www.dataprotection.ro/servlet/ViewDocument?id=1290. The European Commission's decision has been suspended until Quebec makes certain legislative changes.
473 "The Privacy Commissioner's office said it understands a review of the GDPR by the European Commission is required by May 2020": SOLOMON, H. "Give privacy commissioner enforcement power, says parliamentary committee," IT World Canada, March 5, 2018, online: https://www.itworldcanada.com/article/give-privacy-commissioner-enforcement-power-says-parliamentary-committee/402451
474 QUEBEC. Bill 64, An Act to modernize legislative provisions as regards the protection of personal information, online: http://www.assnat.qc.ca/en/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html
475 CANADA. Bill C-11. An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts, Second Session, Forty-third Parliament, 2020.

document unveiled in May 2019 that, rather than a charter, is really a roadmap for the Canadian government's future regulatory initiatives[476].

Those two bills have taken quite different paths in the months since. The Quebec bill was ultimately adopted on September 21, 2021, following a lengthy review by the Quebec Commission on Institutions, during which there were numerous breaks. The majority of the new provisions are scheduled to come into force in September 2023[477]. The federal bill died on the order paper in the summer of 2021, following the announcement that a federal election would be held in September 2021. But even before that announcement, the bill was only at the second reading stage in the House of Commons[478] and did not appear to be on the government's priority legislative agenda at the time. At the time of this report, it is not known whether the re-elected government intends to reintroduce Bill C-11 as is.

5.2. How Do Canadian Laws Address Consumer Concerns?

In the analysis that follows, we will discuss federal and provincial legislation that deals with the protection of personal information in the private sector. We will also discuss the changes proposed by the two bills introduced in 2020. Due to the very short time between the adoption of the Quebec bill and the submission of this report, we are not in a position to review Quebec's Bill 25 (the culmination of Bill 64). We have therefore chosen to limit our review to the January 2021 versions of both bills. Some of our comments on the Quebec draft may therefore no longer be up to date due to amendments made to the draft after that date. In the case of the federal project, this choice has no impact since the text of Bill C-11 was not modified between its tabling in November 2020 and the dissolution of Parliament in August 2021.

We will focus on the different legislative approaches taken and not on the details of the specific provisions contained in the laws or bills in question. How do they address certain privacy risks? How do they conceive of each party's responsibility to protect personal information?

In some cases, the approach taken by Canadian legislators has been criticized by experts or civil society groups. Where appropriate, we will highlight those criticisms and some of the other legislative or regulatory approaches proposed by the authors or implemented in other countries, particularly in the European Union.

---

476 UNION DES CONSOMMATEURS. "A Charter of Rights for Internet Users: For a Canadian Perspective," January 2020, online: https://uniondesconsommateurs.ca/une-charte-des-droits-des-internautes-pour-une-perspective-canadienne/ includes an analysis of the Canadian Digital Charter in light of other instruments developed abroad and internationally for recognizing Internet users' rights (section 3.2.4).
477 NATIONAL ASSEMBLY OF QUEBEC. "Bill 64," online: http://assnat.qc.ca/en/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html (consulted on October 10, 2021).
478 PARLIAMENT OF CANADA. "C-11 – 43rd Parliament, 2nd Session," LegisInfo, online: https://www.parl.ca/LegisInfo/en/bill/43-2/c-11 (consulted on October 10, 2021).

5.2.1 Concerns about the handling of personal information

Recall that the three main concerns identified by Malhotra *et al* all received a high level of support from Canadian survey respondents. Those concerns relate to the extent of personal information collection, the degree of control that consumers have over that collection and over the general handling of their personal information, as well as the state of their knowledge about the information.

Accordingly, we will first examine how applicable Canadian laws address the data-driven economy, consumers' control over their personal information, and companies' transparency in the handling of that information.

5.2.1.1 Canadian laws and companies' transparency in the handling of personal information

The approach of Canadian legislators with respect to individuals' knowledge of the handling of their personal information revolves around an obligation of transparency for companies involved in the handling.

The four Canadian laws applicable to the private sector thus provide that before or at the time of collecting an individual's personal information, a company must explain to him the purposes of doing so[479]. The Quebec and federal laws provide for a number of other elements that must also be disclosed to the individual concerned, either automatically or upon request (particularly regarding access to the file by the company's employees or by the individual himself)[480]. The federal Act, which, it should be noted, is more in the nature of broad principles, also provides that an individual will be able, "without unreasonable effort," to obtain information about an organization's policies and practices for handling his personal information[481].

In order to meet those transparency obligations – which may be more or less stringent depending on the applicable law – Canadian companies generally include the required information in their terms and conditions of use for the goods or services sold, or in their website's privacy policy (to which a window at the bottom of a Web page usually refers), often with the words "I accept the terms and conditions of use" and a box that the user must check to express his consent in order to proceed with his browsing or transaction. Despite a distinct obligation to convey information in an understandable and easily accessible manner[482], we highlighted in section 2.1.1.3 several problems associated in practice with these types of documents. They are long, complex and often full of ambiguous terms. So it's difficult to consider them easily understandable and accessible to the average consumer...

---

[479] PIPEDA, *supra* note 77, Schedule 1, s. 4.2.3; PIPEDA, *supra* note 78, s. 8; BCPIPA, *supra* note 78, s. 10(1)(a); APIPA, *supra* note 78, s. 13(1)(a).
[480] PIPEDA, *supra* note 77, Schedule 1, s. 4.8; PIPEDA, *supra* note 78, s. 8.
[481] PIPEDA, *supra* note 77, Schedule 1, s. 4.8.1.
[482] *Ibid.,* Schedule 1, Art. 4.8.

In addition to the difficulties of understanding, another major problem is the amount of such material to which an individual is exposed online. With every website visited, with every service used online, the individual will be exposed to more and more information about the handling of his personal information.

This reality has led researchers to speak of information overload, making the individual able to adequately process only a fraction of the information he receives[483]. We recall that reading the policies of large organizations such as Facebook, Google, Snapchat and Airbnb takes at least 20 minutes each[484]. A study conducted in 2008 concluded that an individual who reads the privacy policies of all the websites he visits would have to spend about 240 hours per year, the equivalent of 10 full days or nearly 40 minutes per day[485]. It's likely that the time commitment today would be much higher[486].

Unfortunately, several researchers who have studied privacy policies in the private sector have concluded that it's impossible to adequately inform individuals about those policies in the current context:

> If notice (in the form of a privacy policy) finely details every flow, condition, qualification, and exception, we know that it is unlikely to be understood, let alone read. But summarizing practices in the style of, say, nutrition labels is no more helpful because it drains away important details, ones that are likely to make a difference: who are the business associates and what information is being shared with them; what are their commitments; what steps are taken to anonymize information; how will that information be processed and used. An abbreviated, plain-language policy would be quick and easy to read, but it is the hidden details that carry the significance. Thus the transparency paradox: transparency of textual meaning and transparency of practice conflict in all but rare instances[487].

5.2.1.1.1. Increased obligations in proposed legislative reforms

Under the federal and Quebec reforms, the common legislative approach that emphasizes mandatory disclosure of information by a company that intends to handle personal information is maintained in its entirety. In addition, the transparency obligations of businesses are extended to new aspects. Some of those additions are explained by the evolution of technologies, in a context where laws are revised to be better adapted to the

---

[483] BEN-SHAHAR, O and SCHNEIDER, C. E. "The failure of mandated disclosure," University of Pennsylvania Law Review, vol. 159, p. 687, online: https://www.law.upenn.edu/journals/lawreview/articles/volume159/issue3/BenShaharSchneider159U.Pa.L.Rev.647(2011).pdf

[484] COLEMAN, J. "Here's How Long It Would Take to Read All the New Privacy Updates," May 23, 2018, online: https://jonnathancoleman.medium.com/heres-how-long-it-would-take-to-read-all-the-privacy-updates-you-ve-been-getting-cd4f215cff6d

[485] MCDONALD, A. M. and CRANOR, L. F. "The Cost of Reading Privacy Policies," A Journal of Law and Policy for the Information Society, 2008, p. 18, online: https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf

[486] For example, Google's policy was just over 2,000 words long in 2009 compared to 4,000 words ten years later: WARZEL. "Google's 4,000-Word Privacy Policy," *supra* note 138.

[487] NISSENBAUM, H. "A Contextual Approach to Privacy Online," Journal of the American Academy of Arts & Sciences, fall 2011, p. 36, online: https://www.amacad.org/publication/contextual-approach-privacy-online

realities of the Web. For example, Bill 64 (Quebec) provides for mandatory disclosure of a company's use of personal information processing technology that makes it possible to identify, locate or profile the individuals concerned[488].

5.2.1.2. Canadian laws and consumers' control over their personal information

The control that consumers have (or would like to have) over the handling of their personal information is found in Canadian law primarily in the consent provisions. Those provisions must, of course, be read in conjunction with the provisions regarding corporate transparency, since consent will only be valid if it is free and informed.

The treatment of consent in the various laws

All four laws provide that the collection or handling of personal information may only take place, with certain exceptions, with the individual's prior consent, unless otherwise authorized by law[489].

The various laws in force across the country therefore make consumer consent a central element in the handling of personal information by the private sector. They place the consumer, on the surface at least, at the centre of decisions. However, it turns out that the exercise of consent is much more difficult in practice than it appears in the law and that a consumer ultimately has little real control over the handling of his information online. Some people therefore describe the current legislative framework for consent as illusory[490] or overly optimistic[491]. Let's see why.

Three questions are central to analyzing the quality of consent: Is it informed? Is it freely given? And is it manifest? For each of those questions, the realities of the Web negatively affect the answer.

Regarding informed consent, we're reminded of the phenomenon of information overload and the illegible and unclear privacy policies of major corporations studied by the New York Times, which we discussed earlier. Added to this is the difficulty consumers have in assessing the risks and other consequences of their eventual consent, particularly the

---

[488] QUEBEC. Bill 64, *supra* note 474, s. 99 (adding s. 8.1 of APPIPS).
[489] Those other statutory bases are drafted and considered in practice as exceptions to consent. PIPEDA, *supra* note 77, Schedule 1, Principle 4.3; PIPEDA, *supra* note 78, s. 6; BCPIPA, *supra* note 78, s. 14; APIPA, *supra* note 78, s. 7(1).
[490] WORLD ECONOMIC FORUM. "Redesigning Data Privacy: Reimagining Notice & Consent for human technology interaction, white paper," July 2020, p. 4, online: http://www3.weforum.org/docs/WEF_Redesigning_Data_Privacy_Report_2020.pdf
[491] SOH, S. Y. "Privacy nudges: an alternative regulatory mechanism to 'informed consent' for online data protection behaviour," European Data Protection Law Review, vol. 5, No. 1, 2019, pp. 67-68.

longer-term consequences. This reality is sometimes described as "privacy myopia[492]," referring to the vision impairment that makes it more difficult to see distant objects. We observe, then, that the current Web context makes it difficult for consumers to express truly informed consent.

The situation does not improve when it comes to the free nature of online consumer consent. Is the consumer expressing choice without coercion? Does the consumer really have a choice about whether or not to consent to the handling of his personal information by online businesses, for example when dealing with a business that has a monopoly or near-monopoly on the supply of certain goods or services[493]? The simple answer is no. If he refuses to consent to the company's collection and use of his information, he must at the same time give up the goods or services (including, for example, access to a website or a digital platform) that he wants, and that he cannot necessarily do without. This choice, which is particularly present online, leads some experts to speak of a privacy dilemma[494]. This dilemma is all the more difficult to resolve for consumers who understand what they want, but who do not necessarily understand what the company requires in exchange and the real cost that this represents.

On this last point, it should be noted that the four existing laws contain provisions that aim – with varying degrees of success – to address this problem. For example, it is prohibited to make consent to the handling of personal information conditional on the offer of a good or service… unless the operations for which the company is seeking consent are required for the performance of the contract[495] or for "legitimate purposes[496]." Those exceptions are often interpreted too broadly by businesses[497].

Lastly, the seriousness of a consent is also assessed by the manner in which it is expressed by the consumer. In this regard, current legislation gives businesses a great deal of leeway by allowing them to rely on implied consent to handle personal information in certain circumstances, i.e., consent that is inferred from the circumstances. *PIPEDA* allows personal information to be processed on the basis of implied consent where the

---

[492] BYGRAVE, L. and SCHARTUM, D. "Consent, Proportionality and Collective Power," in GUTWIRTH, S. *et al*, eds., Reinventing Data Protection, Springer, 2009, pp. 3-4, online: https://www.researchgate.net/publication/226832769_Consent_Proportionality_and_Collective_Power
[493] *Ibid.*
[494] GOULDING, A. "The identity and privacy dilemma," Newsroom, August 26, 2019, online: https://www.newsroom.co.nz/@ideasroom/2019/08/26/770241/the-identity-and-privacy-dilemma#; BURKHARDT, K. "The privacy paradox is a privacy dilemma," Mozilla Firefox, August 24, 2018, online: https://blog.mozilla.org/internetcitizen/2018/08/24/the-privacy-paradox-is-a-privacy-dilemma/
[495] APPIPS, *supra* note 78, s. 9(1); BCPIPA, *supra* note 78, s. 7(2); APIPA, *supra* note 78, s. 7(2).
[496] PIPEDA, *supra* note 77, Schedule 1, s. 4.3.3.
[497] Note in this regard the filing of multiple complaints in Europe against Google, Facebook, WhatsApp and Instagram by the nonprofit organization None of your business just minutes after the most recent EU regulation (tougher on "forced consent") went into effect: GROTHAUS, M. "Google and Facebook are already accused of breaking GDPR laws," Fast Company, May 25, 2018, online: https://www.fastcompany.com/40577794/google-and-facebook-are-already-accused-of-breaking-gdpr-laws; MOODY, G. "Google hit with first big GDPR fine over 'forced consent'; eight new complaints filed over 'right to access'," Privacy News Online, February 2, 2019, online: https://www.privateinternetaccess.com/blog/google-hit-with-first-gdpr-fine-over-forced-consent-eight-new-complaints-filed-over-right-to-access/

information is not sensitive[498]. The Alberta and B.C. legislation does not distinguish between types of information, but imposes a reasonableness test[499]. Only the Quebec legislation provides that consent must always be manifest (clearly expressed)[500].

Acknowledging implied consent is equivalent to setting up an opt-out system: If the individual does not take any concrete action to indicate his refusal to have his personal information handled, it will be considered that he has accepted. For example, an individual who visits a website implicitly consents to its collection and use of his information if the website indicates somewhere that this is the company's practice[501]. On the surface, this makes sense: A person continues to use a service after learning that it will collect information about him. He must be okay with that, right? In practice, it's far from clear, because of the lack of real competition in some online sectors, but also because this consumer knowledge of company policies and practices is, as we mentioned, purely theoretical and does not reflect reality at all.

The legitimacy of implied consent is therefore called into question depending on the circumstances.

> [...] with opt-out the consent procured is less legitimate than with opt-in regimes. This disparity does not make opt-out consent illegitimate, but it is certainly ambiguous, as opt-out consent might be the product of mere inertia or lack of awareness of the option to opt out[502].

The approach of law enforcement agencies

While the consent framework is central to any discussion of the state of a consumer's control over his personal information, it is not the only element of interest in Canadian law. The feeling that many consumers have of having lost control (or never having had control) over the handling of their data online is likely amplified by a sense that governing institutions are powerless as well.

An analysis of the limited powers of intervention conferred on the agencies responsible for enforcing laws for the protection of personal information in Canada leads to the conclusion that Canadian legislators have chosen to put in place a system that is not primarily intended to punish offending businesses, but rather to assist businesses in developing, improving and correcting their personal information handling practices and policies. This is

---

498 PIPEDA, supra note 76, Schedule 1, s. 4.3.6.
499 BCPIPA, *supra* note 78, s. 8(1); APIPA, *supra* note 78, s. 8(2)(b).
500 APPIPS, *supra* note 78, s. 14.
501 See the Office of the Privacy Commissioner of Canada's comments on implied consent for behavioural advertising: PRIVACY COMMISSIONER OF CANADA. "Guidelines on privacy and online behavioral advertising," December 2011, online: https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/tracking-and-ads/gl_ba_1112/
502 SOLOVE, D. J. "Privacy Self-Management and the Consent Dilemma," Harvard Law Review, vol. 126, 2013, p.1899, online: https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2093&context=faculty_publications

particularly the case at the federal level, which can be explained by the particular origins of its legislation.

The body responsible for enforcing *PIPEDA* is the Office of the Privacy Commissioner of Canada (OPC). Under the Act, the Office of the Privacy Commissioner can receive and investigate complaints from individuals[503], conduct audits[504] and initiate prosecutions[505]. However, it has no real enforcement powers: It can make recommendations following an investigation or enter into (voluntary) compliance agreements with an organization, but if the latter fails to cooperate, the OPC will have to turn to the courts and take (laborious) steps to enforce the law and punish violators. Thus, it has no direct enforcement power[506].

Among the most vocal critics of the OPC's weak powers to act is the OPC itself, which has been calling for changes to the law in this respect for many years! In a 2013 report on the need for *PIPEDA* reform, the OPC stated:

> Soft" recommendations with few consequences for non-compliance are no longer effective in a rapidly changing environment where privacy risks are on the rise.
>
> [... It is fair to ask how a small entity with limited resources, such as our Office, can get the attention of these companies and actively encourage them to comply with PIPEDA, when in fact there are very few consequences for violating Canadian privacy law.[507]

The enforcement agencies in Quebec, Alberta and British Columbia – the Commission d'accès à l'information and the Information and Privacy Commissioners, respectively – have more leeway in the decisions they can make (not just recommendations) following an investigation and/or complaint[508], but they too remain dissatisfied with the lack of teeth in their enforcement powers[509]. Like the federal Commissioner, they don't have the possibility of directly imposing financial penalties on offending companies without an investigation and a criminal conviction[510]. And the fines are not much of a deterrent: at most a few thousand dollars for a first offence in Quebec, with some exceptions[511].

---

503 PIPEDA, *supra* note 77, ss. 12 and fol.
504 *Ibid.* arts. 18 and fol.
505 *Ibid.,* art. 15.
506 OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "The Case for Reforming the Personal Information Protection and Electronic Documents Act," May 2013, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_r/pipeda_r_201305/
507 *Ibid.*
508 DEPARTMENT OF JUSTICE CANADA. "Offices of the Information and Privacy Commissioners: merger and related issues," 2015, online: https://www.justice.gc.ca/eng/rp-pr/csj-sjc/atip-aiprp/ip/p7.html; APPIS, *supra* note 77, s. 83; BCPIPA, *supra* note 77, s. 52; APIPA, *supra* note 77, s. 52.
509 STODDART, J. *et al*. "Modernizing Freedom of Information and Privacy Laws in the 21st Century," CAI, 2013, online: https://www.cai.gouv.qc.ca/modernisation-des-lois-sur-lacces-a-linformation-et-la-protection-des-renseignements-personnels-au-xxie-siecle/; BUCHANAN, J. and FRANKS, K. "BC Privacy Law Reform Update: Commissioner Calling for Changes to BC's Personal Information Protection Act," McCarthy, June 8, 2020, online: https://www.mccarthy.ca/en/insights/blogs/techlex/bc-privacy-law-reform-update-commissioner-calling-changes-bcs-personal-information-protection-act; BURDEN, A. "Canada: Alberta's Legislation On Privacy And Protection Of Personal Information Needs Review: Commissioner," Mondaq, January 7, 2021, online: https://www.mondaq.com/canada/data-protection/1022652/alberta39s-legislation-on-privacy-and-protection-of-personal-information-needs-review-commissioner
510 APPIS, supra note 77, s. 91 *a contrario*; APIPA, supra note 77, s. 52 and s. 59 *a contrario.*
511 APPIS, supra note 77, s. 91; BCPIPA, supra note 77, s. 50 and s. 52 *a contrario*.

5.2.1.2.1. Consumer control according to proposed legislative reforms

The federal and Quebec bills make a number of changes in terms of consumers' control over the handling of their personal information… but not necessarily to their benefit. The bills also reflect a change in approach with respect to law enforcement agencies.

Between strengthening and weakening consent

The Quebec bill departs somewhat from Quebec's current opt-in model by opening the door to implied consent for uses that have other purposes than those for which the personal information was collected, unless it is sensitive;[512] this is a new exception to the requirement for express consent, and is fortunately limited to other uses whose purposes would be compatible with those for which the information was collected. In addition, a requirement to obtain separate consent for each purpose of collection is added to the existing requirements[513].

The federal bill maintains the more generalized opt-out model that is already in place for the handling of non-sensitive information. The bill proposes a few minor changes and rewrites to the existing law that, according to Professor Teresa Scassa, do not justify the government's claims that it is "reforming" consent in order to improve the protection of personal information in the private sector[514]. What is being changed by the federal bill is the breadth of exceptions to the consent principle that are intended to reduce the burden on businesses. Among those new exceptions is the one related to the handling of personal information in the course of business activities for which a reasonable person would expect such collection, use, etc. of personal information[515]. The bill specifies that this exception includes, among other things, situations where it is "impracticable" to obtain consent given the absence of a direct relationship between the business and the consumer[516]. Another concern is that the rewritten federal legislation directly links company transparency obligations to the validity of consumer consent[517]. Thus, where consent is not required, it is not clear that the business still has an obligation to inform the consumer of its practices and policies prior to the collection or other handling of personal information.

---

[512] QUEBEC. Bill 64, *supra* note 474, s. 102 (replacing ss. 12-14 of APPIS).
[513] *Ibid.*
[514] SCASSA, T. "The Gutting of Consent in Bill C-11," 21 December 2020, online: http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=336:the-gutting-of-consent-in-bill-c-11&Itemid=80
[515] CANADA. Bill C-11, *supra* note 475, Part 1, s. 18.
[516] *Ibid.* s. 18(2)(e).
[517] *Ibid.* art. 15(3).

A right to data mobility

Although their revised consent provisions are considerably different, both bills agree on the recognition of a new right for consumers: the right to mobility of personal information[518]. It should be noted, however, that the federal bill provides for a more limited application, by limiting the exercise of this right to certain sectors of activity covered by an additional specific regulatory framework.

Generally speaking, the right to data mobility – known in Europe as the right to data portability[519] – allows individuals to obtain a copy of their personal information held by a service provider for delivery to a new service provider (e.g., bank, telecom, etc.) or to request disclosure directly between the two organizations[520]. By granting individuals a right to data mobility, the legislation increases their control over personal information that has already been collected and used by a company.

The right to data mobility is certainly associated with a conception of personal information as the property of the individuals concerned[521] and with a notion of control over that property, but is this right really a matter of privacy? There is some debate on this issue, but the general view is that it is primarily a competition law measure, aimed at fostering competition in the digital services market by facilitating consumer movement between providers[522]. A right to telephone number mobility (which is undeniably personal information) has existed in Canada for a long time, and has never been associated with a privacy measure…

More strongly deterrent monitoring agencies

The agencies responsible for applying the laws proposed by the two bills are given enhanced powers of intervention, thus making them agencies that should be better able to

---

[518] QUEBEC. Bill 64, *supra* note 474, s. 112 (amending s. 27 of APPIPS); CANADA. Bill C-11, *supra* note 475, Part 1, s. 72.
[519] GDPR, supra note 54, art. 20.
[520] Bill 64 requires that the information be disclosed to the individual, whereas Bill C-11 requires that the information be disclosed directly to the organization designated by the individual.
[521] Scassa on the right to data portability and the right to be forgotten: "These are quasi-ownership rights": T. SCASSA. "Data Ownership," CIGI Papers No. 187, September 2018, p. 2, online: https://www.cigionline.org/publications/data-ownership
[522] DE HERT, P. *et al.* "The right to data portability in the GDPR: Towards user-centric interoperability of digital services," Computer Law & Security Review, vol. 34, No. 2, April 2018, p. 194, online: https://www.sciencedirect.com/science/article/pii/S0267364917303333; T. SCASSA. "Replacing Canada's 20-Year-Old Data Protection Law," CIGI, December 23, 2020, online: https://www.cigionline.org/articles/replacing-canadas-20-year-old-data-protection-law; VAN DER AUWERMEULEN, B. "How to attribute the right to data portability in Europe: A comparative analysis of legislations," Computer Law & Security Review, vol. 33, No. 1, February 2017, p.59, online: https://www.sciencedirect.com/science/article/abs/pii/S0267364916302175

deter potential violators of the law: the power to issue orders[523], enhanced investigative powers[524], the power to impose administrative monetary penalties[525], etc.

By introducing administrative monetary penalties, which have long been called for by the organizations concerned, Quebec legislators are responding to one of the most recurrent criticisms of personal information protection laws here and elsewhere: that they are merely "paper tigers," threatening in appearance but harmless in practice[526].

Unfortunately, the federal government is undermining the OPC's new powers by creating an additional layer: the Personal Information and Data Protection Tribunal. Under Bill C-11, the tribunal is responsible for imposing sanctions that the OPC can only recommend to the tribunal[527]. Moreover, those sanctions are only available for a limited list of violations of the law[528]. It should be noted that the general rules related to the form and validity of consent are not covered![529] So It's important to understand that despite certain changes, federal legislation continues to favour a relatively "soft" approach for its agency responsible for ensuring compliance with the law on privacy protection: forcing a company to end certain non-compliant practices, to improve others, but rarely punishing it financially (or at least not quickly or simply).

A new individual and collective right of action

Both bills also make major changes to the steps that individuals can take in response to the improper handling of their personal information.

Those changes are certainly intended to give more power to individuals in the event of a problem, by expanding the types of penalties to which a company that violates the law is exposed, and by opening the door to more individual restitution. Again, however, the federal version has limitations and impediments that are difficult to justify.

Bill 64 (Quebec) provides for the possibility of compensatory and, in some cases, even punitive[530] damages for persons who have been victims of a violation. Bill C-11 also allows for damages to be awarded, but only if the Office has previously found that there has been a violation of the law (and if that finding has been upheld by the court, if there has been an appeal)[531]. Thus, many victims may be deprived of this right in practice, particularly because of the Office's ability to enter into compliance agreements that terminate complaint

---

[523] CANADA. Bill C-11, *supra* note 475, Part 1, s. 92(2).
[524] QUEBEC. Bill 64, *supra* note 474at ss 144 and fol.
[525] *Ibid.* s. 150 (adding ss. 90.1 and fol to the APPIS).
[526] GOLLA, S. J. "Is Data Protection Law Growing Teeth: The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR?", Journal of Intellectual Property, Information Technology and E-Commerce Law, vol. 8, No. 1, 2017, p. 70.
[527] CANADA. Bill C-11, *supra* note 475, Part 1, ss. 94(1) and 93.
[528] *Ibid.* s. 93(1).
[529] *Ibid.,* s. 93(1) c) and d). Only sections 15(5) and 16 relating to consent are covered.
[530] QUEBEC. Bill 64, *supra* note 474, s. 152 (providing for the addition of s. 93.1 to APPIS).
[531] CANADA. Bill C-11, *supra* note 475, Part 1, s. 106(1).

investigations[532]. That feature of the federal bill is particularly disappointing in that it makes this consumer right conditional on enforcement by an oversight agency whose underfunding is well documented[533]. The consumer's feeling of powerlessness, which the bills appeared aimed at alleviating, will instead likely be amplified by a system whose objective and operation seem opposed to one other!

5.2.1.3. Canadian law and the data-driven economy

Canada's current personal information protection laws were enacted between 1993 and 2003, and the challenges they attempted to address differed significantly from those of today, particularly in terms of scale. The years since their adoption have been rich in developments. Internet users' personal information has become increasingly important in this data-driven economy. Google got involved in behavioural advertising in 2003 with its AdSense advertising arm (and with the purchase of DoubleClick in 2007)[534]. Facebook became ubiquitous in 2006[535]. Then came the connected object boom in 2010[536]. Mayer-Schönberger and Padova summarize the vision – today inadequate – of the European framework (with a historical background similar to Canada's):

> Unsurprisingly, the directive reflects a "small data" world in which data collection, storage and processing is still comparatively expensive and thus undertaken sparingly[537].

Even so, current laws offer some answers to consumer concerns, with two guiding principles that are relevant to the context of big data. Some see this as an effective way to limit the collection and use of information. But others see it as a mismatch between the law and the situation, with the ultimate effect of inhibiting innovation without ensuring effective enforcement[538].

> The big data business model is antithetical to data minimization. It incentivizes collection of more data for longer periods of time. It is aimed precisely at those unanticipated secondary uses, the "crown jewels" of big data[539].

---

[532] *Ibid.* s. 86.
[533] See, for example, the Office of the Privacy Commissioner of Canada, 2018: PRIVACY COMMISSIONER OF CANADA. "privacy Commissioner denounces slow progress on fixing outdated privacy laws," news release, September 27, 2018, online: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/nr-c_180927/
[534] OKO. "The History of Online Advertising, OKO Ad Management," July 19, 2019, online: https://oko.uk/blog/the-history-of-online-advertising
[535] PHILLIPS, S. "A brief history of Facebook," The Guardian, July 25, 2007, online: https://www.theguardian.com/technology/2007/jul/25/media.newmedia
[536] KHVOYNITSKAYA, S. The IoT history and future, ITransition, 25 November 2019, online: https://www.itransition.com/blog/iot-history
[537] MAYER-SCHÖNBERGER. "Regime Change?", *supra* note 541, p. 321.
[538] See, e.g., ZARSKY. "Incompatible," *supra* note 541.
[539] TENE, O and POLONETSKY, J. "Big Data for All: Privacy and User Control in the Age of Analytics," Northwestern Journal of Technology and Intellectual Property, vol. 11, No. 5, 2013, pp. 259-260, online: https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip

The purposes of collecting personal information

All four Canadian statutes require an entity collecting personal information to identify the purposes for which it is being collected[540]. The entity must then disclose those purposes to the individuals concerned. This obligation represents a significant limitation in the context of big data, since one of its interests is the unexpected data and inferences that may arise from the automated processing of so much personal information. Researchers are concerned that the purposes of collection by companies wanting to maintain the added value of big data processing are likely identified in compliance with the letter of the law, but not with its spirit/objective by denouncing, for example, vague purposes[541].

In addition to the requirement to identify the purposes of collection in advance, the federal, Alberta and British Columbia legislation also imposes restrictions on the purposes that are acceptable, i.e., only those "purposes that a reasonable person would consider appropriate in the circumstances[542]." The federal Office of the Privacy Commissioner has issued guidelines on this subject, which, for example, point to discriminatory, unfair or unethical handling of personal information[543]. Quebec law requires that a company have a legitimate interest in the handling of personal information[544]. Some Quebec researchers think the two criteria are ultimately highly similar[545].

Minimization or limitation of collection and retention

A second principle of Canadian law also limits the scope of big data exploitation, by limiting the information collection that will be permitted[546]: The law provides that the collection must be minimal, that is, limited to the information that will be necessary for the purposes

---

[540] PIPEDA, *supra* note 77, Schedule 1, s. 4.2; PIPEDA, *supra* note 78, s. 4; BCPIPA, *supra* note 78, s. 10(1)(a); APIPA, *supra* note 78, s. 13(1)(a).
[541] ZARSKY, T. Z. "Incompatible: The GDPR in the Age of Big Data," Seton Hall Law Review, vol. 47, No. 4(2), 2017, online: https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1606&context=shlr; MAYER-SCHÖNBERGER, V. and PADOVA, Y. "Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation," Columbia Science & Technology Law Review, vol. 17, 2016, p. 322, online: https://www.researchgate.net/publication/303665079_Regime_Change_Enabling_Big_Data_Through_Europe%27s_New_Data_Protection_Regulation
[542] BCPIPA, *supra* note 78, ss 3 and 5(3); APIPA, *supra* note 78, s. 3 ("for purposes that are reasonable"), PIPEDA, *supra* note 77, s. 5(3).
[543] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Unacceptable Data Processing Practices Guidance Document: Interpretation and Application of Section 5(3)," May 2018, online: https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/collecte-de-renseignements-personnels/consentement/gd_53_201805/
[544] APPIPS, *supra* note 78, s. 4(1).
[545] They believe that the guidelines of the Office of the Privacy Commissioner of Canada, which are based on the federal criterion, could be used to guide the interpretation of the provincial criterion as well: DÉZIEL, P-L., BENYEKHLEF, K. and GAUMOND, E. "Repenser la protection des renseignements personnels à la lumière des défis soulevés par l'IA," response document to the questions asked by the Commission d'accès à l'information du Québec in the context of the consultation on artificial intelligence, April 2020, p. 18, online: http://collections.banq.qc.ca/ark:/52327/bs4067010
[546] *Ibid.,* p. 16.

identified[547]. And this concept of limitation is also found elsewhere in the legislation, notably with respect to the use and retention of collected information beyond certain time limits or factual situations. Historically, this principle was aligned with business practices, whereby the costs of retaining data exceeded their potential value, which is certainly no longer the case today[548].

Taking business needs into account in current legislation

While Canada's personal information protection laws were not designed for an economy driven by the exploitation of online data and personal information, legislators have historically paid special (if not priority) attention to business needs in developing those laws.

It should be recalled that Canada needed a legislative framework quickly in order to facilitate its trade relations with Europe, and that this led to the adoption of *PIPEDA* in 2000. The full title of the Act expressly mentions its true purpose: the facilitation and promotion of electronic commerce:

> An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information and transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act[549]

The protection of personal information therefore appears to be a way to encourage electronic commerce by allowing businesses, under certain conditions, to exploit consumers' personal information and by promoting consumer confidence in this practice, given the existence of rules.

Section 3 of the Act states that the framework takes into account "the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information[550]." The needs of businesses and the rights of individuals are thus placed on an equal footing in what resembles an arbitration exercise. The federal Commissioner has in the past criticized the lack of formal recognition of privacy rights in federal legislation and has supported the addition of a preamble as a means of entrenching privacy "in its proper human rights framework[551]."

---

[547] PIPEDA, *supra* note 77, Schedule 1, s. 4.4; PIPEDA, *supra* note 78, s. 5(1); BCPIPA, *supra* note 78, s. 11(a); APIPA, *supra* note 78, s. 11(2).
[548] BENNETT, C. J. and BAYLEY, R. M. "Privacy Protection in the Era of 'Big Data': Regulatory Challenges and Social Assessments" in VAN DER SLOOT, B., BROEDERS and SCHRIJVERS, E. Exploring the boundaries of Big Data, Amsterdam University Press, 2016, p.210, online: https://www.wrr.nl/binaries/wrr/documenten/verkenningen/2016/04/28/exploring-the-boundaries-of-big-data-32/V032-Exploring-Boundaries-Big-Data.pdf
[549] PIPEDA, *supra* note 77.
[550] *Ibid.*, art. 3.
[551] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Modernizing federal privacy Laws to better protect Canadians," Speech, March 9, 2020, online: https://priv.gc.ca/en/opc-news/speeches/2020/sp-d_20200309/

The Alberta and British Columbia laws also emphasize that their objective is to regulate the handling of personal information in a manner that recognizes both the right of individuals to the protection of their information and the needs of business[552]. The Quebec legislation does not as clearly emphasize the importance of business needs in its legislative approach to the protection of personal information, but the legislation's provisions, particularly those dealing with exceptions to consent, suggest that the approach is substantially similar.

5.2.1.3.1. Greater emphasis on information anonymization in proposed legislative reforms

In general, Bills 64 and C-11 do not challenge the legislators' approach of balancing the economic needs of business and the protection of consumer privacy. In fact, the federal bill moves the law even further away from recognizing a fundamental right for consumers, despite repeated requests from the federal Office.

> In fact, the bill arguably gives more weight to commercial interests than the current law by adding new commercial factors to be considered in the balance, without adding any reference to the lessons of the past twenty years on technology's disruption of rights.
>
> In my view, it would be normal and fair for commercial activities to be permitted within a rights framework, rather than placing rights and commercial interests on the same footing[553].

The Office, citing the work of Professor Teresa Scassa, points out that approaching the law from the perspective of the protection of a human right would allow for greater flexibility in the law's interpretation and evolution. In addition to jeopardizing individuals' right to privacy, mass surveillance can cause collective harm and impair other rights, such as the right to equality and protection against discrimination[554].

The bills also maintain the rules related to minimizing the collection of personal information and to identifying purposes in advance, but the Quebec bill does take note of industry criticism of the difficulty in applying the second principle regarding big data. The bill proposes the addition of an exception to the requirement to identify all purposes prior to the collection or use of personal information: The business would not be required to identify additional data handling purposes that are consistent with those for which consent was previously obtained[555]. It should be noted that this exception is more restrictive than its

---

[552] BCPIPA, *supra* note 78, s. 2; APIPA, *supra* note 78, s. 3.
[553] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Submission of the Office of the Privacy Commissioner of Canada on Bill C-11, the Digital Charter Implementation Act, 2020," May 11, 2021, online: https://priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ethi_c11_2105/
[554] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Privacy Law Reform: A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy," 2018-2019 Annual Report to Parliament on the Privacy Act and the Personal Information Protection and Electronic Documents Act, 2019, online: https://priv.gc.ca/en/opc-actions-and-decisions/ar_index/201819/ar_201819/
[555] QUEBEC. Bill 64, *supra* note 474, s. 100 (providing for new s. 12(2)(1) of the *PPACA*).

European counterpart, which provides for this waiver unless the new purposes are incompatible[556].

The bills also define and provide a better framework for the de-identification and anonymization of data collected, which is not insignificant in the context of big data and the processing of personal information using artificial intelligence. In this regard, the federal legislators seem to be more aware of the risks of re-identification and are putting forward a more coercive definition of de-identified information – a definition that covers information that, alone or in combination with other information, could identify the individual concerned[557]. The equivalent definition in Bill 64 does not take indirect identification into account[558]. However, the Quebec bill does define the concept of anonymization: Information is anonymized if it irreversibly can no longer be used to identify the individual concerned, either directly or indirectly[559]. The Alberta and British Columbia laws, which are not currently being reformed, do not mention those concepts.

The inclusion of such definitions is particularly interesting since de-identified information is no longer, in principle, personal information to which protective laws apply (and thus to which consent is required prior to processing by businesses)[560]. Given that big data processing increases the risk of re-identification of de-identified information[561], it is promising that legislators are dealing cautiously with de-identification and anonymization.

---

[556] GDPR, *supra* note 55, art 5(b); SEINEN, W., WALTER, A. and VAN GRONDELLE, S. "Compatibility as a Mechanism for Responsible Further Processing of Personal Data," p.3, online: https://www.bakermckenzie.com/-/media/files/insight/publications/2018/10/compatibility_mechanism_responsible_further_personal_data_processing.pdf?la=en

[557] CANADA. Bill C-11, *supra* note 475, Part 1, s. 2, definition of "de-identify."

[558] QUEBEC. Bill 64, *supra* note 474, s. 100 (providing for new s. 12(4)(1) of APPIS).

[559] *Ibid.* s. 111 (which provides for new s. 23 of APPIS).

[560] It should be noted in this regard that the federal bill does address information handling following de-identification in several sections of Bill C-11. Some see this as confusion on the part of federal legislators, while others see it as a recognition of the limits of current de-identification processes; see also on this subject: SCASSA, T. "Data for Good?: An Assessment of the Proposed Exception in Canada's Private Sector Data Protection Law Reform Bill," December 6, 2020, online: http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=335:data-for-good?-an-assessment-of-the-proposed-exception-in-canada%E2%80%99s-private-sector-data-protection-law-reform-bill&Itemid=80

[561] BENNETT, C. J. and BAYLEY, R. M. "Privacy Protection in the Era of 'Big Data': Regulatory Challenges and Social Assessments" in VAN DER SLOOT, B., BROEDERS and SCHRIJVERS, E. Exploring the boundaries of Big Data, Amsterdam University Press, 2016, p.210, online: https://www.wrr.nl/binaries/wrr/documenten/verkenningen/2016/04/28/exploring-the-boundaries-of-big-data-32/V032-Exploring-Boundaries-Big-Data.pdf. See in this regard the examples of "accidental" re-identification in PURTOVA, N. "The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law," Law, Innovation and Technology, vol. 10, No. 1, 2018, pp. 7-8, online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3036355; FASKEN. "Privacy and Cybersecurity Bulletin," March 1, 2021, online: https://www.fasken.com/en/knowledge/2021/03/1-de-identification-of-personal-information-under-the-proposed-consumer-privacy-protection-act

5.2.2 Specific concerns about the security of personal information collected, processed and stored

Current personal information protection legislation contains some provisions relevant to the security of data processing and storage systems. The presence of those provisions suggests that legislators, contrary to some experts, do not fully distinguish between data security and privacy, or at least perceive them as complementary.

Generally speaking, the laws do not dictate how businesses must ensure the security, integrity and confidentiality of the personal information they collect and hold. The laws provide for more general obligations in this regard[562], and some specify that the level of protection must take into account, among other things, the type and sensitivity of the information in question[563]. The federal Act is the only one that goes into greater detail, expressly requiring the implementation of administrative, technical and physical safeguards[564].

The responsibility of a company that transfers personal information it holds to third-party companies hired to assist in processing that information is treated unequally by Canadian legislators. Only the federal legislation expressly provides that the company must ensure the adequacy of the protection offered by the third party (the level of protection must be comparable to that required by the legislation[565]). The Alberta and B.C. laws more generally emphasize companies' responsibility for the data under their control[566]. The Quebec law is surprisingly silent on this issue.

5.2.2.1 Elimination of personal information held

The Quebec law also appears to be lacking with respect to the handling of personal information when its use is completed or when it should no longer be used; the law simply states that use is no longer permitted.

In contrast, the federal, Alberta and British Columbia laws provide that information must be destroyed, erased or de-identified after use[567]. *PIPEDA* requires an organization to develop guidelines on this issue and to set maximum retention periods[568].

---

562 PIPEDA, *supra* note 77Schedule 1, ss. 4.7 and 4.7.1; BCPIPA, *supra* note 78, s. 35; APIPA, *supra* note 78, s. 34; PIPEDA, *supra* note 78, s. 10.
563 PIPEDA, supra note 77, s. 10; PIPEDA, *supra* note 76, Schedule 1, Arts. 4.7 and 4.7.2.
564 PIPEDA, *supra* note 77, Schedule 1, s. 4.7.3.
565 PIPEDA, supra note 76, Schedule 1, s. 4.1.3 and s. 7.2(2).
566 BCPIPA, *supra* note 78, s. 4(2); APIPA, *supra* note 78, s. 5(1).
567 PIPEDA, *supra* note 76, Schedule 1, ss. 4.5 to 4.5.4; BCPIPA, *supra* note 77, s. 35(2); APIPA, *supra* note 77, s. 35(2).
568 PIPEDA, *supra* note 76, Schedule 1, s. 4.5.2.

5.2.2.2 Sending a notice in case of a privacy incident

PIPEDA imposes an obligation on organizations to report to the Privacy Commissioner and the individual concerned a breach of security that results in an unauthorized disclosure, loss or access to personal information held by the organization, if it is reasonable to believe that the breach poses a real risk of serious harm to the individual in question[569]. Businesses must maintain a record of relevant breaches[570].

In general, the rules for notification following a breach of security or confidentiality are explained by the legislators' desire to ensure a rapid response from the entities and individuals concerned in order to avoid a privacy violation or to lessen its impact, if any[571].

It should be noted that *PIPEDA*'s obligations for notifications of confidentiality incidents are less onerous than those found in the European Union's *GDPR*. Companies subject to the European law are in fact required to report any incident to the competent authorities, unless it "is not likely to result in a risk to the rights and freedoms of natural persons[572]." It is only when a separate notice is sent to the individuals concerned that the question of the harm that may be caused by the breach of security measures is taken into account[573]. Thus, the competent authorities are likely to be in a better position to develop a picture of the state of security measures in certain areas and to respond quickly to recurring problems. The Canadian provision also differs from those adopted in some U.S. states with respect to incident notification, in that it does not provide for specific time limits for notification (e.g., 30-45 days)[574], but rather calls for action "as soon as practicable[575]." Also of note is the inclusion in some U.S. laws of a requirement – with no equivalent in Canada – for companies to notify credit rating agencies of certain confidentiality incidents affecting consumers[576].

The Alberta law also requires mandatory notice to the Commissioner, but not to individuals directly[577]. Neither of the other two provincial laws applicable to the private sector has such a provision. *PIPEDA* has only had these rules[578] since 2018, but the Alberta legislation has had them for over 10 years![579]

---

[569] *Ibid.* ss. 10.1(1) and 10.1(3) and 2(1).
[570] *Ibid.* s. 10.3(1).
[571] ARTICLE 29 DATA PROTECTION WORKING PARTY. "Guidelines on Personal data breach notification under Regulation 2016/679," 18/EN WP250rev.01, October 3, 2017, p. 6.
[572] GDPR, *supra* note 54, art. 33(1).
[573] *Ibid.* arts. 33 and 34.
[574] SERRATO, J. K. *et al*. "US states pass data protection laws on the heels of the GDPR," July 9, 2018, Norton Rose Fullbright, online: https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/
[575] PIPEDA, *supra* note 76, s. 10.1(2).
[576] See, for example, the explanations of the provisions adopted in Alaska, Colorado, Rhode Island and Vermont: DIGITAL GUARDIAN. "The Definitive Guide to U.S. State Data Breach Laws," 2018, online: https://info.digitalguardian.com/rs/768-OQW-145/images/the-definitive-guide-to-us-state-data-breach-laws.pdf
[577] A APIPA, *supra* note 78, s. 34.1.
[578] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "A full year of mandatory data breach reporting: What we've learned and what businesses need to know," Oct. 31, 2019, online: https://www.priv.gc.ca/en/blog/20191031/
[579] ALBERTA. Personal Information Protection Amendment Act, 2009, SA 2009, c 50.

5.2.2.3. Important additions to the proposed legislative reforms

Among the most significant changes in Bill C-11 (federal) and Bill 64 (Quebec) is the inclusion of provisions relating to the security of business information handling and retention systems. The proposed changes are modelled after existing provisions in other Canadian laws or in the *GDPR*.

The desire to considerably modernize companies' obligations regarding data security appears to be in line with consumers' increased concerns about this subject. It also undeniably reflects the important place that the Internet is taking in the reform process.

Prior risk assessment

Bill 64 requires businesses to conduct an assessment of privacy-related factors (APF) prior to the implementation of any information system or electronic service delivery system that involves the processing of personal information[580]. This obligation goes further than the one provided for in *PIPEDA,* for example, with respect to the implementation of security measures for systems; in fact, a company will have to choose and implement the measures in light of the results of its risk analysis[581]. The Quebec APF is largely inspired by the data protection impact analysis (DPIA) developed in Europe[582].

The purpose of this type of analysis is to help companies put in place measures that meet their legal obligations. In that sense, they serve as tools for self-empowerment, which is reminiscent of the coaching approach favored by certain law enforcement agencies[583]. In its guidelines, the Article 29 Data Protection Working Party emphasizes the added value of those analyses for companies to comply with the law[584] (beyond their obligation to carry out the analysis itself).

In adapting this European creation to Bill 64, the Quebec legislators have unfortunately removed an important component of the risk analysis. Only the impacts on privacy are taken into account; the European model deals more broadly with the rights and freedoms of the individuals affected, including the protection of freedom of expression and

---

580 QUEBEC. Bill 64, *supra* note 474, s. 95 (adding s. 3.3 to APPIPS).
581 GDPR, supra note 54, preamble, para. 84.
582 *Ibid.* art. 35.
583 The Office of the Privacy Commissioner of Canada has long provided an assessment tool and guide on its website: PRIVACY COMMISSIONER OF CANADA. "PIPEDA Self-Assessment Tool, July 2008, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/pipeda_sa_tool_200807/. The Commission d'accès à l'information also provides an online companion guide: COMMISSION D'ACCÈS À L'INFORMATION. "Guide d'accompagnement, May 2020, online: https://www.cai.gouv.qc.ca/documents/Guide_EFVP_FR.pdf
584 ARTICLE 29 DATA PROTECTION WORKING PARTY. "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679," 17/EN WP 248, 4 April 2017, p.19, online: https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2017/07/wp248_enpdf.pdf

movement and the right not to be discriminated against, for example[585]. This choice not to consider the impact of personal information handling on other fundamental rights is reiterated in the bill when it comes to automated data processing for decision-making purposes[586].

Incident notices

The Quebec bill includes provisions for notification of privacy incidents to the Commission and to the individuals concerned, "if the incident presents a risk of serious harm[587]." Those provisions are very similar to those already in *PIPEDA*. Once the bill is passed, only the British Columbia law will lack this requirement.

Dealing with fraud that arises from online privacy breaches

Canadian consumers in our survey were particularly concerned about fraud or identity theft resulting from unauthorized access to their personal information held by a company. Similar to the laws currently in place, the proposed legislation does not specifically address those consequences or the assistance that can be provided to victimized consumers. Identity fraud and identity theft are covered by offences in the Canadian Criminal Code. A person who is a victim of identity fraud or identity theft will therefore be referred to the police and the Canadian Anti-Fraud Centre[588].

It should be noted, however, that the Quebec legislators focused more specifically on one aspect of this problem after the Desjardins data leak. The *Credit Assessment Agents Act* was adopted in October 2020 and provides for certain relevant protections that must now be offered by those companies with which victims of a leak or theft of their personal information are likely to do business in order to limit the risks or effects of identity theft. Consumers can apply a security freeze to their file to limit the disclosure of information to third parties[589], receive a security alert when a disclosure is made[590], and have an explanatory note added to their credit file[591]. It should be noted that Bill 64's explanatory notes make no mention of Quebecers' privacy protection, but rather address the need to

---

[585] *Ibid.*, p. 15.
[586] See the comments of the Ligue des droits et libertés: LIGUE DES DROITS ET LIBERTÉS, "Mémoire, consultations particulières et auditions publiques au sujet du projet de loi 64 : loi modernisant des dispositions législatives en matière de protection des renseignements personnels," 2020, pp. 9-10, online: https://liguedesdroits.ca/wp-content/fichiers/2020/09/memoire_projet_loi_64_renseignement_personnel_20200923.pdf
[587] QUEBEC. Bill 64, *supra* note 474, s. 95 (adding s. 3.5 to APPIPS).
[588] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Identity theft and you," October 2020, online: https://www.priv.gc.ca/en/privacy-topics/identities/identity-theft/guide_idt/
[589] QUEBEC. Credit Assessment Agents Act, SQ 2020, c 21, s. 9.
[590] *Ibid.,* art. 10.
[591] *Ibid.* art. 11.

regulate credit rating agencies' commercial practices [592], which had received significant negative coverage in the months preceding the bill's introduction[593]. The potential benefits for consumers with respect to the handling of their personal information are thus a positive consequence, but not the reason for the existence of this new law.

We therefore note that, despite legislators' undeniable desire to integrate more provisions related to the security of computer systems and the personal information they contain into personal information protection legislation, certain subjects remain addressed independently, particularly when it comes to consequences that would result from failure to comply with such legislation.

5.2.3 Specific concerns about the use of personal information for commercial purposes

Online consumer tracking and profiling practices have grown in recent decades. Current personal information protection laws, which were not designed with that in mind, are difficult to apply effectively.

For the laws to apply, the data collected and used must first constitute personal information within the meaning of the laws: This is generally defined as information that concerns an identifiable individual or makes it possible to identify him. Data such as an individual's IP address or the serial number of his connection device alone will not identify an individual. Do the laws cover the handling of such data?

Since the collection and use of such data is intended to develop personalized advertisements tailored to the behaviour of individuals, the Office of the Privacy Commissioner of Canada has issued guidelines advising that information used for online tracking and targeting is generally covered by the legislation[594].

That specific purpose of personal information handling is not subject to specific rules. It is therefore necessary to refer to the general rules of the various laws, mainly with respect to consent. It should be noted that implied consent, the many problems of which were

---

[592] QUEBEC. Bill 53. Credit Assessment Agents Act, First Session, Forty-second Parliament, 2019, explanatory notes.

[593] See for example: "Des clients de Desjardins excédés par le temps d'attente chez Equifax," TVA Nouvelles, July 3, 2019, online: https://www.journaldemontreal.com/2019/07/03/des-clients-de-desjardins-excedes-par-le-temps-dattente-chez-equifax-1; "Des clients de Desjardins peinent à se faire servir en français par Equifax," Radio-Canada, July 4, 2019, online https://ici.radio-canada.ca/nouvelle/1211212/clients-desjardins-equifax-difficultes-service-francais-oqlf; BORDELEAU, S. "Inacceptable": Desjardins lance des mesures pour pallier les "ratés" d'Equifax," Radio-Canada, July 5, 2019, online: https://ici.radio-canada.ca/nouvelle/1211973/desjardins-mesures-accelerer-activation-forfaits-equifax

[594] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Identity Theft," *supra* note 588; see a more detailed analysis of the adequacy of the definition of "personal information" to the practice of behavioural advertising: OPTION CONSOMMATEURS. "Le prix de la gratuité - Doit-on imposer des limites à la collecte de renseignements personnels dans le cadre de la publicité comportementale en ligne?", June 2015, pp. 38-40, online: https://option-consommateurs.org/wp-content/uploads/2017/06/option-consommateurs-2014-2015-gratuite-rapport.pdf

discussed above, is generally considered acceptable in the context of targeted online advertising, if the company has respected its transparency obligations[595].

5.2.3.1 Reforms whose effects remain uncertain

The bills make consent rule changes rules that may be relevant to online tracking and the use of personal information for profiling and targeted advertising. However, the exact effect of those changes remains unclear, given some of the exceptions put forward by legislators.

In general, businesses are required to disclose to consumers the purposes for which they collect personal information and how they intend to use it. The Quebec bill expressly states that this disclosure must include the use of technology whose features make it possible to identify or locate the Internet user or to carry out profiling, as the case may be[596].

Regarding required consumer consent, Bill C-11 provides an exception whereby the collection or use is for a business purpose and a reasonable person would expect it. The specific example given is "an activity in the course of which obtaining the individual's consent would be impracticable because the organization does not have a direct relationship with the individual[597]," which is likely to include many third-party companies that analyze data, particularly for marketing purposes[598]. This circumvention of consent is not possible, however, when personal information is collected or used to influence the individual's behaviour or decisions[599], which should logically pertain to targeted advertising[600]. But not all data handling for commercial purposes is directly aimed at influencing behaviour…

It should be noted that Bill C-11 maintains the possibility of relying on implied consent for the processing of personal information. Similarly, the Quebec bill allows for the existence of implied consent[601] to be considered, depending on the circumstances, even though separate consent is required for each of the purposes for which the data will be collected. It is difficult to see how those two rules will co-exist and what type of consent would ultimately be valid for handling personal information for identification, tracking and profiling purposes or when it is to be sold to other entities.

---

595 OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Guidelines," *supra* note 501; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Policy position on online behavioural advertising," December 2015, online: https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/tracking-and-ads/bg_ba_1206/

596 QUEBEC. Bill 64, *supra* note 474, s. 18 (adding s. 65.0.1(1)(1) to APPIPS).

597 CANADA. Bill C-11, *supra* note 475, Part 1, s. 18(2)(e).

598 YOUNG, D. "New federal privacy law – a fine balance between the GDPR and PIPEDA?", 2020, online: http://davidyounglaw.ca/compliance-bulletins/new-federal-privacy-law-a-fine-balance-between-the-gdpr-and-pipeda/

599 CANADA. Bill C-11, *supra* note 475, Part 1, s. 18(1)(b).

600 YOUNG. "New federal privacy law," *supra* note 598.

601 By prohibiting it *a contrario* for sensitive personal information: QUEBEC. Bill 64, *supra* note 474, s. 19 (amending s. 65.1 of APPIPS).

The Quebec legislators seem to be aware of many Internet users' desire to refuse all forms of online tracking. Without really giving users the tools to do so, the legislators do provide for certain additional transparency obligations. Thus, companies that offer ways to deactivate identification, location and profiling functions must inform consumers[602]. There's no provision, however, if companies don't voluntarily offer those functions, and no obligation to do so…

The Canadian bills don't specifically address the issue of the sale of personal information to third parties (other than a requirement to disclose the name or type of third parties with which the data collected may be shared[603]).

Here as elsewhere, that issue is the subject of too little discussion by legislators and regulators[604]. Nevertheless, we should note some American initiatives on the subject. The *California Consumer Privacy Act*, for example, gives individuals the right to refuse the sale of personal information to third parties. The company must notify the individual of the possibility of a future sale and give him the opportunity to object[605]. Similarly, California and Vermont data broker laws promote greater transparency by requiring state registration of data brokerage firms[606].

5.2.4 Specific concerns about receiving unwanted email

An individual's email address is unquestionably personal information. The collection and use of this personal information is therefore theoretically subject to the general rules set out in the various laws, including those related to consent. However, Parliament has chosen to deal specifically with the problem of unwanted electronic communications under a separate regulatory regime established by the *Canadian Anti-Spam Act* (*CASA)*. Three entities share responsibility for the enforcement of *CASA*: the Office of the Privacy Commissioner of Canada, the Canadian Radio-television and Telecommunications Commission and the federal Competition Bureau[607]. The involvement of the latter two agencies confirms that the problem is not only viewed as an invasion of privacy, but also as a commercial and technological issue. In fact, privacy is not the focus of the legislative framework. Rather, its purpose is "to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic

---

602 *Ibid.* s. 18 (adding s. 65.0.1(1)(1) to APPIPS).
603 CANADA. Bill C-11, *supra* note 475, Part 1, s. 15(3)(e).
604 SHERMAN, J. "Federal Privacy Rules Must Get 'Data Broker' Definitions Right," LawFare, April 8, 2021, online: https://www.lawfareblog.com/federal-privacy-rules-must-get-data-broker-definitions-right
605 STATE OF CALIFORNIA. California Consumer Privacy Act of 2018, ss. 1798.120 and 1798.115(d).
606 California Civil Code § 1798.99.80; Vermont Statute 9 V.S.A. § 2430.
607 OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "The OPC's responsibilities under CASL," March 2014, online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/canadas-anti-spam-legislation/casl_faqs_2014/

means of carrying out commercial activities[608]." This is reminiscent of *PIPEDA*'s objective, which also refers to economic rather than human rights considerations.

In an effort to limit spamming and the inconvenience it causes to all stakeholders, Parliament has strengthened the protections afforded to consumers with respect to the use of their personal information. Ironically, the consent rules in *CASA* are stricter than those in *PIPEDA*, by prohibiting commercial electronic messages to be sent without the recipient's express or implied consent, with some exceptions (an opt-in system specific to electronic communications[609], whereas *PIPEDA* allows for the general use of an opt-out model, with some exceptions[610]).

Why such a restriction on implied consent for electronic communications, but not for online tracking, for example? Does the federal legislator consider one to be more invasive of individual privacy than the other? Or is this more a confirmation that economic considerations are the determining factor in the choice of a regulatory framework for personal information protection? In one case, the practice is perceived as a nuisance to the proper functioning of the digital economy, while in the other, it seems to be perceived as a necessity.

CASA is subject to similar problems as *PIPEDA* with respect to individual consumer remedies. The coming into force of the provisions related to compensatory and statutory damages that may be claimed by consumers in the event of non-compliance with *CASA* has been suspended since 2017 (the year in which the provisions related to the consent required for sending the communications covered came into force)[611]. There is no indication that legislators intend to bring the provisions into force soon. The consumer is thus, once again, deprived of a useful remedy in the event of a breach of his online privacy.

There have been no changes to *CASA* since 2015.

---

608 CANADA. An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, S.C. 2010, c. 23.
609 CRTC. "Compliance and Investigations Information Bulletin CRTC 2012-549," October 10, 2012, online: https://crtc.gc.ca/fra/archive/2012/2012-549.htm; FEKETE, M. and KARDASH, A. "CASL compliance: More than spam. Understanding Canada's anti-spam law," Osler, online: https://www.osler.com/en/resources/in-focus/casl-compliance-more-than-spam-understanding-canada-s-anti-spam-law (consulted on July 10, 2021).
610 OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. Form of Consent, *supra* note 607.
611 MARUSYK, R. and LANFRANCONI, D. "Canada: Update: CASL Private Right Of Action Suspended, But Be Careful, Other CASL Provisions Are Still Alive," Mondaq, July 20, 2017, https://www.mondaq.com/canada/class-actions/610750/update-casl-private-right-of-action-suspended-but-be-careful-other-casl-provisions-are-still-alive; BRUINEMAN, M. "Fate of controversial CASL," Law Times, March 19, 2018, online: https://www.lawtimesnews.com/practice-areas/privacy-and-data/fate-of-controversial-casl-section-unknown/262966

5.2.5 Specific concerns about damage to Internet users' reputation and psychological and physical integrity

Generally speaking, protecting the reputation and physical and psychological well-being of Internet users is beyond the scope of Canada's frameworks for personal information protection.

Thus, no provision of provincial laws for the protection of personal information deals expressly with the reputation of individuals. Only one reference is made in the federal Act, where damage to an individual's reputation is referred to as a serious injury resulting from a breach of security measures that gives rise to the application of section 10.1 (mandatory reporting of a security breach to the Commissioner and the individual)[612].

The reputation and integrity of individuals online are instead addressed by legislators from the perspective of platform liability, criminal law or civil law (with respect to defamation). Online harassment and the dissemination of intimate content without consent are, for example, covered by provisions in the *Criminal Code*[613]. And legislative changes are expected with regard to the handling of certain hateful or illegal content on online sharing and communication platforms[614].

The choice of legislators to address those issues in separate laws and regulations is apparent. Under federal or provincial laws for the protection of personal information, a victim of damage to his reputation resulting from the use of his personal information will have very few tools to seek redress or even to stop a breach.

Under existing legislation, the right to correction of inaccurate personal information held by an entity, and the requirement that the entity no longer use the personal information once the collection's purpose has been fulfilled, may of course be helpful on occasion. But those measures provide a very imperfect and incomplete remedy. The laws only apply in the context of operating a business or commercial activity, while some websites are intended only for personal non-commercial use. And the purposes for collecting and using information are difficult to delineate over time in the context of social media, where situations that could damage the reputation or integrity of Internet users occur more often than not[615].

Nor do current laws provide specific measures for minors, whose reputation and integrity are at greater risk online. Current provincial legislation does not specify an age at which individuals are (generally) able to fully understand the consequences of their privacy

---

612 PIPEDA, *supra* note 76, ss. 10.1(1) and 10.1(3).
613 See for example: CANADA. Criminal Code, RSC 1985, c. C-46, ss. 162 and 264.
614 PAULS, K. "New rules on removal of illegal online content could help in battle against child pornography," Canadian Broadcasting Corporation, January 4, 2021, online: https://www.cbc.ca/news/canada/manitoba/canada-illegal-online-content-child-porn-1.5847695
615 OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Online Reputation," *supra* note 178.

choices and provide meaningful consent. Neither does federal legislation, but the Office has publicly estimated the age to be 13[616].

5.2.5.1. Changes in Quebec only

None of the provisions proposed in Bills C-11 (Canada) and 64 (Quebec) concern anti-social behaviour such as harassment, threats or other types of anti-social behaviour. The treatment of this problem is therefore separate from the framework for the protection of personal information.

The federal bill also does not include any measures related to the protection of reputation. But the Quebec bill does: It even proposes two significant changes in that regard.

The Quebec bill establishes that a minor under the age of 14 cannot consent to the processing of his personal information and that it is up to the person with parental authority to do so for him[617]. An exception is made where the processing is "clearly for the minor's benefit."

Most importantly, Quebec's Bill 64 establishes a right to deletion and de-indexation[618], inspired by the European *GDPR*. The right to deletion, as its name indicates, consists of a right to the deletion of online content, whereas de-indexation does not affect the content as such, but makes it more difficult to access by not allowing access through a search engine (using the name of the person concerned, for example)[619].

Those rights may be invoked where release of the personal information in question contravenes a law or court order or where it causes serious harm to the privacy or reputation of the individual concerned. The harm caused by the dissemination must clearly outweigh the public interest in knowing the information or the freedom of expression of the person disseminating the information. And the measure requested (cessation of dissemination, de-indexing or re-indexing) must not exceed what is required to prevent the harm from continuing. The bill provides for a series of factors to be taken into account in the assessment (minor, public figure, types and sensitivity of information concerned, etc.).

In doing so, Quebec is taking a broad approach, similar to that developed in Europe. The "right to be forgotten" takes its name from the need for certain individuals to see others forget certain past behaviours. As much as technological progress facilitates and promotes the dissemination of information and access to all its manifestations, it also makes this

---

[616] *A.B.* v *Bragg Communications Inc*, 2012 SCC 46, para. 17; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Guidelines for obtaining meaningful consent," May 2018, online: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/
[617] QUEBEC. Bill 64, *supra* note 474, s. 96 (adding s. 4.1 to APPIPS).
[618] *Ibid.* s. 113 (adding s. 28.1 to APPIPS).
[619] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "Draft OPC Position on Online Reputation," 2018, online: https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-online-reputation/pos_or_201801/

process of "forgetting" more complex, hence the interest in setting up a deletion or de-indexation system[620]. The approach has nevertheless been criticized by some because of the potential infringement of freedom of expression and freedom of the press[621], and because of the great leeway left to the search engine in the evaluation of requests[622].

While recognizing the importance of providing remedies for damage to an individual's reputation online, California has taken a different approach to the "right to be forgotten." For example, the *California Consumer Privacy Act does* not provide for the de-indexing of content; instead, it will be possible to request, without having to provide a reason, the deletion of personal information collected by companies about the individual concerned[623].

Similarly, another California law, the *Online Eraser Law*, allows minors to request the erasure of any personal information that they themselves have posted on a website with which they are registered (e.g. social media platforms)[624]. Once again, the law does not provide any particular condition to be met in order to exercise this right (other than being a minor at the time of the posting).

The absence of a requirement to justify and assess the request's merits ensures speedy processing and, presumably, ease and efficiency of the process, but the California approach may not fully protect individuals' online reputations, particularly given the ease and speed with which content available on social media can be copied and reposted by others[625].

5.2.6 Specific concerns about automated decision-making based on personal information

Automated decision-making based on personal information is not subject to specific provisions in current Canadian legislation[626]. This situation is therefore governed by the general rules concerning the use of personal information with the consent (informed and free) of the person concerned and companies' transparency regarding their personal information handling practices. Artificial intelligence systems that enable this type of data

---

620 NEVILLE, A. "Is it a Human Right to be Forgotten? Conceptualizing the World View," Santa Clara Journal of International Law, vol. 15, No. 2, 2017, p. 170.
621 See on this subject: LEE, E. "The Right to Be Forgotten v. Free Speech," I/S: A Journal Of Law And Policy, vol. 12, No. 1, 2015, online: https://kb.osu.edu/bitstream/handle/1811/80043/ISJLP_V12N1_085.pdf
622 LEAGUE OF RIGHTS. "Mémoire," *supra* note 586, p. 13-14.
623 STATE OF CALIFORNIA. California Consumer Privacy Act, *supra* note 605, section 1798.105(a).
624 STATE OF CALIFORNIA. SB-568 Privacy: Internet: minors (2013-2014) (passed September 2013), Section 22581(1), online: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568
625 DEHGHAN, S. "How does California's Erasure Law stack up against the EU's right to be forgotten?", IAPP, April 17, 2018, online: https://iapp.org/news/a/how-does-californias-erasure-law-stack-up-against-the-eus-right-to-be-forgotten/
626 SOOKMAN, B. B., MORGAN, C. S. and GOLDENBERG, A. "Using privacy laws to regulate automated decision making," McCarthy Tétrault, April 30, 2021, online: https://www.mccarthy.ca/en/insights/blogs/techlex/using-privacy-laws-regulate-automated-decision-making

processing represent a challenge for law enforcement[627], as explained above. Moreover, this type of personal information handling poses additional risks to human rights (including the right to non-discrimination)[628].

Currently, a Canadian consumer who refuses the automated processing of his personal information for the purpose of making a decision about him also has to give up the good or service offered by the company. Unfortunately, there is a risk that consumers will consent to such processing without really understanding what it is all about, due to the lack of transparency obligations specific to this type of complex data processing.

5.2.6.1 More transparency proposed

Considering the development and deployment of this type of personal information handling since the adoption of Canada's four laws for the protection of personal information in the private sector in the early 2000s, it is hardly surprising to observe the integration of significant amendments in this regard into Bills 64 and C-11, introduced in 2020.

It should be noted that neither bill retains the following key element of the *GDPR*: the general prohibition on making decisions that produce legal effects for data subjects solely on the basis of the automated processing of their personal information[629]. This prohibition is subject to numerous exceptions, of course, but remains central to the European framework.

Instead, Canadian legislators have chosen to focus on the transparency of companies that proceed in this way and, ultimately, on recognition of a right to explanations for the individuals affected by the decisions. An individual who wants to avoid an automated decision based on personal information that has already been collected should therefore turn to other solutions:

> Under the CPPA [*Consumer Privacy Protection Act*: short name for one of the laws proposed in Bill C-11], any such right would need to be exercised through the right to withdraw consent or the right to be forgotten – which would be at best an indirect and more complicated avenue to achieve such this result[630].

---

627 INNOVATION, SCIENCE AND ECONOMIC DEVELOPMENT CANADA. "Strengthening Privacy in the Digital Age. Proposals to Modernize the Personal Information Protection and Electronic Documents Act," 2019, online: https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html

628 COFONE, I. "Policy Proposals for PIPEDA Reform to Address Artificial Intelligence Report," Office of the Privacy Commissioner of Canada, November 2020, online: https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pol-ai_202011/

629 GDPR, *supra* note 54, art. 22(1); "ARTICLE 29" DATA PROTECTION WORKING PARTY. "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679," 17/EN WP251rev.01, p.19: "The term 'right' in the provision does not mean that Article 22(1) applies only when actively invoked by the data subject. Article 22(1) establishes a general prohibition for decision-making based solely on automated processing. This prohibition applies whether or not the data subject takes an action regarding the processing of their personal data."

630 YOUNG. "New federal privacy law," *supra* note 598.

It should also be noted that both bills provide for a broader application of the rules than the *GDPR*. The federal provisions apply whenever an organization has used automated data processing to make a prediction, recommendation or decision about an individual [631]. The Quebec provision applies to decisions based exclusively on the automated processing of personal information[632]. But unlike the European framework, neither bill requires that those decisions produce legal effects or significantly affect the person concerned[633]. And the federal framework extends to predictions and recommendations based on automated processing of personal information, in addition to decisions.

Both bills require companies to provide explanations to the individuals concerned, upon request, as to the decision and the personal information used to make it[634]. The Quebec bill specifies that those explanations must also include the main factors and parameters that led to the decision[635]. Bill C-11 also provides that prior to the processing of personal information, explanations must be given as to the use that the company intends to make of automated decision-making systems in order to make predictions, recommendations or decisions about individuals[636]. The federal legislators thus adopt a dual approach by recognizing an individual right to *ex ante* and *ex post* explanations[637].

The transparency and explanation obligations aim above all to develop algorithmic responsibility in a context of rapid development of artificial intelligence systems[638]. But the *GDPR* goes further by allowing individuals to make representations to the company regarding a decision made about them and to obtain human intervention from the data controller[639]. We don't find an equivalent in Bills 64 and C-11, despite a recommendation to that effect by the Office of the Privacy Commissioner[640]. And yet, the *GDPR*'s measure is

---

631 CANADA. Bill C-11, *supra* note 475, Part 1, ss. 2 and 63(3).
632 QUEBEC. Bill 64, *supra* note 474, s. 102 (adding s. 12.1 to APPIPS).
633 GDPR, supra note 54, art. 22(1).
634 CANADA. Bill C-11, *supra* note 475, Part 1, s. 63(3); QUEBEC. Bill 64, *supra* note 474, s. 102 (adding s 12.1(2)(1) and (2) to APPIPS).
635 QUEBEC. Bill 64, *supra* note 474, s. 102 (adding s. 12.1(2)(2) to APPIPS).
636 CANADA. Bill C-11, *supra* note 475, Part 1, s. 62(2)(c).
637 The author Gianclaudio Malgieri associates this approach with the concept of "legibility": MALGIERI, G. "Automated decision-making in the EU Member States: The right to explanation and other 'suitable safeguards' in the national legislations," Computer Law & Security Review, vol. 35, No. 5, 2019, p.4, online: https://www.researchgate.net/publication/334359463_Automated_decision-making_in_the_EU_Member_States_The_right_to_explanation_and_other_suitable_safeguards_in_the_national_legislations; see also: MALGIERI, G. and COMANDÉ, G. "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation," International Data Privacy Law, vol. 7, No. 3, November 2017, online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3088976
638 WACHTER, S. and MITTELSTADT, M. "A right to reasonable inferences: re-thinking data protection law in the age of Big data and AI," Columbia Business Law Review, 2019, online: https://www.researchgate.net/publication/327872087_A_RIGHT_TO_REASONABLE_INFERENCES_RE-THINKING_DATA_PROTECTION_LAW_IN_THE_AGE_OF_BIG_DATA_AND_AI
639 GDPR, supra note 54, art 22(3).
640 OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. "A Regulatory Framework for AI: Recommendations for PIPEDA Reform," November 2020, online: https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/reg-fw_202011/

associated with the recognition of another right essential to human dignity: the right to be subject only to reasonable inferences[641].

As proposed by the bills, explanation of a decision does not amount to justification of the decision or of the inferences on which it is based. The possibility for individuals to make representations to challenge the validity of an automated decision therefore seems desirable. Authors such as Wachter and Mittelstadt also recommend additional requirements for a company to establish how the processed data constitute an acceptable basis for drawing inferences (accuracy and statistical reliability of the methods used) and how those inferences are relevant and acceptable for the types of automated decisions involved[642]. It does not appear that the requirement for a general explanation of the decision and of the information used, as written in both bills, extends to that specific information.

Moreover, the right to obtain explanations about the automated processing and the decision made is partly explained by the corollary right to challenge the decision, according to the European advisory body (Article 29 Data Protection Working Party):

> The data subject will only be able to challenge a decision or express their view if they fully understand how it has been made and on what basis[643]

By adopting only one of the two components, even though they are complementary, Canadian legislators are leaving Canadian Internet users vulnerable to the automated processing of their personal information for decision-making purposes.

5.3 Are the Laws Consistent with Consumer Behaviour?

5.3.1 Consumer responsibility

In their desire not to stifle innovation but to satisfy the needs of business in the handling of personal information, Canadian legislators are placing much of the responsibility for protecting their privacy on the shoulders of consumers themselves. While the law imposes certain obligations on businesses to handle personal information, it's often ultimately up to consumers to determine whether or not they consent to the collection or other handling of that information. To that end, it's up to them to become aware of, understand and analyze company practices and the risks they represent, and to assess the price of their consent and the relative value of the benefits it brings. While many Canadian survey respondents were aware of the significant responsibility they currently have, it was less clear that they

641 WACHTER. "A right to reasonable inferences," *supra* note 638.
642 *Ibid.*
643 ARTICLE 29 DATA PROTECTION WORKING PARTY. "Guidelines on Automated individual decision-making," *supra* note 643, p. 16.

were exercising that responsibility with the appropriate level of judgment; many felt that they needed to "do more." But should this burden imposed on them by business – with the endorsement of legislators – fall to them? The views of our interviewees and the authors seem to be quite divided.

The current approach of Canadian legislators is more in keeping with a perspective of the right to privacy as an individual right that each person exercises as he wishes (provided that he can actually exercise it freely). There is a growing chorus of voices advocating a more collective perspective on this right, which would have the potential effect of shifting more responsibility to the state in its control of company practices (either through legislation itself or through monitoring and enforcement authorities).

Bills C-11 and 64 make certain additions that have the effect of placing more responsibility on the shoulders of businesses, notably through the implementation of stricter security and assessment measures[644], but consumer consent remains central. Thus, the division of responsibility between stakeholders in the federal and Quebec legislation is relatively unchanged.

To reduce the burden on consumers to protect their online privacy, government has a number of options that involve shifting that burden to government or to businesses. Here are some examples of possible approaches.

5.3.1.1 An Increased role for the private sector (and government): certification programs

Making consumers bear almost all the responsibility for protecting their privacy online by exercising their right to consent is hardly justified, given the way this right is unfortunately exercised in practice. It would not be wise to leave that responsibility entirely to businesses, whose knowledge and understanding of the current framework tends to be poor[645]. That leaves government, whose role must strike a balance between interference and passivity in the face of company practices.

> A variety of problems plague the exercise of decision-making competence in the data protection field regardless of where that competence is placed. It would seem that the solution to these problems cannot lie in providing either data subjects or data controllers with even more decisional power. At the same time, reverting to a comprehensive licensing scheme administered by DPAs [Data Protection Authorities] seems unrealistic. An important question then is whether decision-making competence can be reorganized in another way that mitigates these problems[646].

---

[644] Consider, for example, the risk assessment that a business would have to perform henceforth before implementing any information system or electronic service delivery that involves personal information handling: QUEBEC. Bill 64, *supra* note 474, s. 95 (adding s. 3.3 to APPIPS).
[645] BYGRAVE. "Consent," *supra* note 492, p. 4.
[646] *Ibid.*, p.5.

Certification programs that "pre-approve" the personal information handling policies and practices of participating companies are potentially a middle ground. The programs reduce the risk to a consumer who has not made (or been able to make) an informed choice about a company's handling of personal information. They reduce the complexity of the required analysis by the consumer, by promoting a standardization of practices within certain sectors. They also help educate companies about the legality and legitimacy of their practices. And they are monitored and approved by the authorities, which gives them additional credibility and seriousness.

Some European states, such as Norway, Sweden and France, have in the past required companies to obtain licences in order to undertake certain types of personal information handling. The demise of those programs is largely due to the significant resources required of authorities to support the operation of such a model[647]. Certification programs that are privately run but legislated also address this problem (although the underfunding of protection authorities remains a problem that goes well beyond this issue). They also give the final say back to consumers (who still have to provide consent), which was not the case in the licensing era[648].

That is precisely what Bill C-11 proposes by granting the Office of the Privacy Commissioner the power to approve potential certification programs developed by private entities[649]. It should be noted that this new rule is once again perfectly in line with Canadian federal legislators' desire to help businesses comply with the law rather than punishing or even deterring them.

5.3.1.2 An Enhanced role for government: upstream prohibition of certain dangerous ways of handling personal information

A more drastic way to reduce the pressure on consumers regarding consent is to directly prohibit companies from adopting certain personal information handling practices that would be deemed unacceptable by society (and consequently by legislators) and that consumer consent could wrongly legitimize. Some authors draw an analogy with seat belts in cars:

> Policy intervention is motivated to the extent that people are poor navigators. Much as seat belts in cars are justified by the fact that people's natural driving habits (as well as those of other drivers) create an unacceptable level of risk, privacy interventions can be justified by similar limitations of individuals' abilities to manage privacy-related risks[650].

---

[647] *Ibid.*, p.3.
[648] *Ibid.*, p.3.
[649] CANADA. Bill C-11, *supra* note 475, Part 1, arts. 76-81.
[650] BRANDIMARTE, L., ACQUISTI, A., and LOEWENSTEIN, G. "Misplaced Confidences: Privacy and the Control Paradox," Social Psychological and Personality Science, vol. 4, No. 3, 2012, online: https://www.cmu.edu/dietrich/sds/docs/loewenstein/MisplacedConfidence.pdf

This approach has not been adopted by Canadian legislators, who, by relying instead on consumers' ability to choose, ignore the risks to which they unfortunately expose themselves. Other legislatures have made different choices. The European Union, for example, has chosen to prohibit the automated processing of personal information for the purpose of making a significant decision about the data subject[651] (although there are multiple exceptions to this prohibition)[652]. According to the *GDPR* guidelines, this prohibition is explained by the risks to the rights and freedoms of individuals potentially affected by the practice[653]. The European Union is also considering banning personal information handling that uses artificial intelligence to establish a social credit score[654] because of the risks of exclusion and discrimination posed by that practice[655].

Another practice is regularly singled out by human rights and Internet advocates as socially reprehensible: the processing of personal information for targeted advertising[656]. In February 2021, European Data Protection Supervisor Wojciech Wiewiórowski publicly encouraged European lawmakers to ban targeted advertising based on data obtained through invasive online tracking [657]. A U.S. coalition that includes some 40 advocacy groups such as the American Economic Liberties Project, the Center for Digital Democracy, the Center for Humane Technology and Public Citizen is also lobbying the U.S. Congress[658].

5.3.2 Consumer inertia

Studies and surveys, including our own, tend to show a certain inertia among Internet users here and elsewhere with respect to the protection of their personal information. They feel powerless in the face of the current handling of their personal information and generally have no intention, desire or ability (perceived or real) to improve things.

How can Canadian legislators take this reality into account in developing reforms and what did they learn in producing Bills C-11 and 64?

---

651 GDPR, supra note 54, art 22(1); ARTICLE 29 WORKING PARTY. "Guidelines on Automated individual decision-making," *supra* note 643, p. 19.
652 GDPR, supra note 54, art 22(2).
653 SECTION 29 WORKING GROUP. "Guidelines on Automated individual decision-making, *supra* note 643, p. 9.
654 EUROPEAN PARLIAMENT. Proposal for a Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts, 21 April 2021, COM/2021/206, Title II, art 5(1)c).
655 *Ibid.,* preamble, para. 17.
656 See for example: MAHDAWI, A. "Targeted ads are one of the world's most destructive trends. Here's why," The Guardian, November 5, 2019, online: https://www.wired.com/story/why-dont-we-just-ban-targeted-advertising/; https://www.theguardian.com/world/2019/nov/05/targeted-ads-fake-news-clickbait-surveillance-capitalism-data-mining-democracy
657 WOOLLACOTT, E. "European Regulator Calls For Ad Targeting Ban," Forbes, February 21, 2021, online: https://www.forbes.com/sites/emmawoollacott/2021/02/11/european-regulator-calls-for-ad-targeting-ban/?sh=6b0a4ec82523
658 Ban Surveillance Advertising" campaign, online: https://www.bansurveillanceadvertising.com/ (consulted on September 10, 2021); LOMAS, N. "US privacy, consumer, competition and civil rights groups urge ban on 'surveillance advertising'," TechCrunch, 22 March 2021, online: https://techcrunch.com/2021/03/22/us-privacy-consumer-competition-and-civil-rights-groups-urge-ban-on-surveillance-advertising/

5.3.2.1 Privacy protection by default and "nudges"

Legislators can implement "privacy nudges" for consumers that reduce the negative effects of their passivity regarding their online privacy. Soh offers the following definition of the concept:

> "Privacy nudges" stem from the use of soft paternalism to nudge users towards improved decision-making in the context of privacy, that is, to make them more "privacy sensitive" or in a manner that reduces users' regret[659].

This approach is not without its critics, especially because of the manipulation it implies (it actively encourages certain choices)[660], but it does have the advantage of preserving a certain degree of autonomy for the consumer[661].

One example of a nudge is the implementation of default settings favourable to consumers. The consumer is free to consent to a lower level of confidentiality, but if he fails to do so, the highest level of confidentiality, offered by the company's default settings, must be applied. A provision of this type is found in Quebec's Bill 64[662]. This type of nudge is easily explained: Studies show that the default option will generally be the one that is maintained, either by choice or by inertia. Willis identifies a few reasons why defaults are the most popular choice, including :

- The time required to change the settings[663] (*transaction barrier*)
- Confusion caused by the default settings (what they represent and how much leeway is given to consumers)[664];
- The tendency to feel less responsible for the consequences of inaction than for the consequences of action[665] (*omission bias*)
- The tendency to prefer to avoid making decisions[666] (*decision avoidance*)
- Perception of the default settings as an implicit recommendation from a more informed party[667].

In adopting a default privacy model, Quebec legislators are aware of that consumer bias and seem to recognize at the same time (for once) that the right to protection of one's personal information should take precedence over the economic considerations of

---

[659] SOH, S. Y. "Privacy nudges," *supra* note 491, pp. 67-68.
[660] *Ibid.,* p. 73.
[661] SOLOVE, D. J. Privacy Self-Management, *supra* note 502.
[662] QUEBEC. Bill 64, *supra* note 474, s. 100 (adding s. 9.1 to APPIPS).
[663] WILLIS, L. E. "Why Not Privacy By Default?," Berkeley Technology Law Journal, vol. 29, No. 1, 2014, p8, online: http://nrs.harvard.edu/urn-3:HUL.InstRepos:11266829
[664] *Ibid.*, p. 9.
[665] *Ibid.* pp. 11-12.
[666] *Ibid.* pp. 12-13.
[667] *Ibid.,* p. 16.

businesses (for whom maximum protection by default is not to their advantage). But as with the rest of the legislative framework in place, the needs of businesses are not entirely ignored. And Quebec legislators are doing them a favour in Bill 64 by not including the related, but more stringent, requirement of confidentiality by design, as provided for example in the *GDPR*[668]. Nor is this principle (or the principle of maximum confidentiality by default, for that matter) found in the federal Bill C-11.

Similarly, the adoption of an opt-in model (discussed above) with respect to consent required from consumers whose personal information a company intends to collect and process could adequately address consumer inertia regarding online privacy. Consumers would no longer be penalized for maintaining the status quo. Unfortunately, the two 2020 bills don't move toward this model.

5.3.2.2 Consent obtained by subterfuge

Nevertheless, Bill C-11 prohibits the use of deception (i.e., the use of a deceptive or misleading practice or the provision of false or misleading information) to obtain a consumer's consent[669]. We don't find an equivalent prohibition in Alberta, B.C. and Quebec laws (or in the Quebec bill), although they do provide that the consent provided must be free and informed, which should naturally restrict the manner in which businesses obtain it.

By adding such a provision to its bill, federal legislators are acting on two fronts. They are trying to make the existing framework more effective by reducing the risk that what happened in Europe will happen in Canada – industry's repeated attempts to circumvent the framework provided in the *GDPR* since it came into force[670]. And the provision responds to the observable behaviour of online consumers (often apathetic and more easily influenced).

Forbrukerrådet, the Norwegian Consumer Council, produced a detailed study in 2018 on the use of those *dark patterns* by companies in Europe. Among other things, the study identifies the widespread practices of making certain consent options inconspicuous (by playing with colour or location), describing the most stringent confidentiality options in a pejorative or guilt-inducing way (this practice is sometimes referred to as *confirmshaming*), and imposing additional steps on consumers who want to opt out of the collection of personal information, for example, as compared to those who opt in[671]. Unfortunately, the provision in Bill C-11 likely does not cover all such practices.

---

[668] GDPR, supra note 54, art 25(1); for more on the principle of privacy by design: KREBS, D. "'Privacy by Design': Nice-to-have or a Necessary Principle of Data Protection Law?", Journal of Intellectual Property, Information Technology and E-Commerce Law, vol. 4, No. 1, 2013, online: https://www.jipitec.eu/issues/jipitec-4-1-2013/jipitec4krebs/jipitec-4-1-2013-2-krebs.pdf

[669] CANADA. Bill C-11, *supra* note 475, Part 1, s. 16.

[670] See, for example, NOUWENS, M. *et al*. "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence," January 8, 2020, CHI '20 CHI Conference on Human Factors in Computing Systems, 2020, online: https://arxiv.org/abs/2001.02479

[671] FORBRUKERRÅDET. "Deceived by design," June 27, 2018, p. 12 and fol, online: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

WHAT EXPERTS SAY

In summer 2021, we spoke with two Canadian university professors who specialize in the protection of personal information online, to get their perspectives on some of the issues raised in this study[672].

The views reported in this chapter, gathered through telephone and video conference interviews[673], are those of:

- Dr. Céline Castets-Renard[674], full professor at the University of Ottawa Faculty of Law (Civil Law Section) and holder of the University of Ottawa Research Chair on Accountable Artificial Intelligence in a Global World and of the Law, Accountability, and Social Trust in AI Chair (associated with the Université fédérale Toulouse Midi-Pyrénées). She has taught several courses on personal data protection, notably from a comparative law perspective.
- Dr. Ignacio Cofone[675], assistant professor at McGill University's Faculty of Law, where he teaches courses on the regulation of artificial intelligence and the handling of personal information. He has published several articles on personal information protection and is currently working on the courts' conceptualization and evaluation of privacy violations[676].

6.1 What General Approach Should Canadian Legislators Take?

From the outset, the two researchers support the position of the Office of the Privacy Commissioner of Canada, which advocates a more human rights-based approach in Canadian laws regarding the protection of personal information in the private sector.

For Dr. Castets-Renard, the addition of a provision that explicitly recognizes the right to protection of personal information would provide leverage for the courts, thus making it easier for them to punish abuses. Using the image of an umbrella, she wants judges (and consumers) to be able to rely on a more general legal provision to recognize a violation of

---

672 We contacted several Canadian researchers. Two ultimately agreed to our requests for interviews. We also invited the privacy offices, to no avail. A summary of our research highlights was sent to respondents prior to the interviews.
673 In addition to talking with us by phone, Dr. Cofone provided additional answers in writing and referred us to some of his articles and research for additional context.
674 UNIVERSITY OF OTTAWA. Biography of Céline Castets-Renard, online: https://droitcivil.uottawa.ca/en/people/castets-renard-celine
675 COFONE, I. Personal website, online: http://www.ignaciocofone.com/
676 COFONE, I. "Privacy Standing," University of Illinois Law Review, 2022, online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782887

privacy rights when the more specific rules fail to do so (particularly in the context of technological advances and artificial intelligence). She argues that the lack of such recognition in *PIPEDA* is currently detrimental to Canadian consumers, especially given the complexity of interpreting the legislation in light of the variety of its purposes (many of which are economic).

The two researchers cite the rights-based approach of the *GDPR* as an example, but at the same time point out the need to adapt it to the Canadian legal context, particularly because European law recognizes two distinct fundamental consumer rights, privacy protection and the protection of personal information, unlike Canadian law, which makes it more difficult to distinguish between the two.

6.2 What Is Each Party's Responsibility?

While there is a need to focus the law more on respecting fundamental rights, there is also a need to rethink the responsibility of each party in protecting personal information online, according to the experts consulted.

The burden on Canadian consumers, for example, appears disproportionate. The analysis and choices expected of them are hardly realistic and ultimately make it somewhat utopian to implement the specific rights provided for in the law. To illustrate his point, Cofone refers to the difficulties expressed by judges in assessing damages following an invasion of privacy in the context of class actions (difficulties so significant that some cases are dismissed). How then can we ask the average consumer, who has no particular knowledge of legal and technological matters, to make that same assessment, when the infringement may still be uncertain at that time?

One way to reduce the burden of responsibility on consumers is to increase the responsibility of businesses. According to Cofone, the drafting of federal legislation in the form of principles rather than clear obligations currently exacerbates the lack companies' accountability in this country with respect to their handling of consumers' personal information. He thinks we need to build on the *GDPR* and put the onus on organizations to demonstrate compliance. That obligation would be beneficial on several fronts: It would strengthen the compliance of companies' practices, facilitate the work of supervisory authorities and bring about a change in culture that would ultimately strengthen public confidence. More specifically, the professor referred to the notion of data traceability, i.e., companies' recording and documentation of their collection and handling of personal information, in order to report the practice to the authorities, when required. Castets-Renard emphasizes companies' ongoing responsibility regarding subcontractors who come into contact with the personal information collected (the choice of contractors, information security, contractors' compliance, etc.). Like Cofone, she points to European advances in this area.

Government responsibility was also raised in the discussions. For Castets-Renard, the processing of certain types of personal information (such as sensitive information) requires a much stricter regime, because it presents greater risks to human rights. The development and implementation of this additional framework is the responsibility of government, which must be more proactive.

6.3 To What Extent Should We Draw on Foreign Reforms?

Not surprisingly, both researchers believe that Canadian legislators should draw heavily on European regulatory frameworks, because they are interesting and useful, but also because of what Castets-Renard calls "legal colonialism." Given Europe's economic and political weight, *GDPR* principles have been adopted by several other countries. Those principles have since become global standards that Canada must meet, particularly to ensure the sustainability of its trade with the old continent.

So how can the *GDPR* be used as a model? Both researchers think the European regulation's text cannot simply be copied. Some of the underpinnings of Canadian laws differ, including the fact that they don't take a fundamental rights approach and don't conceive of privacy rights in exactly the same way. Moreover, the *GDPR* dates back to 2016 and, while it's undeniably a successful reform, there have been some weaknesses and implementation difficulties since then. For Cofone, Bill 64 is an excellent adaptation of the *GDPR* in addressing such weaknesses, including those related to the automated processing of personal information to make decisions about data subjects.

Castets-Renard also stresses the importance of not forgetting the European provisions that give national authorities significant powers to enforce the *GDPR* and related national laws. Without a strong authority, the transposition of European principles (rights and obligations) to Canadian soil may unfortunately only be theoretical.

The two researchers don't look favourably at the possibility that Canadian legislators will be inspired by the American framework for the protection of personal information. The more sectoral and regional nature of the American framework must be avoided at all costs in Canada, in their view. Instead, we should focus on standardizing the rules across the country, so that consumers and businesses can better understand them. Castets-Renard thinks that the regional differences revealed in our survey with respect to the level of concern of Canadian Internet users about the protection of their privacy online do not justify differentiating the framework according to province. Everyone faces the same issues and risks. Rather, it's important that consumers from all walks of life are aware of them, which can be achieved through public education efforts.

6.4 How to Take Technological Advances into Account?

Since the law cannot be continually amended to adapt to rapid technological developments, it was suggested that (technology-neutral) guiding principles such as the necessity, purpose and minimization of personal information collection and use should be put in place or reinforced. According to Castets-Renard, the presence of those guiding principles in Canadian law should be strengthened. The principles, which must guide a company in all stages of interpreting and applying the law, have the advantage of simplifying the recognition and identification of a violation of individual rights.

Both professors also emphasize the importance of privacy impact assessments (PIAs in Canada or DPIAs in Europe) in the context of AI deployment, while recognizing that they should not be an undue burden on businesses, especially SMEs. Cofone further argues that those obligations are not an end in themselves, but a way to help companies implement their broader responsibilities regarding personal information protection.

Lastly, the researchers think that certain issues related to the protection of personal information online, such as the use of artificial intelligence and online cookies, should be addressed in separate legislation or regulations. Castets-Renard said *PIPEDA* and its provincial equivalents are insufficient to address the various issues facing Internet users today. Ultimately, Canada is doing poorly, considering the extent of the digital law framework developed in Europe.

6.5 What to Do about Consent?

Both professors are critical of the emphasis on consent in Canadian law. It does not seem realistic or reasonable to expect consumers to make informed choices in the current context. The asymmetry of power and knowledge between the parties is too great, and it is almost impossible for consumers to assess the benefits and risks of the handling of their personal information, especially given the unpredictable nature of artificial intelligence processing[677].

Cofone thinks the current requirement to obtain consent prior to handling personal information creates a false sense of control among consumers. Automatically checking the "Yes, I agree" box at the bottom of a Web page is not indicative of any real power, he emphasizes. Castets-Renard shares his view and also stresses the absolving nature of this consent-based approach for companies. Strengthening companies' transparency obligations is not at all perceived as a solution to these problems.

Both refer to the European regulatory framework, in which consent is only one legal basis among others for the handling of personal data (and is not the basis used in the majority

[677] COFONE, I. "Policy Proposals for PIPEDA Reform," *supra* note 628.

of cases). Should a similar model be adopted in Canada? Castets-Renard is in favour of abandoning the exclusive importance of consent, a standard whose application seems hypocritical in Canada, given all the exceptions in place (in addition to those proposed in the bills). Cofone also considers that the importance of consent in the Canadian legal framework should be diminished in order to reduce the unrealistic pressure on consumers and to make businesses more accountable in their personal information handling practices. But both researchers stress the importance of establishing a parallel framework for using consent (through guidelines, for example) as well as safeguards and precautions for handling personal information without the consent of the individuals concerned.

6.6 What Future for the 2020 Bills?

The two professors don't fully agree on the next steps to modernize Canada's private sector privacy laws.

Both are satisfied with Quebec's Bill 64, which they consider closer to the *GDPR* and more beneficial to consumers than the federal bill. At the time of the interviews (in the summer of 2021), they were hoping for its rapid adoption and emphasized the importance of adopting the Quebec reform as the first of its kind in the country, and as likely to stimulate and guide the subsequent modernization of other Canadian laws, since a certain standardization of the framework across Canada is essential. It should be noted that the Quebec bill has since been adopted.

But the two professors have differing views on the federal Bill C-11. With an election due in September 2021 before the bill's adoption, it died on the order paper. Should the federal government reintroduce it?

On the one hand, Castets-Renard believes it is better to continue working on the basis of the text of Bill C-11, and therefore to re-table it for quick adoption. She expressed disappointment with the draft and would support a complete rewrite, in an ideal world, but believes that the political reality is that a modest and somewhat unsatisfactory reform should be passed quickly and with certainty, rather than the uncertain and distant passage of a better reform of the federal law. She is concerned that if the reform proposal is substantially revised, it could take several years to introduce and pass a new bill, further delaying the Canadian legislative framework in comparison with the European regulatory framework. In a nutshell, small changes are better than no changes in the short term!

Cofone thinks it's better to do it right, even if it takes a little longer to get reform. He points out that if the text of C-11 is adopted, the next reform of this new law is likely to be many years away. He's not comfortable with the idea that the new law could apply until 2040 or even later, so he favours a complete rewrite of the bill.

In the end, both researchers share the same concerns: the foreseeable unwillingness of federal lawmakers to rework these issues in the short term and the likely slowness of their efforts to reform or update *PIPEDA*. However, they propose a very different response.

CONCLUSION

> Digital citizens live in a world which they cannot see, do not understand and are unable to direct. In the cold light of experience the digital citizen knows that data privacy self-management is a fiction.
>
> Jonathan A Obar[678]

What does it mean to protect one's privacy in 2021? For some, it means being out of sight. For others, it means having choice and control over who watches them, who has access to their personal information and what information specifically, and what they can do with it. For still others, it is about maintaining their ability to make important decisions about their lives, without interference from others. All of these conceptions are valid; there is no universal definition of privacy, so everyone adopts his own definition. Privacy protection is therefore a highly subjective exercise.

The conception of individual privacy protection must also take into account the environment in which the individuals who claim it live. In 2021, taking the Internet into account is essential to any reflection on the subject. The Internet makes it easier for businesses and individuals to collect, access and share personal information, through social media and browser cookies, for example. New technologies, including those using artificial intelligence, then allow for a variety of information processing that was unimaginable just a few years ago, based on a colossal amount of data. The advent and democratization of Internet use have thus brought about a staggering change of scale. Whereas it was once costly and relatively useless for companies to collect and retain their customers' personal information, the opposite is now true. We are seeing the emergence of an economy based on the exploitation of this type of information.

In this context, it is hardly surprising that the results of surveys conducted among consumers here and elsewhere show an ever-increasing level of concern about their online privacy. Many say they are deeply concerned, but feel powerless, convinced that they can't really make a difference, that their personal information is destined to end up at the mercy of companies, governments and hackers, no matter how hard they try to avoid it. The results of the cross-Canada survey and interviews conducted in 2020 also raise concerns about consumers' low awareness of the risks to their privacy online and about the lack of protective behaviours they adopt.

This report focuses on two major defensive weapons available to consumers in their quest for online privacy: laws for the protection of personal information online in the private sector

---

[678] OBAR, J. A. "Big Data and The Phantom Public: Walter Lippmann and the fallacy of data privacy self-management," Big Data & Society, vol. 2, No. 2, October 2015, p. 1, online: https://www.researchgate.net/publication/283438170_Big_Data_and_The_Phantom_Public_Walter_Lippmann_and_the_fallacy_of_data_privacy_self-management

and online privacy enhancing technologies. Both currently have significant weaknesses and do not ultimately allow Canadian consumers to have the final say in how companies handle their online personal information.

Regarding online privacy enhancing technologies, the problems are mostly related to consumers' very low awareness of the subject. Relatively few Canadians are aware of private search engines, private browsers, password managers or virtual private networks, which could address some of their concerns. And even fewer have ever used them! The technologies' contribution remains marginal. And discussions about them are difficult. Consumers are suspicious. They doubt the technologies' operation and effectiveness. They don't feel competent to use them. When they try to find out about them, few resources are able to explain what kind of tools they need to address their concerns. And when they do come across the websites of some providers, the latter are unable to provide adequate information or reassurance because the documentation is either too incomplete or too complex to be accessible. French-speaking consumers are at a serious disadvantage, often being confronted with websites that are entirely or partially unilingual English. It is therefore not surprising that the lack of knowledge of these technologies is particularly marked among French-speaking consumers. This report does identify some providers' good consumer awareness and education initiatives. The other providers would benefit from being inspired by them. Consumers would also gain a lot.

But it's unrealistic to think that all consumers have or will have the desire or ability – even with increased efforts to educate them – to find and then use privacy enhancing technologies so as to further protect their online privacy. Ultimately, those technologies are only complementary tools; the real consumer protections are in the law. At least in theory.

In theory indeed, because the four laws in force in this country that apply to businesses have significant limitations in their application that make some of the rights they provide somewhat utopian, unfortunately. The most glaring example is undoubtedly what is still the central element of those laws, namely consumers' right to control the handling of their personal information by a business. How can they exercise this right if they are unable to understand and evaluate the practices of a company requesting their consent, if they are not able to negotiate with the company or to refuse its request without having to give up access to the goods, services or content it offers? Consumer consent is often neither informed nor free. The current situation – generalized daily acceptance, through automatism, ignorance or powerlessness, but very rarely by real choice, of the terms of service of myriad websites – is certainly not a display of power held by Internet users thanks to the prior consent requirement.

The difficulties of enforcing consent due to the unequal balance of power between the parties have always existed, but appear all the more important in the digital and data economy. Generally speaking, in fact, the current laws for the protection of personal information in the private sector are more difficult to apply to online business practices. Why? If those laws are technology-neutral, i.e., if they apply as much offline as online, they were simply not designed for the Internet. They were passed between 1993 and 2003 and

have not been significantly reformed since, despite the ever-growing loss of control by online consumers.

So here we are in 2021. Major challenges await Canadian legislators in modernizing privacy laws for the protection of personal information in the private sector. Some have already begun the exercise, as demonstrated by the Quebec and Canadian government bills, which are inspired, although not always sufficiently, by the major European reform of 2016. Some specific concerns of Canadian consumers in the digital context are addressed. Others unfortunately remain unaddressed…

The Quebec bill was recently adopted (September 2021). The federal bill died on the order paper. The federal government will have to reintroduce a *PIPEDA* reform bill. Hopefully, two elements will be included this time that are key to effective protection of consumers' personal information: an approach centred on the recognition and protection of human rights; and an obligation for businesses to offer the highest level of personal information protection by default. The fiction of control pointed out by Professor Obar cannot continue.

Surprisingly weak links between actors

This report leads to another conclusion. There is a clear disconnect between the concerns and actions of consumers, businesses willing to help them, and government. Consumer protection needs are not necessarily being met by the providers of online privacy enhancement tools. Consumers say their concerns are not addressed by current laws or are not treated as seriously as they should be. And certain fundamental principles of those laws appear incompatible with consumer behaviours or reflexes.

Yet it's difficult to put all the blame on government. Consumers don't always make it easy for government. They say they're concerned, but find it very difficult to offer any explanation of what they're actually concerned about. They say they're concerned about online profiling, for example, but don't know what it is in practice. They're oddly confident that their privacy is adequately protected online, while at the same time admitting that they know very little about the risks to it. They don't want or feel empowered to change their online behaviour, even though they believe their fellow citizens should do so. It's hard to understand these consumers!

Government also appears somewhat confused. It claims to be protecting a fundamental right, but regularly gives the last word and apparently attaches the main importance to the economic interests of business (despite the catchy title of some laws). It adopts a conception of privacy based on control of personal information, but in practice grants relatively little control to the individuals concerned.

In short, the various stakeholders all have a role to play in protecting online privacy, but currently seem to be acting in different plays…

RECOMMENDATIONS

Recommendation 1

Whereas the Internet has a significant impact on the exercise of consumers' right to privacy;

Whereas the Internet jeopardizes the right to privacy, including the protection of individuals' personal information;

Whereas several major thefts and leaks of personal information have occurred in recent years, particularly as a result of computer system hacking;

Whereas the general level of concern for online privacy is relatively high among Canadian consumers;

Whereas laws for the protection of personal information in the private sector were enacted over 20 years ago and have been subject to very few amendments since;

Whereas new technologies have profoundly changed the way personal information is collected, used and retained by businesses;

Whereas some rules provided in laws for the protection of personal information in the private sector are not adapted to current practices for handling personal information online;

UNION DES CONSOMMATEURS RECOMMENDS THAT CANADIAN LEGISLATORS:

Promptly reform the (federal and provincial) laws for the protection of personal information in the private sector to better reflect the needs of consumers and the realities of the Web and new technologies.

Recommendation 2

Whereas the Internet is a global network that does not stop and is not limited to countries' physical borders;

Whereas many foreign countries have enacted new laws for the protection of personal information in recent years;

Whereas the *General Data Protection Regulation* (*GDPR*) was adopted in Europe in 2016 and was generally applauded as the first major reform with respect to the protection of personal information, despite criticism of specific provisions;

Whereas Europe is an important economic partner for Canada and the *GDPR* limits the transfer of personal information toward countries with lower levels of personal information protection;

UNION DES CONSOMMATEURS RECOMMENDS THAT CANADIAN LEGISLATORS:

Draw on the legislative principles developed in foreign initiatives, most notably the *GDPR*, in developing a comprehensive and consistent reform of federal and provincial laws for the protection of personal information in the private sector.

Recommendations 3 and 4

Whereas privacy is recognized as a fundamental right in Canada;

Whereas the fundamental rights of individuals are interdependent and mutually reinforcing; and whereas the right to privacy is therefore intrinsically linked to the exercise of other fundamental rights;

Whereas certain new technologies, including artificial intelligence systems, have the potential to be used in ways that expose consumers' fundamental rights to increased risks;

Whereas, in the event of a conflict between the achievement of commercial objectives and the protection of privacy, it is important that respect for a fundamental right prevail;

Whereas the *GDPR* is based on the recognition and respect of fundamental rights and freedoms, in particular the right of individuals to the protection of personal data;

UNION DES CONSOMMATEURS RECOMMENDS THAT FEDERAL LEGISLATORS:

Adopt a comprehensive human rights-based approach to *PIPEDA* reform;

Explicitly recognize a consumer privacy right in the said law.

Recommendations 5 to 7

Whereas consumers' control over their online privacy is exercised primarily through the expression of free and informed consent to the handling of their personal information;

Whereas consumers' control over the handling of their online personal information is intimately linked to the preservation of their dignity and human autonomy;

Whereas the opt-out model in Canadian laws for the protection of personal information in the private sector are inadequate, in part because:

- They do not take into account the current difficulties faced by consumers in trying to learn about, understand and evaluate the personal information handling practices of businesses;
- They do not address the dilemma that online consumers regularly face (choosing between privacy and their access and use of basic goods and services offered online);

Whereas Canadian consumers have a moderately high level of concern about loss of control over the handling of their personal information online (flow, collection, use);

Whereas current laws for the protection of personal information in the private sector provide little meaningful recourse for consumers whose right to privacy has been violated;

Whereas oversight agencies responsible for ensuring compliance with laws for the protection of personal information in the private sector have no direct enforcement authority and are severely underfunded;

UNION DES CONSOMMATEURS RECOMMENDS THAT CANADIAN LEGISLATORS:

Maintain and strengthen free and informed consent as the basis of the existing legislative framework for the protection of personal information in the private sector and limit exceptions likely to weaken or render that consent meaningless;

Implement an opt-in consent model (explicit and distinct) for all non-essential handling of personal information;

Grant to public organizations an unconditional right of private action on behalf of consumers whose personal information has not been handled lawfully.

Recommendation 8

Whereas consumers' control over their personal information, which they exercise primarily through consent, is intimately linked to safeguarding the dignity and autonomy of individuals;

Whereas expressing adequate consent is difficult online, in part because:

- Consumers are unable to sufficiently know and understand the practices used for handling their personal information and to adequately assess the risks they face in giving consent;
- Consumers often have no choice but to consent to the handling of their personal information if they want to use or access goods and services offered online;
- Some companies use subterfuge to obtain consent (*dark patterns*);

Whereas the default option will generally be chosen by consumers, due to lack of time or knowledge and to certain psychological biases;

Whereas Canadian consumers have a relatively modest general level of knowledge and understanding of online privacy risks and exhibit a certain inertia in the face of those risks;

UNION DES CONSOMMATEURS RECOMMENDS THAT CANADIAN LEGISLATORS:

Require companies that collect personal information through technological products or services provide the highest level of confidentiality by default.

Recommendations 9 to 9.2

Whereas Canadians seem to feel that they are not doing enough to protect their privacy online due to a lack of time, ability, knowledge or a general sense of powerlessness;

Whereas current legislation for the protection of personal information in the private sector places much of the responsibility for protecting their privacy on the shoulders of consumers themselves;

Whereas consumers are unable to exercise that responsibility adequately;

UNION DES CONSOMMATEURS RECOMMENDS THAT CANADIAN LEGISLATORS:

Make legislative changes to lighten consumers' responsibility and make it easier for them to protect their personal information.

Whereas consumer consent can be instrumentalized by businesses to legitimize personal information handling practices that run counter to collective values and the public interest or constitute unreasonable infringements of individual or collective rights;

Whereas Canadian consumers have a moderately high level of concern about automated decision-making based on personal information and about online tracking and profiling for advertising purposes;

Whereas automated processing of personal information for the purpose of making a decision about the person concerned is likely to infringe his fundamental rights, including the right to privacy and the right to non-discrimination;

Whereas the European Union has chosen to prohibit under the *GDPR*, with certain exceptions, automated processing of personal information for the purpose of making a significant decision about the person concerned;

Whereas targeted advertising that results from invasive online tracking strongly infringes on consumers' right to privacy;

UNION DES CONSOMMATEURS RECOMMENDS THAT CANADIAN LEGISLATORS:

Consider prohibiting certain practices that are contrary to the public interest or that pose unreasonable risks to the fundamental rights of individuals – for example:

- Handling personal information obtained through invasive online tracking for targeted advertising purposes;
- Automated processing of personal information for the purpose of making a decision about the person concerned, except where there are specific transparency requirements and an effective right of objection.

Whereas businesses' level of knowledge and understanding of the existing framework for the protection of personal information tends to be low;

Whereas certification programs promote businesses' greater awareness of the rules and best practices for handling personal information;

Whereas certification programs tend to standardize practices within certain sectors and thus can reduce the cost to consumers (in time, analysis, etc.) of raising their awareness;

UNION DES CONSOMMATEURS RECOMMENDS THAT CANADIAN LEGISLATORS:

Promote and oversee the implementation of certification programs for personal information handling practices in the private sector.

Recommendations 10 and 11

Whereas certain systems and new technologies, including those related to artificial intelligence, expose consumers' personal information to increased risks;

Whereas issues related to the insecure storage and the hacking of personal information online are of high concern to Canadian consumers;

Whereas the framework in current laws for the protection of personal information in the private sector, and for the security and retention of personal information held by businesses, appears incomplete and insufficient in light of businesses' use of new technologies;

Whereas there have been cases of large-scale hacking of personal information held by companies in recent years;

Whereas the *GDPR* provides for companies' obligation to carry out a data protection impact assessment in certain situations where the processing of personal information by means of new technologies likely poses a risk for the rights and freedoms of individuals;

UNION DES CONSOMMATEURS RECOMMENDS THAT CANADIAN LEGISLATORS:

Clarify and strengthen the obligations and legal liability of businesses with respect to the security of personal information they collect, use or retain;

Require companies to conduct a data protection impact assessment or a privacy impact assessment in certain circumstances, similarly to what is required under the *GDPR*.

Recommendations 12 and 13

Whereas the Canadian and Quebec governments introduced bills in 2020 related to the protection of personal information in the private sector;

Whereas the Quebec bill was adopted by the Quebec National Assembly on September 21, 2021;

Whereas the federal Bill C-11 died on the order paper in the summer of 2021 following the dissolution of the Canadian Parliament;

Whereas the federal bill has been widely criticized by experts and the Office of the Privacy;

Whereas the federal bill did not provide an adequate level of protection for consumer privacy online;

UNION DES CONSOMMATEURS RECOMMENDS THAT FEDERAL LEGISLATORS:

Not reintroduce the text of Bill C-11 in the next Parliament;

Rethink and rewrite the *PIPEDA* reform bill entirely,

- By taking more lessons from the *GDPR*;
- By consulting experts and stakeholders in advance and publicly, and by taking into account their criticisms of Bill C-11;
- By taking into account the recommendations in this report.

Recommendations 14 and 15

Whereas online privacy enhancement tools can significantly improve the privacy of consumers who use them;

Whereas many Canadian consumers have relatively low levels of digital literacy;

Whereas Canadian consumers:

- Make very little use of the various online privacy enhancement tools, with few exceptions;
- Display a considerable lack of awareness of online privacy enhancement tools;
- Are fairly confused about the usefulness and operation of various online privacy enhancement tools;
- Strongly distrust certain tools;

Whereas Francophone Canadian consumers have a significantly lower awareness of online privacy enhancement tools than their Anglophone counterparts;

Whereas French is the first language of nearly a quarter of the Canadian population;

Whereas it is important to facilitate access to clear information about the online privacy enhancement tools available to Canadian consumers in order to encourage their use;

Whereas among the primary sources of information about online privacy enhancement tools are the tool providers' websites;

Whereas our review of online privacy enhancement tool providers' websites reveals:

- A lack of clear and complete information in French on the usefulness and operation of the tools;
- The provision of useful and innovative information and support resources by some providers
- (e.g., virtual assistant, podcast, newsletter, user community);

UNION DES CONSOMMATEURS RECOMMENDS THAT PROVIDERS OF ONLINE PRIVACY ENHANCEMENT TOOLS:

Provide more French-language information on their websites;

Continue or increase their efforts to simplify and popularize the information on their websites, including the use of simple wording, easily understandable examples or explanations, visual aids or innovative support resources.

Recommendation 16

Whereas information presented by online privacy enhancement tool providers about the usefulness and use of the tools may be biased due to the providers' financial considerations;

Whereas it is important that Canadian consumers have access to unbiased information about their online privacy protection, including the various possible risks to their privacy and the behaviours and tools that can reduce or avoid them;

Whereas many Canadian consumers have relatively low levels of digital literacy;

Whereas Canadian consumers:

- Have a relatively modest overall level of knowledge and understanding of online privacy risks;
- Regularly misunderstand the personal information handling practices of companies;
- Hardly adopt any online privacy behaviours;
- Have very low usage of various online privacy enhancement tools, with few exceptions;
- Have very little knowledge of online privacy enhancement tools;
- Have significant confusion about the usefulness and operation of the various online privacy enhancement tools;
- Strongly distrust certain tools;

UNION DES CONSOMMATEURS RECOMMENDS THAT THE FEDERAL AND PROVINCIAL GOVERNMENTS:

Develop information programs and tools (in several languages) for Canadian Internet users to:

- Explain the online risks to privacy and personal information
- Present protective behaviours to adopt online
- Demystify and expose the benefits of using online privacy enhancement tools.