Ottawa Law Review
Revue de droit d'Ottawa

Deceptive Design and Ongoing Consent in Privacy Law

Jeremy Wiener

Volume 53, numéro 1, 2021–2022

URI : https://id.erudit.org/iderudit/1105760ar
DOI : https://doi.org/10.7202/1105760ar

Aller au sommaire du numéro

Éditeur(s)

Ottawa Law Review / Revue de droit d'Ottawa

ISSN

0048-2331 (imprimé)
2816-7732 (numérique)

Découvrir la revue

Citer cet article

Wiener, J. (2021). Deceptive Design and Ongoing Consent in Privacy Law. *Ottawa Law Review / Revue de droit d'Ottawa*, *53*(1), 133–169. https://doi.org/10.7202/1105760ar

Résumé de l'article

La *Loi sur la protection de la vie privée des consommateurs* est la première loi sur la protection de la vie privée à réglementer les pratiques trompeuses en matière de protection de la vie privée qui retirent le droit au consentement d'une personne. Le problème, c'est qu'il n'existe pas de cadre réglementaire permettant de déterminer comment la loi pourrait réellement s'appliquer. Cet article résout le problème en comblant trois lacunes dans la recherche. En premier lieu, il classe différents types de subterfuges selon la notion « d'avis et du choix » du droit relatif au respect de la vie privée, présentant ainsi une méthode d'analyse aux chercheurs et chercheuses et aux organismes de réglementation.

Ensuite, l'article rend concret ce cadre réglementaire en faisant une analyse comparative des enquêtes menées par la *Federal Trade Commission* des États-Unis et le Commissariat à la protection de la vie privée du Canada (CPVP). Ceci permettra de faire la lumière sur la façon dont la Loi pourrait être interprétée, et offre un survol exhaustif d'un aspect représentatif des enquêtes du CPVP.

Enfin, l'article tente de déterminer si la Loi définit le consentement comme étant une capacité illimitée d'agir, ce qui protégerait la vie privée des gens puisque ceci inclurait les pratiques trompeuses qui visent non seulement les situations « je suis d'accord », mais aussi celles qui vont au-delà de « je suis d'accord ».

Finalement, cet article agit en tant que guide pour les juges et les organismes de réglementation dans l'application de la Loi, aide les décideurs et décideuses politiques à élaborer davantage de dispositions législatives pour réglementer les pratiques trompeuses en ce qui concerne la protection de la vie privée, et s'accorde avec la doctrine en comblant les lacunes mentionnées ci-dessus.

Deceptive Design and Ongoing Consent in Privacy Law

Jeremy Wiener

THE *Consumer Privacy Protection Act* is the first proposed privacy statute to regulate the deceptive privacy practices that undermine individuals' right to consent. The problem is that there is no framework for determining how the Act might actually apply. This article resolves the issue by filling three gaps in the literature.

First, it categorizes different types of deception according to privacy law's notice-and-choice framework, providing a method of analysis for scholars and regulators. It then concretizes the framework by comparatively surveying investigations led by the United States' Federal Trade Commission and Office of the Privacy Commissioner of Canada (OPC). This will shed light on how the Act can be interpreted, and will constitute a comprehensive survey of a thematic area of OPC investigations.

Finally, the article explores whether the Act defines consent as an act of ongoing agency, which would protect peoples' privacy by covering deception that occurs not only at "I agree moments," but also beyond "I agree moments." Ultimately, this article guides judges and regulators in enforcing the Act, assists policy-makers in developing more statutory provisions that regulate deceptive privacy practices, and contributes to doctrine by filling the aforementioned gaps.

LA *Loi sur la protection de la vie privée des consommateurs* est la première loi sur la protection de la vie privée à réglementer les pratiques trompeuses en matière de protection de la vie privée qui retirent le droit au consentement d'une personne. Le problème, c'est qu'il n'existe pas de cadre réglementaire permettant de déterminer comment la loi pourrait réellement s'appliquer. Cet article résout le problème en comblant trois lacunes dans la recherche. En premier lieu, il classe différents types de subterfuges selon la notion « d'avis et du choix » du droit relatif au respect de la vie privée, présentant ainsi une méthode d'analyse aux chercheurs et chercheuses et aux organismes de réglementation.

Ensuite, l'article rend concret ce cadre réglementaire en faisant une analyse comparative des enquêtes menées par la *Federal Trade Commission* des États-Unis et le Commissariat à la protection de la vie privée du Canada (CPVP). Ceci permettra de faire la lumière sur la façon dont la Loi pourrait être interprétée, et offre un survol exhaustif d'un aspect représentatif des enquêtes du CPVP.

Enfin, l'article tente de déterminer si la Loi définit le consentement comme étant une capacité illimitée d'agir, ce qui protégerait la vie privée des gens puisque ceci inclurait les pratiques trompeuses qui visent non seulement les situations « je suis d'accord », mais aussi celles qui vont au-delà de « je suis d'accord ».

Finalement, cet article agit en tant que guide pour les juges et les organismes de réglementation dans l'application de la Loi, aide les décideurs et décideuses politiques à élaborer davantage de dispositions législatives pour réglementer les pratiques trompeuses en ce qui concerne la protection de la vie privée, et s'accorde avec la doctrine en comblant les lacunes mentionnées ci-dessus.

CONTENTS

Deceptive Design and Ongoing Consent in Privacy Law

*Jeremy Wiener**

INTRODUCTION

Google and Facebook's user interfaces (UIs) contain misleading language that causes individuals to consent to the lowest possible privacy setting.[1] And they are not alone. Organizations routinely deceive individuals into sharing more personal information than they otherwise would.[2] This undermines the consent-based model for privacy protection, as well as public trust in the government's ability to protect peoples' privacy.[3]

As a result, governments, scholars, and civil societies are increasingly exploring how deception impacts an individual's right to consent to their personal information's collection and processing.[4] For example, Canada's

* Jeremy Wiener is a JD/BCL Candidate at McGill University. The author thanks Ignacio Cofone, as well as his friends and family, for their support and guidance. The article also benefitted from comments by Anna Gignac-Eddy and the *Ottawa Law Review*'s editors and anynymous reviewers. Any mistakes are his own.

1 See "Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us From Exercising Our Rights To Privacy" (27 June 2018) at 31–39, online (pdf): *Forbrukerrådet* <fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>.

2 See Part IV, below.

3 See e.g. Ignacio Cofone, "Policy Proposals for PIPEDA Reform to Address Artificial Intelligence Report" (November 2020), online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pol-ai_202011/> [Cofone, "Policy Proposals"].

4 See e.g. Sebastian Rieger & Caroline Sinders, "Dark Patterns: Regulating Digital Design" (May 2020) at 24–26, online (pdf): *Stiftung Neue Verantwortung* <www.stiftung-nv.de/sites/default/files/dark.patterns.english.pdf> (discussing government and regulatory bodies' efforts); Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Cambridge, Mass: Harvard University Press, 2018) (comprising the most seminal discussion of deceptive design) [Hartzog, *Privacy's Blueprint*]; Mark Sullivan, "These

last federal government tabled a bill to replace the country's private-sector privacy law, the *Personal Information Protection and Electronics Document Act* (*PIPEDA*)[5] with the *Consumer Privacy Protection Act* (*CPPA*).[6] The *CPPA* proposed to prohibit organizations from obtaining or attempting to obtain an individual's consent by engaging in a deceptive or misleading practice.[7]

The problem is that there is no unified analysis of how such a statutory provision might apply. This might deter regulators and policy-makers from adopting such an anti-deception model.

This article seeks to resolve the issue by filling three gaps in the literature. First, it categorizes the different types of deception according to privacy law's notice-and-choice framework, and then distinguishes the different moments at which deception can occur: at "I agree moments," and beyond "I agree moments."

It then concretizes this categorization by comparatively surveying investigations led by the United States' Federal Trade Commission (FTC) and the Office of the Privacy Commissioner of Canada (OPC). This will shed light on how a statutory provision that regulates deceptive privacy practices might apply to the specific practices that individuals regularly find themselves in, and will constitute one of the first comprehensive surveys of a thematic area of OPC investigations.

Finally, the article explores whether privacy statutes that regulate deceptive practices should be interpreted as applying beyond "I agree moments." This is an important question, because only regulating deception at "I agree moments" would disembody law from individuals' lived experiences.

Related to this last area of exploration, the article argues that privacy statutes should be interpreted as granting not only a right to consent, but a right to consent as an act of ongoing agency. Such a right to ongoing consent would mean that privacy statutes regulating deception apply beyond "I agree moments." This would cover the entirety of a company's dealings with individuals and would thus more fully appreciate individuals' embodied experiences and understandings.

---

are the Deceptive Design Tricks and Dark Patterns That Steer Your Clicks" (25 June 2019), online: *Fast Company* <www.fastcompany.com/90369183/deceptive-design-tricks-and-dark-patterns-that-steer-your-clicks>.

5 SC 2000, c 5 [*PIPEDA*].

6 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*, 2nd Sess, 43rd Parl, 2020 (terminated at the Parliamentary session's conclusion) [*CPPA*].

7 *Ibid* at cl 16.

To demonstrate this, the article proceeds in five parts. Part I contextualizes the problem. It discusses the deficiencies of language-based notice-and-choice, showing the importance of recognizing how digital space's design impacts user experience. Part II explores deception. It defines it in relation to other forms of influence, examines the legal standard for determining whether a deceptive representation or practice actually occurred, and categorizes the three different types of deception according to privacy law's notice-and-choice framework. Part III distinguishes deception that occurs at versus beyond "I agree moments"—a novel distinction that appreciates that the entirety of an organization's dealings with a user affect individuals' understandings. Part IV exemplifies written and design-based deception at "I agree moments" by surveying investigations led by the United States' FTC and Canada's OPC. Part V then provides examples of deception occurring beyond "I agree moments," and argues that privacy statutes that regulate deception should be interpreted as applying to it. To make this point, the section distinguishes privacy from contract law, looks to notions of ongoing consent in other areas of law, and examines privacy statutes' general schemes. The paper then concludes.

I. DESIGNING FOR NOTICE-AND-CHOICE'S DEFICIENCIES

Notions of autonomy and consent have long underpinned understandings of privacy.[8] They began affecting private-sector privacy law in the 1980s when they were articulated in the United States' Fair Information Practice Principles (FIPPs).[9] The FIPPs informed privacy protection laws around the world, such as *PIPEDA*.[10] It is therefore not surprising that the OPC describes individual autonomy as the "foundation for the consent principle,"[11] and that Canada's former privacy commissioner, Jennifer Stoddart,

8 See especially Alan F Westin, *Privacy and Freedom* (New York: Atheneum Press, 1967) (characterizing privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" at 7). See also *R v Dyment*, [1988] 2 SCR 417, 55 DLR (4th) 503 ("[g]rounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual" at 427).

9 See Paul M Schwartz & Daniel J Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Information" (2011) 86 NYUL Rev 1814 at 1814.

10 See Lisa M Austin, "Is Consent the Foundation of Fair Information Practices: Canada's Experience under PIPEDA" (2006) 56:2 UTLJ 181 at 181.

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

described consent as "the fundamental principle on which *PIPEDA* is based."[12]

Consent's current paradigm is notice-and-choice, also known as "knowledge and consent."[13] "Notice" occurs where an organization presents the what-when-how of their privacy practice.[14] "Choice" signifies accepting or rejecting those terms.[15] Notice generally precedes choice, and is inextricably linked to it.[16] Consent requires both.[17]

The consent-based model of privacy protection, however, is subject to much criticism.[18] Many are calling on privacy law to shift away from consent as a result.[19] But Europe's recently enacted *General Data Protection Regulation* (*GDPR*), the *California Consumer Privacy Act* (*CCPA*), and proposed privacy bills in Canada and the United States do not shift away from consent entirely. In these, consent remains one of the primary legal bases for processing individuals' personal information.[20] Examining how to strengthen consent is thus worthwhile.

---

12 Jennifer Stoddart, "The *Personal Information Protection* and *Electronic Documents Act*: An Overview of Canada's New Private Sector Privacy Law" (last modified 31 March 2004), online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/opc-news/speeches/2004/sp-d_040331/>.

13 *PIPEDA*, *supra* note 5 (stating that consent requires "knowledge and consent" at Principles 4.3, 4.3.2).

14 *Ibid* at Principles 4.2, 4.8; *CPPA*, *supra* note 6 at cl 15(3).

15 *PIPEDA*, *supra* note 5 at Principle 4.3; *CPPA*, *supra* note 6 at cl 15(1).

16 *CPPA*, *supra* note 6 at cl 15(2).

17 *PIPEDA*, *supra* note 5 at Principle 4.3.

18 See generally Joel R Reidenberg et al, "Privacy Harms and the Effectiveness of the Notice and Choice Framework" (2015) 11:2 I/S: A JL & Policy for Information Society 485.

19 See e.g. Daniel J Solove, "Privacy Self-Management and the Consent Dilemma" (2013) 126:7 Harv L Rev 1880 at 1900–903; See Ignacio Cofone, "Beyond Data Ownership" 43 Cardozo L Rev at 63–65 [forthcoming in 2021] [Cofone, "Ownership"] (arguing that ex-post use-restrictions and accountability would strengthen the consent-based model of privacy protection); Neil Richards & Woodrow Hartzog, "A Duty of Loyalty for Privacy Law" 99 Washington UL Rev [forthcoming in 2021] (arguing that fiduciary duties are a potential solution to consent-related problems).

20 See EC, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJ, L 119/1, art 6(1) [*GDPR*]; *California Consumer Privacy Act of 2018*, 3 CIV § 1798.120–21, 1798.135(2) (2018) [*CCPA*]; Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information*, 1st Sess, 42nd Leg, Quebec, 2020, cl 9 (assented to 22 September 2021), SQ 2021, c 25 [Bill 64]; US, SB 2330, *Data Transparency and Privacy Act*, 101st Gen Assem, Reg Sess, Ill, 2020, ss 25(1), 35(d).

Doing so requires appreciating consent's weaknesses. Dissecting privacy policies, and the ubiquitous form of notice that emerged in the 1990s,[21] is a good place to start. In short, privacy policies are confusing to read, and are infrequently read.[22] Even the sitting Chief Justice of the Supreme Court of the United States does not read them.[23] This might be because, according to Helen Nissenbaum, privacy policies are characterized by a "transparency paradox": if privacy policies comprehensively describe an organization's practices, then the policy will be too long and complicated for the average user to read or understand; and if they are short and simple, then they will not be detailed enough for users to make informed choices.[24]

Acknowledging the deficiencies of traditional language-based notice, privacy doctrine is increasingly examining how digital space's design impacts user experience.[25] It is not alone in this regard. Social scientists have long appreciated how design influences human behaviour in the physical world.[26] In architecture, for example, Jeremy Bentham designed the modern prison panopticon to encourage passivity.[27] More recently, the

21 See Allyson W Haynes, "Online Privacy Policies: Contracting Away Control Over Personal Information?" (2007) 111:3 Penn St L Rev 587 at 593–94.

22 See generally Joel R Reidenberg et al, "Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding" (2015) 30:1 BTLJ 39 ("ambiguous wording in typical privacy policies undermines the ability of privacy policies to effectively convey notice of data practices to the general public" at 40); James P Nehf, "Shopping for Privacy Online: Consumer Decision-Making Strategies and the Emerging Market for Information Privacy" (2005) 2005:1 JL Technology & Policy 1 ("[a] study of 1500 adult Internet users concluded that less than one percent thought a Web site's privacy policy was relevant in determining the site's credibility" at 20).

23 See Andrew Malcolm, "Chief Justice Roberts on Tiny Type" (20 October 2010), online (blog): *Los Angeles Times* <latimesblogs.latimes.com/washington/2010/10/chief-justice-john-roberts-state-of-the-union.html>.

24 See Helen Nissenbaum, "A Contextual Approach to Privacy Online" (2011) 140:4 Dædalus 32 at 36. See also Aleecia M McDonald & Lorrie Faith Cranor, "The Cost of Reading Privacy Policies" (2008) 4:3 I/S: A JL & Policy for Information Society 543 at 563 (finding that it would take the average internet user 244 hours to read the privacy policies of the websites they visit each year); M Ryan Calo, "Against Notice Skepticism in Privacy (and Elsewhere)" (2012) 87:3 Notre Dame L Rev 1027 at 1033 (finding that simpler privacy policies that use icons and graphics only marginally improve understanding).

25 See generally Ari Ezra Waldman, "Privacy's Law of Design" (2019) 9 UC Irvine L Rev 1239; Hartzog, *Privacy's Blueprint*, *supra* note 4.

26 See e.g. Leonardo Benevolo, *The Origins of Modern Town Planning* (Cambridge, Mass: MIT Press, 1967). See also Ari Ezra Waldman, "Privacy, Notice, and Design" (2018) 21:1 Stan Tech L Rev 74 at 100–107 (discussing how design has influenced human understanding in the fields of fine art, architecture, interior design, and urban design).

27 See Jeremy Bentham, *The Panopticon Writings*, ed by Miran Božovič (London, UK: Verso, 1995).

Design Against Crime Research Centre reduced petty crime in an area that had seen high rates of bicycle and bag theft by adding lights and spaces for people to socialize.[28]

Law also frequently regards design. For instance, product liability largely concerns how defective design can cause harm.[29] Contract law recognizes that design enables understanding by invalidating clauses deemed illegible due to their physical representation or location.[30] And in intellectual property law, following years of underdevelopment, design patents have burst onto the stage.[31]

It is thus fitting that privacy law concerns itself with digital design. As Julie Cohen put it, not regulating design's effect on notice-and-choice would divorce privacy law from "embodied experience."[32] It would reflect what philosophers call "theoretical knowledge," as opposed to the practical knowledge gained through interactive spatial life.[33] Recognizing this, Ryan Calo suggests that policy should encourage "visceral notice," defined as notice that does not rely exclusively on language or its symbolic equivalent.[34]

The key, naturally, is appreciating design's impact on not only notice, but also choice. This may indeed be at the heart of what the former

28 See Lorraine Gamman & Adam Thorpe, "Design Against Crime as Socially Responsive Design for Public Space" (Presentation delivered at the UK/Brazil Workshop on Innovation and Investment in Research and the Creative Economy, December 2007) [unpublished].

29 See CCQ ("[a] thing has a safety defect where…it does not afford the safety which a person is normally entitled to expect, *particularly by reason of a defect in design* or manufacture", art 1469) [emphasis added]; *Lambert v Lastoplex Chemicals*, [1972] SCR 569, 25 DLR (3d) 121 (finding that the "cautions on the label affixed to the container cans" insufficiently warned users of the risk of harm and were thus defective at 575). See also Paul D Rheingold, "Proof of Defect in Product Liability Cases" (1971) 1971 Insurance LJ 645 (recognizing that there are generally two types of defects in product liability cases: "construction flaw" and "design flaw" at 646).

30 See e.g. *Dell Computer Corp v Union des consommateurs*, 2007 SCC 34 at para 90 (discussing articles 1435 to 1437 of the CCQ, which regulate external, illegible, incomprehensible, and abusive clauses' validity); *Thornton v Shoe Lane Parking Ltd*, [1971] 1 All ER 686 ("[i]n order to give sufficient notice, it would need to be printed in red ink with a red hand pointing to it, or something equally startling" at para 690).

31 See Peter Lee & Madhavi Sunder, "Design Patents: Law Without Design" (2013) 17 Stan Tech L Rev 277 at 277.

32 Julie E Cohen, "Cyberspace As/And Space" (2007) 107:1 Colum L Rev 210 at 225–27.

33 Edward Rubin, "The Internet, Consumer Protection and Practical Knowledge" in Jane K Wynn, ed, *Consumer Protection in the Age of the 'Information Economy'* (London, UK: Routledge, 2016) 35 at 40–44 (traditional notice relies on theoretical knowledge).

34 *Supra* note 24 at 1034–35. See also Albert Mehrabian, *Silent Messages* (Belmont, CA: Wadsworth Publishing Company, 1971) at 43–44 (famously stating that 93% of communication is non-verbal).

Information & Privacy Commissioner of Ontario, Ann Cavoukian, meant when she suggested that law adopt Privacy by Design (PbD), generally characterized as the approach of embedding privacy into the design specifications of various technologies.[35] The *GDPR* and Quebec's proposed Bill-64 contain PbD language, but their PbD provisions are broadly worded and do not specifically reference deceptive design.[36] As a result, European data regulators have only just begun thinking about how to investigate and sanction deceptive design.[37] Deepening our collective reflection on how to best regulate deceptive design is important. Accordingly, this article is one of the first to determine how a privacy-specific statute might actually regulate deceptive notice-and-choice. To facilitate the analysis, the next part discusses deception's distinguishing features.

II. UNDERSTANDING DECEPTION

Understanding deception is essential to regulating it. Accordingly, this part first defines deception by distinguishing it from other forms of influence, such as persuasion and manipulation.[38] It then examines deception in private and statutory law.[39] Finally, it considers how privacy doctrine classifies different deceptive practices, and fills a gap in the literature by categorizing deception according to notice-and-choice.[40]

A. Defining Deception

Deception must be distinguished from other forms of influence: persuasion, coercion, manipulation, and nudging. Not doing so might create confusion as to whether a particular practice is covered by an attempt to regulate deceptive design.

35 Ann Cavoukian, "Privacy by Design" (January 2009) at 2, online (pdf): *Information and Privacy Commissioner of Ontario* <www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf>.

36 *GDPR*, *supra* note 20 (requiring organizations to "implement appropriate technical and organisational measures", art 25(2)); Bill 64, *supra* note 20 ("an enterprise who collects personal information…must ensure that the parameters of the product or service provide the highest level of confidentiality by default" at cl 100).

37 Rieger & Sinders, *supra* note 4 at 24–26.

38 See Part II-A, below.

39 See Part II-B, below.

40 See Part II-C, below.

Daniel Susser, Beate Roessler, and Helen Nissenbaum's work on manipulative digital media defines deception's distinguishing features.[41] This and the next four paragraphs borrows heavily from their article. To illustrate how deception differs from other forms of influence, let us use an example that can be easily applied to the context of privacy law: deciding which car to buy at a dealership.

Persuasion is seen as the most respectful form of influence because it is the salesperson openly appealing to another's capacity for conscious deliberation by providing reasons for buying a more expensive car model.[42] In persuading, the salesperson can, for instance, highlight the car's unique features, or offer a discounted purchase price. Joel Rudinow refers to such reasons as "*resistible* incentives."[43] They are resistible in the sense that the buyer still has the choice to buy the car that they wish.

Coercion, in contrast, impedes choice by eliminating "acceptable alternatives."[44] It involves "*irresistible* incentives."[45] The famous "gun to your head" metaphor exemplifies coercion. As Ignacio Cofone discusses in the context of COVID-19, one might be coerced into consenting to a particular contact tracing app's privacy practice if not consenting to it means being barred from social participation.[46] Coercion ultimately undermines voluntary choice.[47] With this said, it is similar to persuasion in that both operate overtly and rely on another's *ability* to choose and self-govern. As Susser, Roessler, and Nissenbaum put it, "[i]f one did not understand that the only acceptable option available to them was to do as their coercer instructed, or if they could not act on that understanding, then they would

41 See Daniel Susser, Beate Roessler & Helen Nissenbaum, "Online Manipulation: Hidden Influences in a Digital World" (2019) 4:1 Georgetown L Technology Rev 1.

42 *Ibid* at 14–15.

43 Joel Rudinow, "Manipulation" (1978) 88:4 Ethics 338 at 342 [emphasis added].

44 Allen W Wood, "Coercion, Manipulation, Exploitation" in Christian Coons & Michael Weber, eds, *Manipulation: Theory and Practice* (Oxford: Oxford University Press, 2014) 17 at 21–23.

45 Rudinow, *supra* note 43 (stating that "irresistible incentives" can only be avoided through "heroism, madness, or something similarly extraordinary" at 341) [emphasis added].

46 See Ignacio Cofone, "Immunity Passports and Contact Tracing Surveillance" (2021) 24 Stan Tech L Rev 176 at 195, 197. See also *R v Big M Drug Mart Ltd*, [1985] 1 SCR 295, 18 DLR (4th) 321 ("coercion includes indirect forms of control which determine or limit alternative courses of conduct available to others" at 336–37).

47 See generally Steven Penney, "Consent Searches for Electronic Text Communications: Escaping the Zero-Sum Trap" (2018) 56:1 Alta L Rev 1 at 8 (canvasing the standard of voluntary consent to search and seizure).

have no motivation or no means to go along with the coercer's plan."[48] In this sense, the coerced, like the persuaded, are the final deciders.

Manipulation differs in this respect. Instead of relying on one's ability to self-govern, it interferes with "the self-governed (and self-governing) activity we call 'making up one's own mind about how to act.'"[49] To use a more visual analogy, "[t]he manipulative person 'steers' the other as a driver steers an automobile."[50] Granted, manipulation rarely deprives one of total self-government.[51] But it seeks to interfere with it as much as possible, and to this end operates most effectively when it is subtle and sneaky.[52] This explains why, while the coerced "feels used," the manipulated "feels *played*."[53]

Deception is a type of manipulation.[54] The British Columbia and Ontario Courts of Appeal define deception as an act of leading someone to believe something that is not true.[55] So do the *Oxford English Dictionary* and *Merriam-Webster Dictionary*.[56] An example of deception is a salesperson making one believe that the car they are thinking of purchasing comes with a navigation system at no extra cost when there are really hidden fees. A salesperson can lead one to this false belief by exploiting the cognitive biases related to "framing effects" and heuristics.[57] This can be done by, for

48 *Supra* note 41 at 15.

49 Sarah Buss, "Valuing Autonomy and Respecting Persons: Manipulation, Seduction, and the Basis of Moral Constraints" (2005) 115:2 Ethics 195 at 195.

50 Wood, *supra* note 44 at 33–34.

51 Susser, Roessler & Nissenbaum, *supra* note 41 (holding that this is why "people intuitively believe that … people should almost always be excused for doing things they were coerced to do, but only sometimes excused for things they were manipulated into doing" at 17).

52 *Ibid* at 17, 20.

53 *Ibid* at 17 [emphasis in original].

54 *Ibid* (referring to deception as "an important tool in the manipulator's toolkit" at 21).

55 See *Private Career Training Institutions Agency v Vancouver Career College (Burnaby) Inc*, 2011 BCCA 69 [*Private Career Training*] (defining "mislead" as to "cause to have a wrong impression" at para 32); *R v Wolf*, [1973] 5 WWR 226, 12 CCC (2d) 228 (Alta SC (AD)) [*Wolf* cited to WWR] (defining the word "mislead" as to "lead into a wrong direction or into a mistaken action or belief" at 234). See also *R v Westfair Foods Ltd*, [1986] 41 Man R (2d) at para 24, 33 BLR 163 (QB) [*Westfair Foods*].

56 See JA Simpson & ESC Wiener, eds, *The Oxford English Dictionary*, 2nd ed (Oxford: Oxford University Press, 1989) ("[t]o lead astray in action or conduct; to lead into error" sub verbo "mislead"); Frederick C Mish et al, eds, *Merriam-Webster's Collegiate Dictionary*, 11th ed (Springfield, Mass: Merriam-Webster, 2003) ("to lead in a wrong direction or into a mistaken action or belief" sub verbo "mislead").

57 Amos Tversky & Daniel Kahneman, "Judgement Under Uncertainty: Heuristics and Biases" (1974) 185:4157 Science 1124 at 1127–28 (discussing the "availability heuristic," which regards how individuals give more weight to evidence that is more available in their

instance, responding to a question in a way that is technically factual but causes reasonable people to hold false beliefs.

Deception differs from another kind of manipulation that does not influence beliefs at all: nudging. Richard Thaler and Cass Sunstein define nudging as "any aspect of the choice architecture that alters peoples' behavior in a predictable way without forbidding any options or significantly changing their economic incentives."[58] To return to our car dealership example, a salesperson might nudge individuals to buy the more expensive car model by putting it at the showroom's front under bright lights, or by adding an enjoyable odor to the car's inside.

Defining deception in relation to these forms of influence is important. This is because a design might be manipulative or nudging, but not deceptive. For example, social media platforms such as Facebook's UI deploy design elements, such as the "pull-to-refresh," which addict users to their platforms.[59] Being addicted to a particular platform undermines one's ability to engage in the cost-benefit analysis that privacy law's notice-and-choice framework depends on.[60] It may thus be manipulative. However, it is not deceptive because the addictive design does not lead one to believe something that is not true.[61] Similarly, nudges can be manipulative but not necessarily deceptive—a distinction that will prove particularly important in examining practices that impede choice modification.[62]

---

memory); Amos Tversky & Daniel Kahneman, "Rational Choice and the Framing of Decisions" (1986) 59:4 J Bus 251 (noting that "[f]raming is controlled by the manner in which the choice problem is presented as well as by norms, habits, and expectancies of the decision maker" at 257).

58 Richard H Thaler & Cass R Sunstein, *Nudge: Improving Decisions About Health, Wealth, and Happiness* (New Haven, NY: Yale University Press, 2008) at 6. See also Ignacio N Cofone, "The Way the Cookie Crumbles: Online Tracking Meets Behavioral Economics" (2016) 25:1 Intl JL & IT 38 (discussing how some "advocate for choice mechanisms that nudge people into making better [privacy-related] choices" at 47).

59 Vikram R Bhargava & Manuel Velasquez, "Ethics of the Attention Economy: The Problem of Social Media Addiction" (2020) 31:3 Bus Ethics Q 321; US, *Optimizing for Engagement: Understanding the Use of Persuasive Technology on Internet Platforms*, 116th Cong (25 June 2019) (Tristan Harris).

60 See Woodrow Hartzog, "The Case Against Idealising Control" (2018) 4 European Data Protection L Rev 423 ("[d]esire has powerful tendency to dampen scepticism. If we users want it bad enough, we can rationalize any decision" at 427); Nora D Volkow & Joanna S Fowler, "Addiction, a Disease of Compulsion and Drive: Involvement of the Orbitofrontal Cortex" (2000) 10:3 Cerebral Cortex 318 at 323.

61 See generally Alan I Leshner "Addiction Is a Brain Disease, and It Matters" (1997) 278:5335 Science 45 at 46 (discussing how addiction is a brain disease and chronic, relapsing disorder).

62 See the text accompanying notes 138–41, 153–54, and the two sentences following note 154.

Before discussing this, though, the next subsection explores deception's constitutive components.[63]

B. Deception in Private and Statutory Law

There are two components to deception: how a deceptive representation or practice must be carried out (the *actus reus*, for lack of a better term), and the mental element associated with it (the *mens rea*).

The required mental element will be discussed first. The common law causes of action that regard deception are the tort of deceit and fraudulent misrepresentation in inducing a contract. While the two were historically understood as discrete causes of action,[64] courts have increasingly referred to them interchangeably, causing the distinction between them to blur.[65] In *BG Checo International Ltd v British Columbia Hydro and Power Authority*, the Supreme Court held that there was insufficient evidence to find the tort of deceit because the would-be deceiver lacked intention.[66] Yet more recently, Justice Karakatsanis defined the tort of deceit (now "civil fraud") for a unanimous Supreme Court as a false representation made with "some level of knowledge of the falsehood of the representation" that causes another to act and suffer a loss.[67] However, in arriving at this definition, the Court relied on an 1889 decision of the House of Lords, and did not address the line of cases holding that the tort of deceit requires that a party make a representation that they knew was false with the intention to deceive. As a result, there now seems to be some ambiguity in the law, as some appellate courts continue to interpret the tort of deceit as requiring intention.[68]

63 See Part II-B, below.

64 See e.g. *Kelemen v El-Homeira*, 1999 ABCA 315 [*Kelemen*] (recognizing that "[t]he tort action is founded in law whereas the contract action is based in equity" at para 5).

65 See e.g. *Dhillon v Dhillon*, 2006 BCCA 524 [*Dhillon*] (writing that "[w]hile fraudulent activities in the civil context (*i.e.* 'civil fraud') can occur in innumerable ways, the 'civil fraud' cause of action is recognized in Canada as the tort of deceit, also referred to as the tort of fraud or fraudulent misrepresentation" at para 77).

66 [1993] 1 SCR 12 at 54, 99 DLR (4th) 577, Iacobucci & Sopinka JJ, dissenting (but not regarding the required mental element). See also *XY, LLC v Zhu*, 2013 BCCA 352 at para 19; *3com Corporation v Zorin International Corporation* (2006), 211 OAC 222 at para 7, 148 ACWS (3d) 819; *Dhillon*, *supra* note 65 at para 77; *Kelemen*, *supra* note 64 at paras 7–8, 14.

67 *Bruno Appliance and Furniture, Inc v Hryniak*, 2014 SCC 8 at para 21 [*Bruno Appliance*].

68 See e.g. *Paulus v Fleury*, 2018 ONCA 1072 (holding that "[t]he intention that the opposing party rely on the representation is an essential element of civil fraud" at paras 9–10, 32); *Warkentin v BMO Nesbitt Burns Inc*, 2018 MBCA 22 ("[d]ishonest intent is required in order to establish the tort of deceit" at para 29). But see *Boyd v Cook*, 2016 BCCA 424 at paras 24–26 (citing *Dhillon* and *Bruno Appliance* as if they are both good law without discussing

In contrast, the civil law's equivalent to fraudulent misrepresentation, dol, requires intention to deceive.[69] The *Restatement of the Law Third* likewise suggests that civil fraud requires intent.[70]

So too does the use of the term "deception" in what was the once-tabled *CPPA*. The *CPPA* proposed to regulate "false or misleading information" and "deceptive or misleading practices."[71] "False" denotes a comparison between the literal representation and factual reality—a question of truth. "Misleading," on the other hand, concerns what the reasonable person is "led to believe."[72] A representation can thus be false but not misleading (or deceptive), or it might be misleading (or deceptive) but not false.[73] Misleading, in the private law context, has not been interpreted as requiring a mental element.[74] If deception is also interpreted as not requiring a mental element, as the Canadian common law seems to understand it,[75] then it becomes indistinguishable from "misleading." The problem with this reading is that principles of statutory interpretation do not tolerate having two different terms with the same meaning.[76] As a result, if the *CPPA* had been enacted as written, deception would have been interpreted as

---

their disagreement regarding whether intention is required, but applying *Bruno Appliance* to the facts before the court).

69 See *Clément et Frères Ltée c Club Auto-Neige Montmagny Inc* (1993), [1994] RL 377 at para 15, 43 ACWS (3d) 865 (Qc CA) [*Clément et Frères*]; CCQ, *supra* note 29, art 1401. See also art 1137 C civ.

70 See The American Law Institute, *Restatement of the Law Third: Torts: Liability for Economic Harm* (St. Paul, Minn: American Law Institute Publishers, 2020) at § 9 [*Restatement*].

71 *Supra* note 6 at cl 16.

72 *Private Career Training*, *supra* note 55 at paras 32–33; *Wolf*, *supra* note 55 at 234; *Westfair Foods*, *supra* note 55 at para 24. For a discussion on the "general impression" standard that determines whether a representation is misleading, see *Richard v Time Inc*, 2012 SCC 8 at paras 45–60.

73 See *Panzer v Zeifman*, [1978] 20 OR (2d) 502, 88 DLR (3d) 131 (CA) [*Panzer* cited to OR] (holding that, though "neither the vendor nor the agents expressly stated anything which was untrue," given "what the agents said…and the manner in which the matter was presented the purchaser here could only have reached a conclusion which in fact was wrong" at 509).

74 See e.g. *R v Wholesale Travel Group Inc*, [1991] 3 SCR 154, 84 DLR (4th) 161 (defining false or misleading advertising "without reference to the culpability of the accused's conduct," meaning that it encompasses "innocent, negligent, reckless and intentionally false misrepresentation" at 174); *R v Allied Towers Merchants Ltd*, [1965] 2 OR 628 at 631, 1 CCC 220 (H Ct J) (concluding that "misleading" is a strict liability offence unless otherwise indicated).

75 *Bruno Appliance*, *supra* note 67 at para 21.

76 See Ruth Sullivan, *Statutory Interpretation*, 2nd ed (Toronto: Irwin Law, 2007) at 156 (referring to tautology).

requiring intention—as per the civil law and the *Restatement*.[77] Thus, for the purposes of this article, deception will be considered to require an intention to deceive.

Regarding how a misleading or deceptive representation or practice must be carried out (the *actus reus* component), the civil law holds that fraud can result from silence or concealment.[78] This is similar to the criminal law on sexual fraud, which can also occur via non-disclosure.[79] Canadian common law, in contrast, is reluctant to recognize a duty to disclose.[80] This might be because there is no overarching duty of good faith in the common law, as in the civil law.[81]

With that said, Jack Balkin and others are increasingly arguing that many online service providers who collect and process personal information should be treated according to fiduciary principles.[82] Such fiduciary obligations would include a duty to disclose.[83] But even if no fiduciary obligations exist, the common law holds that active concealment or half-truths may qualify as fraudulent misrepresentation.[84] And as will be shown below,

77 CCQ, *supra* note 29, art 1401; *Clément et Frères*, *supra* note 69 at para 15; *Restatement*, *supra* note 70, s 9.

78 CCQ, *supra* note 29, art 1401. See also *Bank of Montreal v Bail Ltée*, [1992] 2 SCR 554, 93 DLR (4th) 490 (discussing the duty to disclose information).

79 See *R v Hutchinson*, 2014 SCC 19 at para 67.

80 See e.g. *Martel Building Ltd v Canada*, 2000 SCC 60 ("[i]t would defeat the essence of negotiation and hobble the marketplace to extend a duty of care to the conduct of negotiations, and to label a party's failure to disclose its bottom line, its motives or its final position as negligent" at para 67).

81 See generally *Bhasin v Hrynew*, 2014 SCC 71 at para 73 (recognizing an organizing principle of good faith in contractual performance that does not create a duty of loyalty or of disclosure); *CM Callow Inc v Zollinger*, 2020 SCC 45 (noting that the "duty of honest performance is a contract law doctrine, setting it apart from other areas of the law that address the legal consequences of deceit with which it may share certain similarities" at para 50).

82 See Jack M Balkin, "The Fiduciary Model of Privacy" (2020) 134:11 Harv L Rev 11; Jack M Balkin, "Information Fiduciaries and the First Amendment" (2016) 49:4 UC Davis L Rev 1183. See also Richards & Hartzog, *supra* note 19; US, AB 680, *New York Privacy Act*, 2021–22, Reg Sess, NY, 2021, s 1102 [*NYPA*] (proposing to establish data fiduciaries).

83 See also Richard Nolan, "A Fiduciary Duty to Disclose?" (1997) 113:2 Law Q Rev 220 at 222. See generally Remus Valsan, "Fiduciary Duties, Conflict of Interest, and Proper Exercise of Judgement" (2016) 62:1 McGill LJ 1 at 9–11.

84 See e.g. *Alevizos v Nirula*, 2003 MBCA 148 at para 21 (regarding half-truth); *Abel v McDonald*, [1964] 2 OR 256, 45 DLR (2d) 198 (CA) (regarding active concealment); *Sidhu Estate v Bains*, [1996] 10 WWR 590 at paras 30, 33, 25 BCLR (3d) 41 (CA) (regarding active concealment); *Panzer*, *supra* note 73 at 509 (regarding half-truth).

deceptive notice-and-choice rarely, if ever, concerns non-disclosure, and can almost always be characterized as active concealment or a half-truth.[85]

C. Categorizing Deceptive Notice-and-Choice

The first comprehensive examination of deceptive UI design was carried out by Woodrow Hartzog in his seminal 2018 book, *Privacy's Blueprint: The Battle to Control the Design of New Technologies*.[86] In it, Hartzog argues that legislators should discourage three kinds of design: deceptive, abusive, and dangerous.[87] He defined abusive design as design that "unreasonably exploits our cognitive limitations, biases, and predictable errors to undermine autonomous decision making."[88] The difficulty, which Hartzog recognizes, is that these different types of design overlap (deceptive design, for example, is often abusive).[89]

The same is true for the categories of deception and unfairness that Daniel Solove and Woodrow Hartzog developed in analyzing the United States' FTC's enforcement of section 5 of the *Federal Trade Commission Act* (*FTC Act*), which prohibits "unfair or deceptive acts or practices in or affecting commerce."[90] This is because, given the way that the FTC has enforced the *FTC Act*, the same general type of design can be both deceptive and unfair. Solove and Hartzog provide four types of deceptive design: broken promises of privacy, general deception, insufficient notice, and data security.[91] One of their types of unfair design is deceitful data collection.[92] *Re Aspen Way* is provided as an example of it.[93] In that case, the FTC held that installing spyware on users' laptops without notice was unfair.[94] The problem, as far as classifying deceptive and unfair practices goes, is that this type of design also comes within the "insufficient notice" archetype. Another problem, as far as its application to other jurisdictions such as

85 See Parts IV to V, below.

86 *Supra* note 4.

87 *Ibid* at 16, 121.

88 *Ibid* at 144.

89 *Ibid* at 143.

90 15 USC § 45 (2018) [*FTC Act*].

91 See Daniel J Solove & Woodrow Hartzog, "The FTC and the New Common Law of Privacy" (2014) 114:3 Colum L Rev 583 at 628–38.

92 *Ibid*.

93 *Ibid* at 641.

94 See US, Federal Trade Commission, *Re Aspen Way Enterprises, Inc* (File No 112 3151, Docket No C-4392) (2013), online (pdf): *FTC* <www.ftc.gov/sites/default/files/documents/cases/2013/04/130415aspenwaycmpt.pdf>.

Canada and Europe goes, is that it is specific to the FTC's differentiation between deceptive and unfair practices.

There is currently no universally applicable classification of the different types of deceptive privacy law related practices. This is particularly unfortunate given the global wave of privacy reform and the increasing interest in regulating deceptive design.[95]

To fill this gap, this article schematizes deception according to notice-and-choice. The scheme differentiates three types of deceptive practices.[96] The first two relate directly to notice, and the third relates directly to choice. The first is "deception that insufficiently notifies of privacy-invasive activities" (deception that insufficiently notifies). The second is "deception that notifies greater privacy protection than is actually implemented" (deception that notifies greater privacy protection). Both types of deceptive notice give users the impression that the organization in question collects and processes people's personal information in ways that are more privacy-protective than they really are. The third is "deception that impedes choice modification." This type of deception discourages people from opting-out of a particular privacy practice, or from withdrawing their consent to their personal information's continued collection and processing. The categorization is illustrated:

TABLE 1: CATEGORIZING DECEPTIVE PRACTICES RELATED TO NOTICE-AND-CHOICE

Notice	Choice
Deception that insufficiently notifies	Deception that impedes choice modification
Deception that notifies greater privacy protection	

In the above categorization and in the below discussion, to facilitate analysis and reading, this article uses the term deception to refer to both it and its intention-free counterpart (misleading). It is nonetheless important to remember that the terms are different because their differences are

95 See generally "Data Protection Laws of the World" (2021), online: *DLA Piper* <www.dlapiperdataprotection.com> (regarding the wave of privacy reform); Rieger & Sinders, *supra* note 4 at 25–26.

96 See Table 1, above.

significant. The fact that "deception" requires an organization's intention, but that "misleading" requires no mental element at all, means that the former is a much more morally culpable breach of law than the latter.[97] It may thus justify harsher sanction.[98] Relatedly, deception is more difficult for those enforcing the *CPPA* to demonstrate, as imputing intention is difficult. In any case, the above categorization and below discussion apply to both deceptive and misleading information.

III. DISTINGUISHING DIFFERENT "I AGREE MOMENTS"

In privacy law, consent is often conceptualized as occurring at a clearly identifiable moment, as it is in contract law.[99] Take Canada's once-proposed *CPPA* as an example. Clause 15(2) of that Bill is entitled, "Timing of consent," and states that "consent must be obtained at or before the time of the collection of…personal information."[100] Clause 15(3) states that "consent is valid only if" organizations fulfil certain requirements "at or before the time that the organization seeks the individual's consent."[101] Both clause 15(2) and 15(3) stress that consent occurs at a particular moment in time. This article refers to such moments as "I agree moments."

In the context of private-sector privacy law, "I agree moments" can occur in two different situations. The first is when an individual initially consents to an organization's privacy policy. The second is when an individual consents to a different privacy practice after having initially consented to one. An example of the first type is when one agrees to Facebook's terms and conditions when creating an account. An example of the second type is when one changes one's privacy preferences, or when one publishes a picture but changes the setting from "Public" to "Friends Only." What defines "I agree moments" is that they are moments of consent that occur at discrete and clearly identifiable moments in time, akin to the moments of contract formation and modification.[102] Any statute that regulates obtaining consent by deception must apply to these moments; if it did not, then the

97 See Kent Roach, *Criminal Law*, 7th ed (Toronto: Irwin Law, 2018) at 204 (referring to intent as the highest level of *mens rea*).

98 *CPPA*, *supra* note 6 at cls 93(1)–(2), (4).

99 See the text accompanying notes 157–59.

100 *CPPA*, *supra* note 6 at cl 15(2).

101 *Ibid* at cl 15(3).

102 See GHL Fridman, *The Law of Contract in Canada*, 4th ed (Scarborough, ON: Carswell, 1999) at 16–17 (discussing contract formation).

statute would apply to nothing, and a fundamental principle of statutory interpretation is that Parliament does not speak in vain.[103]

Deception *at* "I agree moments" can be distinguished from deception *beyond* "I agree moments." The latter captures all deception that does not occur at the former. It concerns the entirety of an organization's dealings with a user. In this sense, it is analogous to what the *Uniform Commercial Code* refers to as "course of performance," which comprises the conduct that arises after parties form a contract and begin to perform their obligations.[104]

The difference between deception at and beyond "I agree moments" is fundamental. Deception might occur at such moments where a trust-mark, such as a medal icon labelled "trusted security award," is displayed on the page(s) users see when first creating an account or when reading a notice regarding an updated privacy policy. Alternatively, deception beyond "I agree moments" might occur when the same trust-mark is displayed on any page appearing at times other than specific "I agree moments."

Interactions beyond these specific moments have a great impact on what Julie Cohen refers to as users' embodied experiences.[105] This is partly because individuals spend very little time interacting with online service providers' user interfaces at "I agree moments" relative to beyond. For example, while an individual may spend five minutes creating a Facebook account and reading the notices regarding updated privacy preferences, they may spend several hours interacting with Facebook's user interface on a daily or weekly basis. The changes in individuals' understanding caused by interactions beyond "I agree moments" then influence how individuals interpret the notice and choices presented to them at "I agree moments." For example, if an online service provider does not display deceptive trust-marks during "I agree moments" but displays dozens of them on every other page users interact with, then users might believe that the service provider implements privacy practices that are more protective of user-privacy than they actually are, which would influence how users understand notice and choice. Not regulating deception beyond "I agree moments" would thus harm individuals' right to consent. Whether laws that regulate deceptive design should be interpreted as actually applying beyond "I

103 See e.g. *Quebec (AG) v Carrières Ste-Thérèse Ltée*, [1985] 1 SCR 831, 20 DLR (4th) 602 ("[t]he legislator does not speak in vain" at 838).

104 See § 1-303(a).

105 Cohen, *supra* note 32 at 225–27.

agree moments" will be examined below.[106] Deceptive notice-and-choice's different moments are illustrated:

TABLE 2: ILLUSTRATING THE TYPES OF DECEPTIVE PRACTICES BY THE MOMENTS AT WHICH THEY OCCUR

	Notice	Choice
At "I agree moments"	Deception that insufficiently notifies	Deception that impedes choice modification
	Deception that notifies greater privacy protection	
Beyond "I agree moments"	Deception that insufficiently notifies	Deception that impedes choice modification
	Deception that notifies greater privacy protection	

Moments can be deceptive because of the way they are written, designed, or both. If a regulation prohibits obtaining an individual's consent by acting in a deceptive manner, then the regulation should apply to both written and designed deception.

To provide useful examples of such types of deception and illustrate how this article's framework would be implemented in practice, this article looks to previous OPC investigations and FTC settlements. Looking to the FTC's enforcement of section 5 of the *FTC Act* will also prove insightful because it is perceived as having precedential weight in the United States.[107] And just like the United States' jurisprudence has persuasive authority in Canada,[108] the FTC's settlements should have persuasive authority over the OPC and the courts enforcing Canadian privacy law. Similarly, examining the OPC's investigations of alleged breaches of *PIPEDA*, along with the reasoning it relied on to determine whether a breach actually occurred, will shed light on how far the OPC has and might be willing to go in interpreting facts relating to deceptive notice-and-choice. A bonus of laying out the OPC's investigations is that few, if any, doctrinal articles have comprehensively surveyed a thematic area of the OPC's findings, as this article seeks to do.

106 See Part V-B, below.

107 Solove & Hartzog, *supra* note 91 at 619–22.

108 See Adam M Dodek, "Comparative Law at the Supreme Court of Canada in 2008: Limited Engagement and Missed Opportunities" (2009) 47 SCLR (2d) 445 at 463–65 (discussing how Justice Binnie engaged in "doctrinal comparativism" and how "comparative experience establishes a presumption" for Justice Deschamps in the context of the right to be free from arbitrary search and seizures).

IV. DECEPTIVE "I AGREE MOMENTS"

This part exemplifies deceptive "I agree moments." It discusses text-based deception first, and design-based deception second. It is important to remember that deception is being used synonymously with misleading, for ease of analysis and reading, but that the terms differ in that the former requires intention whereas the latter requires no mental element.

A. Deceptively Written "I Agree Moments"

The OPC already investigates written deception that insufficiently notifies at "I agree moments." *PIPEDA* Principles 4.3.2 and 4.3.3 required organizations to make "reasonable effort" to notify individuals of their privacy practice in a "reasonably understand[able]" fashion.[109] In *PIPEDA* Case Summary #2003-148, an airline notified individuals that the purpose for collecting their information would be "baggage tracing."[110] The airline, notably, failed to specify that this included filing personal information in a tracing system used by third-party air transport organizations.[111] The OPC held that the notice was "not…stated…in a manner reasonably conducive to the complainant's understanding of how the information would actually be used."[112] As a result, it led reasonable people to believe that their data would not be filed in a tracing system used by third-party organizations when it would be. The notice did so by representing a half-truth: by only telling half the story. The OPC came to a similar conclusion in *PIPEDA* Report of Findings #2009-008, where Facebook notified users that their new privacy practice's purpose was "preserving the integrity of the site."[113] They held that "vague and open-ended" notices do not lead reasonable people to beliefs that capture the essence of an organization's privacy

109 *Supra* note 5.

110 Office of the Privacy Commissioner of Canada, Air Traveller Offended by Airline's Information Requirements for Baggage Claim, PIPEDA Case Summary #2003-148 (Ottawa: OPC, 2003).

111 *Ibid.*

112 *Ibid.*

113 Office of the Privacy Commissioner of Canada, *Report of Findings Into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) Against Facebook Inc Under the Personal Information Protection and Electronic Documents Act*, by Elizabeth Denham (Ottawa: OPC, 2009) at para 51. See also Office of the Privacy Commissioner of Canada, *Facebook Agrees to Stop Using Non-Users' Personal Information in Users' Address Books*, PIPEDA Report of Findings #2018-003 (Ottawa: OPC, 2018) at para 82.

practices and thus undermines informed choice and consent.[114] The FTC, not surprisingly, also regulates vague notice.[115] So too should any statute that regulates deceptive practices.

The OPC has never explicitly investigated written deception that notifies greater privacy protection at "I agree moments." This is because this type of deception seems uncommon relative to written deception that insufficiently notifies and design-based deception that notifies greater privacy protection. All types of deceptive notice give users the impression that the organization in question collects and processes people's personal information in ways that are more privacy-protective than they really are. However, it might be easier for an organization to engage in deceptive notice by adopting a vague and open-ended privacy policy (deception that insufficiently notifies),[116] or by adding design elements such as trust-marks to a privacy policy (deception that notifies greater privacy protection),[117] than by using language that seems to but does not actually promise more privacy protection than is actually implemented.

With this said, the OPC's Early Resolved Case Summary #2017-003 provides insight into what this type of deception might look like.[118] The case concerned a bank engaging in credit score inquiries on an individual's credit file after the individual had closed their banking account. The bank's privacy policy stated that the bank "retained the ability" to perform credit inquiries after an individual registers for a credit product, but noted that an individual "could withdraw their consent at any point in time" if they wished the credit inquiries to cease. The bank continuing to perform

114 Office of the Privacy Commissioner of Canada, *Air Canada Allows 1% of Aeroplan Membership to "Opt Out" of Information Sharing Practices*, PIPEDA Case Summary #2002-42 (Update) (Ottawa: OPC, 2005).

115 See e.g. US, Federal Trade Commission, *Re Sears Holdings Management Corporation* (File No 082 3099, Docket No C-4264) (2009), online (pdf): *FTC* <www.ftc.gov/sites/default/files/documents/cases/2009/09/090604searscmpt.pdf> (respondent Sears invited users to install a software application on their computer that would track their "online browsing," but Sears failed to specify that "online browsing" included information provided in secure sessions when interacting with third-party websites, shopping carts, online accounts, and headers of web-based email).

116 See e.g. Office of the Privacy Commissioner of Canada, *Profiles on PositiveSingles.com Dating Website Turn up on Other Affiliated Dating Websites*, PIPEDA Report of Findings #2013-003 (Ottawa: OPC, 2013) at paras 60–68 [Office of the Privacy Commissioner of Canada, *PositiveSingles*].

117 See e.g. the text accompanying notes 126–27.

118 Office of the Privacy Commissioner of Canada, *Bank Agrees to Cease Performing Credit Checks on Individuals Who Are No Longer Clients* (Ottawa: OPC, 2018).

credit inquiries after an individual closed their account did not breach the privacy policy because closing one's account does not necessarily entail withdrawing one's consent to continued credit score inquiries. However, the wording may lead individuals to the reasonable belief that it does, as the complainant seemed to think.[119] Granted, as far as written-deceptive notice at "I agree moments" goes, the line separating insufficient notice and notice that promises greater privacy protection is blurry. Deception that notifies greater privacy protection is much more common, and problematic, where it is design-based at "I agree moments," and when it occurs beyond these specific moments.[120]

The OPC has also never investigated written deception that impedes choice modification at these moments. Choice modification at "I agree moments" occurs when a user has the opportunity to change their default choice from opt-in to opt-out, or *vice versa*. *PIPEDA* and the courts interpreting it are clear that whether consent can be default opt-out (meaning an individual has consented by default to their personal information's processing) depends on the personal information's sensitivity and the individual's reasonable expectations.[121] The Federal Court of Appeal has likewise held that consent is invalid if an individual is not notified of their choice to opt-out.[122] *PIPEDA* and the OPC are silent, however, on how the choice itself must be presented in words. See for example the FTC's opinion in *Re Facebook, Inc.*, where Facebook notified users that their updated privacy policy allows facial recognition technology to identify people in user-uploaded pictures and videos "[i]f it is turned on."[123] Facebook users were clearly notified of the privacy-invasive activity, but the notice's wording implied that users' default choice was opt-out when it was really opt-in. As a result, reasonable people were led to believe that the choice they exercised in their privacy preferences would prevent Facebook's facial recognition technology from collecting their data, when in reality their data was collected if they did not take the time to change their privacy

119 *Ibid*.

120 See e.g. the text accompanying notes 126–127.

121 See *Englander v Telus Communications Inc*, 2004 FCA 387 at para 60 [*Englander*]; *Townsend v Sun Life Financial*, 2012 FC 550 at para 25; *PIPEDA*, *supra* note 5 at Principles 4.3.5–4.3.6. See also *CPPA*, *supra* note 6 at cl 15(4).

122 *Englander*, *supra* note 121 at para 67.

123 US, Federal Trade Commission, *Re Facebook, Inc* (File No 092 3184, Docket No C-4365) (2019) at para 14, online (pdf): *FTC* <www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf >.

preferences.[124] Facebook's notice was deceptive to impede choice modification, and should therefore be regulated by any statute that prohibits practices that attempt to obtain consent by deception.

B. Deceptively Designed "I Agree Moments"

The OPC has only once investigated designed deception that notifies greater privacy protection at "I agree moments," and this was in its landmark 2016 joint investigation with Australia's Privacy Commissioner into Ashley Madison.[125] Ashley Madison (AM) is a dating website for married persons. AM's registration page displayed trust-marks that conveyed a high level of security, including a medal icon labelled "trusted security award," a lock icon indicating the website was "SSL secure," and a badge that the website offered "100% discrete service."[126] Despite the fact that AM's Terms of Service contradicted the trust-marks by warning users that their personal information's security could not be guaranteed, the OPC held that the UI's design was "material in the reasonable user's consideration of whether to choose to provide AM with their personal information."[127] The OPC concluded, for the first and only time, that an organization violated *PIPEDA*'s often overlooked prohibition on "consent obtained by deception."[128] Two elements influenced the OPC's reasoning in the AM case. First: the fact that some individuals might not have consented *but for* the fictitious trust-marks.[129] Second: the fact that the trust-marks appeared to have been *deliberately* designed to deceive.[130]

One question is whether both "but for" causation and an organization's intention to mislead should be required to prove deception. Regarding the

124 *Ibid* at paras 144–54.

125 See *Joint Investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner*, PIPEDA Report of Findings #2016-005 (Ottawa: OPC, 2016) [Office of the Privacy Commissioner, *AM*].

126 *Ibid* at para 51.

127 *Ibid* at paras 51–52, 191.

128 *PIPEDA*, *supra* note 5 at Principles 4.3.5.

129 Office of the Privacy Commissioner, *AM*, *supra* note 125 ("it is reasonable to expect that some individuals might have chosen not to share their personal information with [Avid Life Media Inc] if they had not been misled at registration by the fictitious security trust-mark" at para 192).

130 *Ibid* ("appears to have been designed by [Avid Life Media Inc] to *deliberately* foster a false general impression" at para 193). See also Denham, *supra* note 113 (relying on a different principle than 4.3.5, the OPC held that "allegations of deception are serious and require at least some evidence of an intent to deceive" at para 377).

latter, as discussed above, deception necessitates intention.[131] If government seeks to enact a lower standard for finding a harmful practice, then it should use the intention-free term of misleading. Regarding "but for" causation, whether it is required depends on the given statutory provision's wording. If a statute states that "an organization must not obtain" an individual's consent by using a deceptive practice, then "but for" causation is required. If the statute merely states that an organization "must not attempt to obtain" an individual's consent by using a deceptive practice, then the organization in question does not need to have successfully obtained consent. Given that "attempt" necessitates intention,[132] then the only thing that must be shown to find a breach of statute is a deceptive practice.

Moving on, the OPC has never investigated designed deception that insufficiently notifies at "I agree moments."

The FTC's opinion in *Re Snapchat, Inc.* provides an example of this type of deception.[133] Snapchat is a mobile app that allows users to send pictures to their friends. During registration, prior to the FTC settlement, it prompted users to "Enter [their] mobile number to find [their] friends on Snapchat!"[134] The prompt implied that only a user's mobile phone number would be collected upon registration. But upon entering their mobile number, Snapchat also collected the names and phone numbers of all the contacts in a user's mobile device address book.[135] This amounts to design-based deception that insufficiently notifies by half-truth.[136] Snapchat's privacy policy, though, expressly stated that they would not collect users' mobile device's address book.[137] The FTC could have therefore simply resolved this case by pointing to a breach of Snapchat's privacy policy. They nonetheless took the opportunity to shine a spotlight on design-based deception that insufficiently notifies at "I agree moments."

---

131 See Part II-B, above.

132 See e.g. *Union of Bank Employees, Local 2104 v Canadian Imperial Bank of Commerce* (1985), 10 CLRBR (NS) 182 at 194, 85 CLLC 16,021: "'attempt' can lead us to no other conclusion but that there must be an intention on the part of the party alleged to have violated the section to have done what is prohibited by that section. No intention would be required were the word 'attempt' not included in that subsection; the word, however, is there and must be given its meaning."

133 US, Federal Trade Commission, *Re Snapchat, Inc* (File No 132 3078, Docket No C-4501) (2014), online (pdf): *FTC* <www.ftc.gov/system/files/documents/cases/141231snapchatcmpt.pdf>.

134 *Ibid* at para 25.

135 *Ibid* at para 26.

136 *Ibid* at para 29 (referring to false or misleading).

137 *Ibid* at para 30.

The OPC already investigates designed deception that impedes choice modification at "I agree moments." In its Guidelines for obtaining meaningful consent, which indicates how it interprets *PIPEDA*, the OPC states that choices to opt-in or opt-out must be "easily accessible," defined in subsequent investigations as "immediate and convenient."[138] While this requirement has only been applied to opting-out of personal information processing for *secondary purposes* (meaning different purposes than individuals first consented to), the OPC once applied this requirement in *obiter* to initial "I agree moments."[139] In both situations, opting-out by calling a 1-800 number or checking off a box was deemed a reasonably immediate and convenient design.

However, UI designs that render modifying one's choice inaccessible are not deceptive or misleading because they do not lead users to believe something relating to their choices that is not true. They may constitute nudges in the sense that they affect individuals' "choice architecture" and thus behaviour.[140] But not all nudges are manipulative,[141] and even if they were, prohibiting deceptive practices falls short of prohibiting manipulative practices.

Deceptive design that does impede choice modification at "I agree moments" is similar to written deception that impedes choice modification at "I agree moments." For instance, similar to Facebook using the words "[i]f it is turned on" to announce a new facial recognition technology that they deployed,[142] a green check-mark next to the word "privacy" on a notice announcing a new practice might lead users to believe that their default choice is opt-out when it is really opt-in.

V. DECEPTION BEYOND "I AGREE MOMENTS"

Interpreting laws that regulate deceptive practices as applying beyond "I agree moments" would focus on the entirety of a company's dealing with

138 Office of the Privacy Commissioner of Canada, "Guidelines for obtaining meaningful consent" (May 2018), online: *OPC* <www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/> [Office of the Privacy Commissioner of Canada, "Meaningful Consent"]; *PIPEDA*, *supra* note 5 at Principle 4.3.5.

139 See e.g. Office of the Privacy Commissioner of Canada, *Bank Does Not Obtain the Meaningful Consent of Customers for Disclosure of Personal Information*, PIPEDA Case Summary #2003-192 (Ottawa: OPC, 2003). See also Office of the Privacy Commissioner of Canada, *Stolen Laptop Engages Bank's Responsibility*, PIPEDA Case Summary #2005-289 (Ottawa: OPC, 2005) (applying to initial "I agree moments").

140 Thaler & Sunstein, *supra* note 58 at 6.

141 See Part II-A, above, for a definition of deception.

142 See the text accompanying notes 123–24.

a user. It would more fully appreciate users' embodied experiences and understandings, and would strengthen their right to consent as a result.[143] The OPC has never investigated any type of deceptive notice-and-choice beyond "I agree moments." To provide examples of such deception, this part first surveys different FTC settlements.[144] It then determines whether laws that regulate deceptive practices can and should be interpreted as applying beyond "I agree moments" by looking to notions of ongoing consent in other areas of law, privacy statutes' overall schemes, and doctrine and expert opinion.

A. Examples of Deception Beyond "I Agree Moments"

The most prevalent and pernicious form of deception beyond "I agree moments" is deception that notifies greater privacy protection than is actually implemented.[145] *Re PayPal, Inc.* provides an example of such deception.[146] The case concerned Venmo, a mobile phone application that facilitates sending money to friends. The application publicly displayed all peer-to-peer transactions on a user's profile page.[147] Users who wished to restrict the visibility of their future transactions could do so via the application's "'[s]ettings' menu."[148] In this respect, Venmo is like most other mobile applications that have a "settings" menu. The problem with Venmo's was that its design led users to believe that changing the setting labelled "default audience" for "future transactions" to "participants only" would limit their transactions' visibility. But to actually do so, users had to change a second setting, which they might have realized if the first setting was labelled differently or if the second one was more prominently displayed.[149] *PayPal* thus provided the FTC with the opportunity to hold that a settings menu's design can be deceptive even if the organization implements users' choices.

Another example of design-based deception beyond "I agree moments" would be if an online service provider suddenly adds trust-marks that

143 Cohen, *supra* note 32 at 225–27.

144 See Part V-A, below.

145 Hartzog, *Privacy's Blueprint*, *supra* note 4 at 169.

146 US, Federal Trade Commission, *Re Paypal, Inc* (File No 162 3102, Docket No C-4651) (2018), online (pdf): *FTC* <www.ftc.gov/system/files/documents/cases/1623102_c-4651_paypal_venmo_complaint_final.pdf> [*PayPal*].

147 *Ibid* at para 17.

148 *Ibid* at para 18.

149 *Ibid* at paras 19–25.

convey greater privacy protection than is actually implemented to their platform's homepage, or if that same homepage states that "we take your privacy very seriously and are doing our utmost to protect it" when this statement falls short of what the organization actually does and notified users that they would do in its privacy policy.[150]

Deception that insufficiently notifies beyond "I agree moments" is less common than deception that notifies greater privacy protection. This is because it is more likely to regard deception by silence rather than active concealment or half-truth. Further, holding companies responsible for all silences that lead individuals to believe that an organization's privacy practice is more protective might create unduly onerous duties to notify that only inundate users with information.[151] With this said, there are at least two general forms of deception that insufficiently notify beyond "I agree moments." The first is where organizations fail to redress deception that notifies greater privacy protection. In *PayPal*, for example, Venmo could have notified their users about how their privacy preference settings worked, but never did. The second occurs where an organization notifies users about their privacy practices on their homepage, for example, in a way that leads individuals to believe that they protect it more than they actually do.

The final type of deception beyond "I agree moments" is deception that impedes choice modification. As shown above, not all practices that impede choice modification constitute deception.[152] For example, in *Re Sony BMG Music Entertainment,* digital rights management software was installed on consumers' computers in a way that consumers were unable to find or remove the software through reasonable effort.[153] Amazon provides a more famous, and yet-to-be-investigated, example. To delete one's Amazon account, users have to click on "Help," "Contact Us," "Prime or Something Else," "Login and Security," and then, finally, "Close My Account," only to then be forced to have a "live chat with an Amazon associate" explaining

150 Office of the Privacy Commissioner of Canada, *PositiveSingles*, *supra* note 116 at paras 52–54 (discussing how information linked to a button labelled "How we protect your privacy" uses language indicating that the organization protects peoples' privacy more than they actually do and notified users that they would).

151 Nissenbaum, *supra* note 24 at 36 (discussing the "privacy paradox" and consequent fact that providing users with more information is not helpful).

152 See the text accompanying notes 140–41.

153 US, Federal Trade Commission, *Re Sony BMG Music Entertainment* (File No 062 3019, Docket No C-4195) (2007) at para 20, online (pdf): *FTC* <www.ftc.gov/sites/default/files/documents/cases/2007/01/070130cmp0623019.pdf>.

why they wish to delete their account.[154] Both UI designs are problematic because they make exercising one's right to withdraw consent more difficult. They constitute nudges because they alter individuals' behaviour by altering their "choice architecture." But they are not false, misleading, or deceptive because they do not lead users to believe something relating to choice that is not true.

An example of a practice impeding choice modification beyond "I agree moments" that is deceptive is an organization providing users with information or engaging in a practice that reasonably leads individuals to believe that they have withdrawn their consent when they really had not. To return to the Amazon example, this might occur if a large green checkmark appears after users click "Close My Account" because this might give them the reasonable impression that they do not need to have a "live chat with an Amazon associate" to actually withdraw their consent.

B. Interpreting Statutes by Looking to Ongoing Consent

In Canada, the modern approach to statutory interpretation is characterized by Elmer Driedger's modern principle, which holds that "the words of an Act are to be read in their entire context and in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act, and the intention of Parliament."[155] This "entire context" includes the Act's legislative scheme and broader legal context. In reading an Act, it is presumed that the legislature does not intend to change the common law.[156] At issue is whether "obtaining or attempting to obtain consent" occurs only at identifiable "I agree moments." What follows is an interpretation of privacy law that looks to broader legal contexts, privacy statutes' general scheme, as well as doctrine and expert opinion.

The first legal context one might look to for guidance is contract law. Contractual consent is understood as being expressed in an instant at a

154 Nerdwriter1, "How Dark Patterns Try to Trick You Online" (28 March 2018) at 00h:00m:19s, online (video): *YouTube* <www.youtube.com/watch?v=kxkrdLI6e6M>.

155 *Rizzo & Rizzo Shoes Ltd (Re)*, [1998] 1 SCR 27 at para 21, 154 DLR (4th) 193, citing Elmer A Driedger, *The Construction of Statutes*, 2nd ed (Toronto: Butterworths, 1983) at 87; *Bell ExpressVu Limited Partnership v Rex*, 2002 SCC 42 at para 26, citing Elmer A Driedger, *The Construction of Statutes*, 2nd ed (Toronto: Butterworths, 1983) at 87 [*Bell ExpressVu*]; *R v Appleby*, 2009 NLCA 6 at para 21; Sullivan, *supra* note 76 (referring to Elmer Driedger's modern principle as the "mantra of statutory interpretation in Canada" at 42).

156 Sullivan, *supra* note 76 at 156.

theoretically identifiable moment.[157] Once consent is expressed, the contract is formed and the parties' obligations become fixed. There is, granted, some doctrinal debate about whether courts should regard contracts as crystallizing over time, instead of forming in an instant, to better accord with business practice.[158] But Canadian courts have generally rejected this approach, insisting that contractual consent occurs at clearly identifiable moments.[159] If the same logic were to apply to interpreting the act of consenting, then statutory provisions applying to obtaining consent by enaging in deceptive practices would not apply beyond "I agree moments."

Contract and privacy law, however, are fundamentally different. Contracts are about alienating one's property or labour.[160] Privacy, on the other hand, is a traditionally inalienable human right that the Supreme Court has recognized as inextricably linked to other traditionally inalienable human rights.[161] This has not stopped some from suggesting that individuals should have property rights over their personal information so that they could transfer it in exchange for financial compensation.[162] Propertizing privacy is, after all, not inherently inconsistent with the common law.[163] However, it might be inconsistent with Canadian civil law. The civil law's "patrimony" organizes all rights that have financial value, excluding a person's rights and obligations that do not have economic value, which are

157 See SM Waddams, *The Law of Contracts*, 4th ed (Aurora, ON: Canada Law Book, 1999) at 66–67; Fridman, *supra* note 102 at 16–17.

158 See e.g. Margaret H Ogilvie, "Surely the Next to Last Shot in the Battle of Forms!" (2011) 51:2 Can Bus LJ 307 at 308–309, 313.

159 See generally Mary J Shariff & Kevin Marechal de Carteret, "Revisiting the Battle of the Forms: A Case Study Approach to Legal Strategy Development" (2009) 9 Asper Rev Intl Bus & Trade L 21; *Cariboo-Chilcotin Helicopters Ltd v Ashlaur Trading Inc*, 2006 BCCA 50 (referring to the "battle of forms" at para 18).

160 See generally AM Honoré, "Ownership" in AG Guest, ed, *Oxford Essays in Jurisprudence* (London, UK: Oxford University Press, 1961) 107 at 107 (stating that property rights are usually reflected in contractual or succession arrangements).

161 See *Dagg v Canada* (*Minister of Finance*), [1997] 2 SCR 403 at para 66, 148 DLR (4th) 385 (recognizing that privacy is inextricably linked to other human rights, such as the right to life, liberty, and security of the person). See also *Universal Declaration of Human Rights*, GA Res 217A (III), UNGAOR, 3rd Sess, Supp No 13, UN Doc A/810 (1948) 71, art 12.

162 See e.g. James Rule & Lawrence Hunter, "Towards Property Rights in Personal Data" in Colin J Bennett & Rebecca Grant, eds, *Visions of Privacy: Policy Choices for the Digital Age* (Toronto: University of Toronto Press, 1999) 168; Richard S Murphy, "Property Rights in Personal Information: An Economic Defense of Privacy" (1996) 84:7 Geo LJ 2381 at 2416.

163 Cofone, "Ownership", *supra* note 19 at 17–20 (noting that proposals to propertize privacy are really about property rules and not property rights).

known as personality rights.[164] Personality rights are "extrapatrimonially bound up in the person's very existence" and are therefore not susceptible to exchange: they are inalienable.[165] Per the Civil Code of Quebec, privacy constitutes such an inalienable extrapatrimonial personality right.[166] As Quebec's Minister of Justice explained, the fact that privacy is so connected to one's personality means that privacy cannot be contractually ceded.[167] Granted, the Supreme Court of Canada recently recognized that the personality right to one's own image has dual extrapatrimonial and patrimonial aspects,[168] evidencing the civil law's "essential tension between privacy-based and property-based conceptions of personality."[169] Nonetheless, not only does Quebec's proposed Bill 64 not grant a property right over personal information—neither does the *CCPA*, the *New York Privacy Act*, or other proposed bills in the United States.[170]

Further, there is an emerging trend whereby the traditionally inalienable personality rights and harms that privacy implicates—reputational harm, bodily harm, and sexual harm[171]—are deemed to involve "ongoing consent." Ongoing consent, here, does not refer to the notion that consent remains indefinitely valid once it is given.[172] Rather, it refers to the notion

164 Nicolas Kasirer, "Translating Part of France's Legal Heritage: Aubry and Rau on the *Patrimoine*" (2008) 38:2 RGD 453 at 464.

165 *Ibid*.

166 *Supra* note 29, art 3. See also *Savard c Curtin-Savard*, 2012 QCCS 3523 ("les droits de la personnalité sont extrapatrimoniaux, en ce qu'ils sont intransmissibles, incessibles, insaisissables et imprescriptibles" at para 50).

167 See Quebec, Ministère de la justice, *Commentaires du ministre de la Justice: Le Code civil du Québec*, vol 1 (Québec, Publications du Québec, 1993) ("[c]et article pose également la règle de l'incessibilité des droits de la personnalité, car même si en certains cas ces droits ont des incidences sur le patrimoine, ils sont tellement liés à la personnalité qu'ils ne peuvent faire l'objet d'une cession" at 6).

168 See *Aubry v Éditions Vice-Versa*, [1998] 1 SCR 591 at paras 51, 67, 157 DLR (4th) 577.

169 Eric H Reiter, "Personality and Patrimony: Comparative Perspectives on the Right to One's Image" (2002) 76:3 Tul L Rev 673 at 673.

170 Bill 64, *supra* note 20; *CCPA*, *supra* note 20; *NYPA*, *supra* note 82; Cofone, "Ownership", *supra* note 19 (citing Julie Cohen as stating that "'none of the bills recently before Congress purports, in so many words, to recognize property rights in personal data'" at 14).

171 See e.g. Ignacio N Cofone, "Online Harms and the Right to be Forgotten" in Ignacio N Cofone, ed, *The Right to be Forgotten: A Canadian and Comparative Perspective* (London, UK: Routledge, 2020) 1 at 5–9 (discussing different harms that privacy implicates).

172 See Michelle J Anderson, "Marital Immunity, Intimate Relationships, and Improper Inferences: A New Law on Sexual Offences by Intimates" (2003) 54:5 Hastings LJ 1465 at 1475 (noting that this notion of ongoing consent justified the marital rape exemption).

that consent is ongoing and can thus be revoked at any moment.[173] Take the law of health and consent to medical treatment as an example. As the late Lorne Rozovsky put it:

> To many in the care-giving professions, consent is nothing more than obtaining a patient's signature on a "consent" form. Such an impression belies the fact that consent is a "process" which involves a treatment relationship and effective communication…the signed consent form is nothing more than *evidence of* consent. It is not *the* consent itself.[174]

Consent is an ongoing process in health law.[175] What this means in practice is that health practitioners must disclose information to patients that might influence their consent to treatment.[176] Because a patient's consent is determined by constantly evolving facts, such as their personal lifestyle and economic situation, the specific treatment that is to be performed, and the practitioner that will perform it, health practitioners must get to know their patients and maintain effective channels of communication with them.[177] Not surprisingly, then, the Canadian guidelines on consent to biomedical research stress the importance of continuously providing research participants with all the information they require to maintain their ongoing consent throughout a research project.[178]

Similar can be said regarding sexual assault law, where the Supreme Court has defined consent, according to Parliament's intention, as an ongoing state of mind.[179] As a result, one must communicate consent to

---

173 See e.g. Randall R Curren, "Punishment and Inclusion: The Presuppositions of Corrective Justice in Aristotle and What They Imply" (1995) 8:2 Can JL & Jur 259 (discussing the Platonic idea that a "legitimate rule of law rests in *real* and *ongoing* consent" at 265 [emphasis in original]); John Mukum Mbaku, "Entrenching Constitutionalism in African Countries: Lessons from America's Founding Fathers" (2019) 55:1 Tex Intl LJ 89 at 139–40 (discussing the social contract principle that government stands on peoples' original and ongoing consent).

174 Lorne Elkin Rozovsky, *The Canadian Law of Consent to Treatment*, 2nd ed (Toronto: Butterworths, 1997) at 1 [emphasis in original].

175 *Ibid*.

176 See *Hopp v Lepp*, [1980] 2 SCR 192 at 210, 112 DLR (3d) 67; *Reibl v Hughes*, [1980] 2 SCR 880 at 884, 114 DLR (3d) 1.

177 Rozovsky, *supra* note 174 at 9–13.

178 See e.g. Interagency Advisory Panel on Research Ethics, *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans*, Catalogue No MR21-18/2010E-PDF (Ottawa: PRE, 2010), arts 3.2–3.3.

179 See e.g. *R v JA*, 2011 SCC 28 at paras 3, 39 (referring to an "ongoing conception of consent, rather than advance consent to a suite of activities" at para 39).

each sexual act or purpose.[180] Saskatchewan's legislature has recently followed this trend by amending *The Privacy Act* to make it so that distributing an intimate image of an individual requires their ongoing consent.[181]

It would, accordingly, seem inconsistent with the broader legal context if Canadian privacy law is not deemed to require ongoing consent. This is especially true considering that most statutes, similar to the law relating to sexual harms, require organizations to obtain fresh consent when new and different purposes for processing an individual's personal information arise.[182]

Viewing consent as ongoing also accords with privacy statutes' overall scheme in several ways. As Jennifer Barrigar, Jacquelyn Burkell and the late Ian Kerr stated, "the *continued use* of an individual's personal information must be understood as a necessary consequence, not of the initial consent to collect the information, but rather of that person's *continuing consent* to the organization to use that information."[183] Their opinion was grounded in the fact that individuals who consent to their personal information's processing still retain a right to control their information. This so-called right to control refers to several different rights, such as the right to accuracy or to correct (*i.e.*, the right to request that one's personal information be corrected if it is inaccurately represented by an organization), and the right to withdraw consent and have one's personal information deleted.[184] One may rebut Kerr's understanding of "consent-as-ongoing-agency" by claiming that the right to control is artificial insofar as users rarely exercise their right to withdraw consent under *PIPEDA*. But just because individuals

180 See *R v Goldfinch*, 2019 SCC 38 at para 44.

181 RSS 1978, c P-24. See also *The Privacy Amendment Act, 2018*, SS 2018, c 28, s 7.5.

182 *GDPR*, *supra* note 20, para 32. See also Ignacio N Cofone & Adriana Z Robertson, "Consumer Privacy in a Behavioral World" (2018) 69:6 Hastings LJ 1471 at 1503 (noting that organizations describing the informativeness of the personal data they collect from individuals is essential to adequate notice and informed consent); Cofone, "Ownership", *supra* note 19 at 38–47 (describing purpose specification and the importance of requiring that stated purposes be specific).

183 Jennifer Barrigar, Jacquelyn Burkell & Ian Kerr, "Let's Not Get Psyched Out of Privacy: Reflections on Withdrawing Consent to the Collection, Use and Disclosure of Personal Information" (2006) 44:1 Can Bus LJ 54 at 59–60 [emphasis in original].

184 For the right to accuracy, see e.g. *PIPEDA*, *supra* note 5 at Principles 4.6, 4.9.5 ("[w]hen an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required" at Principle 4.9.5); *NYPA*, *supra* note 82, s 1102(5). For the right to delete and withdraw consent, see e.g. *NYPA*, *supra* note 82 ("[i]mmediately delete the personal data if consent is withheld, denied, or withdrawn", s 1102(2)(g)(iii)); *CCPA*, *supra* note 20 at § 1798.105.

infrequently exercise a right does not mean that it ceases to exist or is irrelevant in statutory interpretation.[185]

The OPC, in its Guidelines for obtaining meaningful consent, follows Kerr in writing that "informed consent is an ongoing process" that changes as circumstances change.[186] It elaborates by stating that organizations should not rely on consent that occurred in a static moment in time, but should rather treat it as a dynamic and interactive process.[187] Implied is that all notices inform individuals' choice to withdraw their consent, and that permitting deceptive notices beyond "I agree moments" would undermine individuals' right to an informed consent process. This particular element of the OPC's Guidelines for obtaining meaningful consent, however, is not binding.[188] It nonetheless remains an expert's opinion on how the right to consent should be regarded.

Not regulating deception beyond "I agree moments" would wholly undermine meaningful, free, and informed consent. In Canada, it would also be inconsistent with the broader legal context in which privacy law is situated. It would allow organizations to deceive users into never exercising their right to withdraw consent or request their personal information's erasure. Accordingly, given that all embodied user experiences implicate consent, statutes that regulate deceptive practices must be applied holistically to the entirety of a company's dealings with individuals.

CONCLUSION

Deception's impact on individuals' right to consent is increasingly explored. The problem is that there is no unified analysis of how such a statutory provision might apply. This article determines how privacy statutes that regulate deceptive practices should apply.

In doing so, it schematizes deception according to privacy law's notice-and-choice framework, identifying three types: deception that insufficiently notifies, deception that notifies greater privacy protection, and deception that impedes choice modification. It also distinguishes the moments that these types of deception can occur: at and beyond "I agree moments." This article then concretizes this framework by surveying a thematic area of previous FTC and OPC investigations.

185 *Bell ExpressVu*, *supra* note 155 at para 26.

186 Office of the Privacy Commissioner of Canada, "Meaningful Consent", *supra* note 138.

187 *Ibid*.

188 *Ibid*.

Finally, the article demonstrates that privacy statutes should be interpreted as granting not only a right to consent, but a right to consent as an act of ongoing agency. This notion on "consent as ongoing agency" is relatively novel in privacy law, and would make it so that privacy statutes apply not only to deception at "I agree moments," but also deception beyond "I agree moments." Regulating deception beyond "I agree moments" is important, as it would cover the entirety of a company's dealings with individuals and would thus more fully appreciate individuals' embodied experiences and understandings. It would thus more closely reflect a right to meaningful consent—the right that most privacy statutes today seek to rely on to protect privacy.