Canadian Journal of Law and Technology

Volume 19
Number 2 *Technology-facilitated Gender-based Violence*

Article 8

1-2022

Responding to Deficiencies in the Architecture of Privacy: Co-Regulation as the Path Forward for Data Protection on Social Networking Sites

Laurent Cre´peau
New York University School of Law

Responding to Deficiencies in the Architecture of Privacy: Co-Regulation as the Path Forward for Data Protection on Social Networking Sites

Laurent Crépeau[*]

Abstract

Social Networking Sites like Facebook, Twitter and the like are a ubiquitous part of contemporary culture. Yet, as exemplified on numerous occasions, most recently in the Cambridge Analytica scandal that shook Facebook in 2018, these sites pose major concerns for personal data protection. Whereas self-regulation has characterized the general regulatory mindset since the early days of the Internet, it is no longer viable given the threat social media poses to user privacy. This article notes the deficiencies of self-regulatory models of privacy and contends jurisdictions like Canada should ensure they have strong data protection regulations to adequately protect the public. However, while underscoring the economic value of Big Data technologies, it posits regulation does not necessarily need to come at the cost of economic prosperity. By adopting a co-regulatory model based on regulatory negotiation, various stakeholders can come together and draft robust and flexible data protection regulations, including both tailored rules and oversight mechanisms. Beginning with a survey of the challenges and opportunities of Big Data and social networking sites (I), this article then canvasses the data protection framework of three jurisdictions, namely the United States, Canada, and the European Union (II). Finally, it shows the clear advantages of co-regulation as a regulatory paradigm and offers an outline for the regulation of social networking sites using regulatory negotiation (III).

INTRODUCTION

In the wake of the Cambridge Analytica scandal, in which personally identifiable data from as many as 80 million Facebook users was used by a political consulting firm to craft targeted ads aimed at potential Republican voters in the 2016 United States Presidential Election,[1] privacy regulation re-entered the popular mind as an apparent critical problem to palliate, which only a few weeks before seemed almost inessential. Of course, privacy protection is an important issue — one to which an already immense amount of scholarship has been dedicated.[2] However, after a few years, it has largely been forgotten and it is

---

[*] LL.M (New York University); B.C.L., J.D. (McGill University). The author would like to thank Professor Richard Janda for his comments on a preliminary version of this paper.

[1] See Carole Cadwalladr, "I made Steve Bannon's psychological warfare tool': meet the data war whistleblower", *The Guardian* (18 March 2018), online: < www.theguardian.-com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-ban-non-trump > .

unclear what has in fact changed in Facebook's data protection practices, if anything.[3]

Social Networking Sites (SNSs) are now at the forefront of privacy debates.[4] Yet, legislators often appear inefficient at implementing more robust regulations on SNSs in spite of the scrutiny that they have received.[5] Among other reasons, this could be because the population is uncertain of the benefits of regulating SNSs.[6] This sentiment is predicated, for better or for worse, on an unwillingness to see government regulation creep into the economic and social landscape. This indecisiveness combined with the deregulation philosophy that prevailed during the rise of the Internet naturally translated into the promotion of self-regulation, that is, "a regulatory system in which business representatives define and enforce standards for their sector with little or no government involvement."[7] To this day, SNSs have greatly benefitted from this regulatory approach as it has given them the leisure to develop free from burdensome regulation.[8]

---

2 See Lee A Bygrave, *Data Privacy Law: An International Perspective*, (Oxford: Oxford University Press, 2014) at 8-17 (discussing the evolution of data privacy law discourse).

3 See Pete Evans, "Facebook sees biggest stock market value drop in history as growth slows", *CBC* (26 July 2018), online: < www.cbc.ca/news/business/facebook-stock-plunge-1.4762449 > .

4 We define "social networking sites", following Boyd and Ellison, as "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system." See danah m boyd and Nicole B Ellison, "Social Network Sites: Definition, History, and Scholarship" (2008) 13:1 J Computer-Mediated Communication 210 at 211.

5 See Sean Kilpatrick, "Parliamentary report recommends modernizing Canada's privacy law", *The Globe and Mail* (4 March 2018), online: < //www.theglobeandmail.com/technology/parliamentary-report-recommends-modernizing-canadas-privacy-law/article38203771/ > ("[the report] also heeded repeated calls by the Office of the Privacy Commissioner of Canada to be given enforcement powers with "teeth," including the right to impose fines and more flexibility to choose what to investigate"); Nuala O'Connor, "Reforming the U.S. Approach to Data Protection and Privacy" (30 January 2018), online: *Council on Foreign Relations* < www.cfr.org/report/reforming-us-approach-data-protection > ("Most Western countries have already adopted comprehensive legal protections for personal data, but the United States — home to some of the most advanced, and largest, technology and data companies in the world — continues to lumber forward with a patchwork of sector-specific laws and regulations that fail to adequately protect data.").

6 See Olivia Solon, "Americans 'evenly split' over need to regulate Facebook and other big tech", *The Guardian* (1 November 2017), online: < www.theguardian.com/technology/2017/oct/31/americans-evenly-split-over-need-to-regulate-facebook-and-other-big-tech > ; Nicole Riva, "Canadian content rules for online media have weaker support, survey suggests", *CBC News* (3 June 2016), online: < www.cbc.ca/news/canada/angus-reid-crtc-canadian-content-1.3613646 > .

7 See e.g. Dennis D Hirsch, "The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?" (2011) 34 Seattle UL Rev 439 [Hirsch, "The Law"].

However, SNSs have now become too important to be left alone. First, they accrue immense amounts of personal information, the availability of which impels us to redefine the boundaries of the *private* self.[9] Second, opaque and negligent uses, excessive tracking, and lax protections of data on SNSs' part[10] pose real dangers to consumers' rights.[11] Third, with the powers of Big Data technologies readily available, personal data can be analyzed and distilled into extremely precise accounts of its users' personalities and behaviours that can be used to potentially nefarious ends.[12]

SNSs are as powerful today as ever. They constitute an extended public place with unmatched capabilities to bombard subjects with information and often accompany them in their most well-guarded intimacy. As such, they are used in many fields, including, most prominently, business and politics as a gateway inside people's minds.[13] As such, given the contemporary prevalence and extensive reach of SNSs,[14] their regulation is not only important in this day and age, but necessary. A vast literature already exists on possible methods of regulating SNSs.[15] More recently, questions about regulating hate speech,

---

8 See John T Soma, Stephen D Rynerson & Erica Kitaev, *Privacy Law in A Nutshell*, 2nd ed, (St. Paul: West Academic Publishing, 2014) at 156.

9 See John B Thompson, "Shifting Boundaries of Public and Private Life" (2011) 28:4 Theory, Culture & Society 49. Information hitherto considered strictly private increasingly becomes a commodity among others for private and public actors. Notably, China is currently establishing a "social credit system," which plans to use surveillance technology and personal data of citizens to reward them according to their "trustworthiness." See Charles Rollet, "The odd reality of life under China's all-seeing credit score system", *WIRED* (5 June 2018), online: <www.wired.co.uk/article/china-social-credit>.

10 See Annalisa Merelli, "Facebook knew Cambridge Analytica was misusing users' data three years ago and only banned the company this week", *Quartz* (17 March 2018), online: <qz.com/1231643/cambridge-analytica-illegally-obtained-data-from-50-million-facebook-users-to-run-trump-ads/>.

11 See Maria LaMagna, "The sad truth about how much your Facebook data is worth on the dark web" (6 June 2018), online: *MarketWatch* <www.marketwatch.com/story/spooked-by-the-facebook-privacy-violations-this-is-how-much-your-personal-data-is-worth-on-the-dark-web-2018-03-20> (Facebook and PayPal logins stolen by hackers due to poor data protection are sold on the dark web for a handful of dollars, exposing users to identity theft).

12 See e.g. Lesley Fair, "The FTC's settlement with Facebook: Where Facebook went wrong" (29 November 2011), online: *United States, Federal Trade Commission* <www.ftc.gov/news-events/blogs/business-blog/2011/11/ftcs-settlement-facebook-where-facebook-went-wrong>.

13 See e.g. Nicole Rustin-Paschale, "Online Behavioral Advertising and Deceptive Campaign Tactics: Policy Issues" (2011) 19 Wm & Mary Bill Rts J 907; Alexis C Madrigal, "What Facebook Did to American Democracy", *The Atlantic*, online: <www.theatlantic.com/technology/archive/2017/10/what-facebook-did/542502/>.

14 See e.g. Chris Smith, "If you thought Facebook's data collection is scary, wait until you check your Google account", *BGR* (28 March 2018), online: <bgr.com/2018/03/28/google-vs-facebook-user-data-collection/>.

misinformation[16] and political campaigning on social media have come to the forefront.[17] Many people see the spread of extreme political discourse as worrisome given the audience they can potentially reach using SNSs. Moreover, analyzing personal data to win elections now reaches bafflingly high degrees of effectiveness, targeting specific strata of the undecided voter population with just the right advertisement to make them change their mind.[18]

Self-regulation has had a prominent role in shaping the regulatory landscape of data protection. In the early years of the Internet, before SNSs like Facebook and Twitter became well-established names, this regulatory model which had come to characterize the regulation of various aspects of the Internet was already being criticized[19] and has remained controversial throughout Facebook, Twitter and other SNSs' growth.[20] Many authors continue to favour it[21] while also suggesting improvements to make this approach adequate while retaining its defining liberal, free-market approach to regulation.[22]

---

[15] See generally Eva Lievens & Peggy Valcke, "Regulatory Trends in a Social Media Context" in Monroe E Price, Stefaan Verhulst & Libby Morgan, eds, *Handbook of Media Law* (London: Routledge, 2013) 557.

[16] See Jack Nicas, "Alex Jones and Infowars Content Is Removed From Apple, Facebook and YouTube", *The New York Times* (6 August 2018), online: < www.nytimes.com/2018/08/06/technology/infowars-alex-jones-apple-facebook-spotify.html >. The increasing prevalence of hate speech online has already pushed EU regulators to react with its Code of Conduct on Countering Illegal Hate Speech Online. See Hui Zhen Gan, "Corporations: The Regulated or The Regulators? The Role of IT Companies in Tackling Online Hate Speech in the EU" (2017) 24 Colum J Eur L 111. See Karen Hao, "How Facebook and Google Fund Misinformation", (20 November 2021), online: MIT Technology Review < https://www.technologyreview.com/2021/11/20/1039076/facebook-google-disinformation-clickbait/ >

[17] See Eitan D Hersch, *Hacking the Electorate: How Campaigns Perceive Voters* (Cambridge: Cambridge University Press, 2015).

[18] Timothy Summers, "Facebook is killing democracy with its personality profiling data", *The Conversation* (21 March 18), online: < theconversation.com/facebook-is-killing-democracy-with-its-personality-profiling-data-93611 >; Tahiat Mahboob, "How Facebook was Harnessed to Micro-Target Voters and Promote Donald Trump", *CBC* (28 March 2018), online: < www.cbc.ca/passionateeye/features/how-facebook-was-harnessed-to-micro-target-voters-and-promote-donald-trump >.

[19] See e.g. Jonathan P Cody, "Protecting Privacy Over the Internet: Has the Time Come to Abandon Self-Regulation?" (1999) 48:4 Cath U L Rev 1183; Mary J Culnan, "Protecting Privacy Online: Is Self-Regulation Working?" (2000) 19:1 J Pub Pol'y & Marketing 20.

[20] See Hirsch, "The Law," *supra* note 7; Asma Vranaki, "Regulating Social Networking Sites: Facebook, Online Behavioral Advertising, Data Protection Laws and Power" (2017) 43 Rutgers Computer & Tech LJ 168.

[21] See e.g. Catherine Schmierer, "Better Late Than Never: How the Online Advertising Industry's Response to Proposed Privacy Legislation Eliminates the Need for Regulation" 17:4 Rich JL & Tech 1.

[22] See e.g. Timothy E Deal, "Moving Beyond 'Reasonable': Clarifying the FTC's Use of Its Unfairness Authority in Data Security Enforcement Actions" (2016) 84:5 Fordham L Rev 2227; Ira S Rubinstein, Ronald D Lee & Paul M Schwartz, "Data Mining and

This article echoes much of the criticism already made of self-regulation and offers additional arguments for its insufficiency in the context of SNSs. It argues that commitment to a co-regulatory approach is necessary to ensure the proper regulation of SNSs' data protection practices while fostering innovation and profitable access to data for SNSs and their business partners. Co-regulatory models favour implementing clear data protection obligations for SNSs and empowering regulators with new powers to monitor SNS data protection practices. At the same time, it looks to keep the most useful aspects of self-regulation to facilitate sophisticated and context-specific rulemaking and information-sharing.

Part I gives an overview of the shortcomings of SNSs' data protection practices, looking specifically at the problems posed by online behavioural advertising and third-party data sharing. Part II looks at data protection laws in the United States, Canada, and the European Union. Finally, Part III underscores the failures of self-regulation and proposes a co-regulatory approach that promotes transparency and accountability through framework legislation and regulatory negotiations to balance the economic benefits of data with adequate protection.

PART I: *THE DATA LANDSCAPE AND SOCIO-CULTURAL AND ECONOMIC ASPECTS OF DATA*

In this Part, we begin by briefly describing the main aspects of Big Data as regards personal data processing and the data-driven economy. Combined with technologies available today, advertisers and other third parties can garner immense economic benefits from the use of personal data. As such, data processing and sharing practices should not be entirely stopped — if monitored appropriately, consumers and various industries could reap major benefits from personal data processing. Trends from consumer behaviour surveys, as well as the concepts of *architecture of disclosure* and *privacy paradox*, allow us to nevertheless understand the crucial importance of regulating data practices of SNSs, since they underscore the inefficiency of market forces to induce adequate privacy practices in SNSs. Finally, we examine online behavioural advertising and data disclosures by SNSs to third parties and demonstrate the risks of each practice.

(a) Setting the Table: Data, Big Data, Artificial Intelligence, the Data-Driven Economy, and the Social Media Revolution

"Data represents the lowest raw format of information or knowledge."[23] "Big Data can be defined as volumes of data available in varying degrees of

Internet Profiling: Emerging Regulatory and Technological Approaches" (2008) 75 U Chicago L Rev 261.

[23] Krish Krishnan, *Data Warehousing in the Age of Big Data* (Waltham, MA: Elsevier, 2013) at 3.

complexity, generated at different velocities and varying degrees of ambiguity, that cannot be processed using traditional technologies, processing methods, algorithms, or any commercial off-the-shelf solutions."[24] As this definition alludes to, Big Data is often characterized by its singular dimensions, called the "three Vs": Volume (that is, the amount of data), Velocity (that is, the speed at which data is collected, used, and disseminated), and Variety (that is, the multiple types and sources of data).[25] Sometimes, a fourth V is added for Veracity, which directs attention to the possible inaccuracy of data,[26] or Value, referring to the economic value derived from Big Data.[27] SNSs process immense quantities of data through mining technologies that allow the rapid organization of troves of data. Among these technologies, artificial intelligence ("AI") tools are used to analyze widely different forms of data to discern various patterns and note their significance based on a set of algorithms. A prominent example is machine learning, which can be defined as a "knowledge discovery and enrichment process where the machine represented by algorithms mimics human or animal learning techniques and behaviours from a thinking and response perspective."[28] Machine learning is essentially a self-learning technique that requires minimal human intervention and can thus facilitate automation. Its powers are often used by SNSs when collecting data to accrue personal data, discern patterns, and craft online persona, which are then attributed to users. These profiles are then used to target individual, personally-based content.[29]

Since the late 20th century, ever more sophisticated technologies and processing architectures have led to increasingly powerful tools to analyze complex and vastly different types of data sets.[30] To illustrate how powerful Big Data and AI can be, let us take the example of the personal data generated by Facebook. Every second, thousands of clicks from millions of users are gathered. These serve to track each user's choices and navigations on Facebook's interface — every status update, post, comment, or page "liked", visited, or made by the user is taken and processed by Facebook. Given Facebook's 1.45 billion daily active users worldwide, this tracking creates massive volumes of data to process constantly.[31] In addition to user-generated content produced on a day-to-day

---

[24] *Ibid*. at 5.

[25] *Ibid*. at 15.

[26] See e.g. Victoria L Rubin, "Veracity Roadmap: Is Big Data Objective, Truthful and Credible?" (2014) 24:1 Advances in Classification Research 1, online: context = fims pub > .

[27] See Maurice E Stucke & Allen P Grunes, *Big Data and Competition Policy* (Oxford: Oxford University Press, 2016) at 15ff.

[28] Krishnan, *supra* note 23 at 236.

[29] See Abdul Muhammad, "AI's Hidden Patterns Transform Content, Marketing and Advertising on Facebook" (20 February 2018), online: *Ad Age* < www.adweek.com/digital/abdul-muhammad-rbb-communications-guest-post-ai-facebook/ > .

[30] See OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being* (Paris: OECD Publishing, 2015) at 23.

basis, SNSs also collect information such as name, email address, mailing address, telephone number, credit card number, IP address, browser type, operating system, Internet service provider, URLs of sites from which a user arrives or to which a user goes when leaving the service's website, interactions with third-party services like surveys and polls, country, gender, location, information generated when the SMS account is used to log in to a third-party website or application, date of birth, interests, hobbies, lifestyle choices, groups with which one is associated (i.e., company, school), search queries, and private messages and their metadata.[32] Distilling this data to extract trends and patterns greatly depends on flexible technologies that are not only able to take in mountains of disparate data, but are also able to process them quickly, effectively, and with a fair degree of accuracy.[33]

Seeing as the worldwide production of data is expected to continue to widely increase over time,[34] data processing technologies receive considerable investments annually from the private sector and are refined with the help of emerging technologies like AI.[35] This ever-greater capacity of distilling massive amounts of information into a meaningful format has major economic potential. Even more significant is the fact that SNSs and the Internet provide an entirely new medium over which people's lives can extend. Contrary to real life, however, every single action can be documented, which allows the creation of consistently more accurate individual user portraits detailing each user's personality and behaviour.

More than being simply saturated with information, in a data-driven economy, SNSs are effective and far-reaching sources of data because they elicit rich user interaction with their platform to achieve important concentrations of highly personalized data. The insight to be gained from analyzing this data is incomparable — no one source of data is as complete and tailored as an SNS. Through the various actions it offers each user, a given SNS can accumulate as much as several gigabytes of information on an individual.[36] With hundreds of

---

[31] This is as of April 2018. See See Josh Constine, "Facebook beats in Q1 and boosts daily user growth to 1.45B amidst backlash", *TechCrunch* (25 April 2018), online: < techcrunch.com/2018/04/25/facebook-q1-2018-earnings/ > .

[32] See Adam I Cohen, *Social Media: Legal Risk and Corporate Policy* (New York: Wolters Kluwer, 2013) at 117-18.

[33] See Krishnan, *supra* note 23 at 5.

[34] See McKinsey & Company, *Big Data: The Next Frontier for Innovation, Competition, and Productivity* (McKinsey & Company, 2011) at 6 (global data generated annually is projected to increase by 40%).

[35] See NewVantage Partners, *Big Data Executive Survey 2018: Data and Innovation: How Big Data and AI are Driving Business Innovation* (Boston: NewVantage Partners, 2018) at 9, online: < newvantage.com/wp-content/uploads/2018/01/Big-Data-Executive-Survey-2018-Findings.pdf > (97.2% of respondent firms invest in Big Data or Artificial Intelligence).

[36] See Dylan Curran, "Are you ready? Here is all the data Facebook and Google have on you", *The Guardian* (30 March 2018), online: < www.theguardian.com/commentisfree/

millions if not billions of daily users, all of whom are interconnected in various ways, SNSs are consequently among the most actual and well-supplied sources of personal information. They are also among the most consistent sources of worldwide personal data — since millions of people from all across the world possess social media accounts, SNSs make available information about the minds and habits of peoples from most geographical areas.

Ultimately, this data provides a powerful blueprint for a consumer's intimate thoughts, worldview, and interests — on a macro and micro scale. When analyzed using today's technologies, personal data can be distilled into individual user profiles using AI technologies, which offer advertisers, businesses, and researchers a significant tool they can use to market their products and reach new audiences.[37] This goes as far as processing information with AI algorithms to target ads not only for precise product types that a consumer has shown interest in, but also related products in anticipation of that consumer's developing and potential interests. For example, an SNS could find that a given consumer, even though they never considered becoming vegetarian, is likely to become vegetarian within two years. The consumer could therefore be targeted with more advertising related to vegetarianism in the future.[38]

These tools will inevitably continue to prove useful in an increasingly service-driven economy.[39] In one 2016 survey, only 5.4% of consulted firms stated that they did not have any Big Data initiative or plan to introduce one.[40] Furthermore, a 2018 report by McKinsey & Company estimated that "AI could potentially deliver additional economic output of around $13 trillion by 2030, boosting global GDP by about 1.2 percent a year."[41]

In short, there are major economic benefits to Big Data. Their importance is not negligible and should counsel nuance when evaluating potential regulation efforts.[42] Given the breadth of information coming from social media, it is

---

2018/mar/28/all-the-data-facebook-google-has-on-you-privacy> (the author of this piece found that Google had accumulated over 5.5GB of data on them — the equivalent of millions of Microsoft Word documents).

37 This is most evident in the profitability of targeted advertising, which has been calculated to yield revenues 2.68 times greater than non-targeted advertising. See National Advertising Initiative, "Study Finds Behaviorally-Targeted Ads More Than Twice As Valuable, Twice As Effective As Non-Targeted Ads Online", (24 March 2010), online (pdf): *National Advertising Initiative* <www.networkadvertising.org/pdfs/NAI_Beales_Release.pdf>.

38 See Frederik J Zuiderveen Borgesius, *Improving Privacy Protection in the Area of Behavioural Targeting* (Alphen aan den Rijn: Kluwer International, 2015) at 83.

39 See Krishnan, *supra* note 23 at 15.

40 NewVantage Partners, *Big Data Executive Survey 2016: An Update on the Adoption of Big Data in the Fortune 1000* (Boston: NewVantage Partners, 2016) at 5.

41 See McKinsey & Company, *Notes from the AI Frontier: Modeling the Impact of AI on the World Economy* (Brussels: McKinsey & Company, 2018) at 3.

42 See David A DeMarco, "Understanding Consumer Information Privacy in the Realm of Internet Commerce: Personhood and Pragmatism, Pop-Tarts and Six-Packs" (2006)

nonetheless crucial to closely monitor the impact that these technologies can have on privacy and a person's integrity. However, as we show in the next section, these benefits come, in practice, at the expense of consumers, as insights from behavioural economics demonstrate that SNS users are reluctant to change their privacy practices despite the genuine interest they might have in protecting their data.

(b) An "Architecture of Disclosure" and the Privacy Paradox

The primary purpose of SNSs is for individuals to connect with each other with reduced barriers of time and energy required for interactions to take place.[43] People overwhelmingly engage in SNSs for this purpose — a strong social imperative exists in that regard.[44] However, despite surveys suggesting people care about their privacy, when the risks and shortcomings of SNSs are pointed out to them, users tend not to change their behaviour.[45] This is generally known as the Privacy Paradox.[46] One might interpret this behaviour as disclosing a lack of genuine interest in privacy. However, a great part of this behaviour is rooted in a utility calculus rooted in what people see as the basic purpose of SNSs: the relationship to a network of people that provides connection[47] and allows for self-disclosure.[48] In a survey of Facebook users, it was found that only 35.9% of participants would be willing to change to a SNS that guarantees them more privacy.[49] Among those, a third would switch only if their social network would

84:4 T L Rev 1013 (arguing the dangers of Internet commerce as regards information privacy are occasionally overestimated and overemphasized and that, as such, they end up obscuring its economic benefits). Paul M Schwartz & Daniel J Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Information" (2011) 86 NYUL Rev 1814 (arguing academics should not underestimate the economic effects of too-radical solutions such as stopping the flow of information altogether). Contra Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (2010) 57 UCLA L Rev 1701 (suggesting a reduction in data flow).

43 See José Marichal, *Facebook Democracy: The Architecture of Disclosure and the Threat to Public Life* (Abingdon, UK: Routledge, 2012) at 40.

44 *Ibid*. at 34.

45 See Wouter Martinus Petrus Steijn, "The Cost of Using Facebook: Assigning Value to Privacy Protection on Social Network Sites Against Data Mining, Identity Theft, and Social Conflict" in Serge Gurwith, Ronald Leewes, & Paul de Hert, eds, *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, (Dordrecht: Springer, 2016) 323 at 323.

46 See e.g. H Brian Holland, "Internet Expression in the 21st Century: Where Technology and Law Collide: Privacy Paradox 2.0" (2010) 19 Widener L J 893.

47 See Judith Donath, "Signals in Social Supernets" (2007) 13:1 J Computer-Mediated Communication 231.

48 See Andrew M Ledbetter et al, "Attitudes Toward Online Social Connection and Self-Disclosure as Predictors of Facebook Communication and Relational Closeness" (2011) 38:1 Communication Research 27.

49 See Steijn, *supra* note 45 at 333.

be willing to switch as well.[50] "In other words, the social utility of SNSs appears to be the primary reason individuals make use of the sites and thus have to accept the potential privacy threats as a cost for participation."[51] As such, despite the spectre of grave privacy violations hovering over SNS users, the allure of SNSs is such that consumers are induced to refrain from making more rational choices, such as choosing more secure SNS options. A further illustration of this is a study which claims only 9% of Americans deleted their Facebook account following the reveal of the Cambridge Analytica scandal.[52] Considering the scandal was by far Facebook's greatest controversy to this day and touched on some of the most fundamental aspects of privacy, this number reveals the weight utility takes over privacy.

Taking advantage of this situation, SNSs can then induce consumers into divulging more and more private information by setting up their interface to favour disclosures. In the context of Facebook, Marichal compellingly describes these characteristics as forming a *choice architecture*.[53] In our view, this observation also applies to other major SNSs like Twitter, Instagram, and LinkedIn. A *choice architecture* derives from a behavioural economics institutionalist approach to decision-making and posits that "institutions can influence decision-making by structuring choice so that the costs associated with an institution's desired behaviour is [*sic*] significantly lower than the behaviour desired by the individual *ceteri paribus*."[54] As such, despite users' earnest wishes to protect their privacy, SNSs are set up so as to induce disclosure of their information. Notably, default settings are aimed towards allowing disclosures of information because people will seldom take the time to change them, let alone become aware that they can be changed.[55] More subtly, by making highly visible activity from other people in their network,[56] and providing users with the opportunity to choose to receive highly personalized content based on their interests,[57] the SNS is encouraging users to disclose in turn — thereby creating more insightful personal data for SNSs to analyze and re-use. Thus, through providing consistently more content to meaningfully engage with, SNS create a

---

50 *Ibid.* at 336.

51 *Ibid.*

52 A further illustration of this can be found in an assessment of the #DeleteFacebook movement, which claims that only 9% of Americans deleted their Facebook account following the Cambridge Analytica scandal. See Carolina Milanesi, "US Consumers want more transparency from Facebook", (11 April 2018), online: *Tech.pinions* < techpinions.com/us-consumers-want-more-transparency-from-facebook/52653 > .

53 See Marichal, *supra* note 43 at 37. The concept of "choice architecture" was coined and developed in Richard H Thaler & Cass R Sunstein, *Nudge: Improving Decisions about Wealth, Health and Happiness* (New Haven: Yale University Press, 2008).

54 See Marichal, *supra* note 43 at 38.

55 *Ibid.* at 39.

56 *Ibid.* at 40.

57 *Ibid.* at 37.

choice architecture that ultimately leads to more disclosures of personal data.[58]

In such a context, SNSs and their business partners are set to reap great economic benefits from their users. Given the wide breadth of information available on SNSs, the dangers of this data spreading on the Internet through online behavioural advertising and third-party data sharing and subsequently being used to cause individual SNS users harm are nothing short of alarming, as we explain below.

(c) Online Behavioural Advertising

Advertising is the main source of profit for SNSs.[59] Since its early years, the Internet has established a path for the advertising industry to reach new audiences. However, new tracking technologies developed a few years in its infancy allowed for the expansion of the already well-established practice of targeted advertising into online behavioural advertising (that is, "the practice of tracking consumers' activities online to target advertising"[60]) created one of the greatest obstacles to Internet privacy. This hazard is exacerbated by social media.

Starting the 1970s, advertising became a much more fragmented art. Advertisers became interested in targeting specific groups of people with advertisements aimed at particular segments of the population.[61] In the 1980s and 1990s, "direct marketing progressed to database marketing," which entails "the use of consumer databases to enhance marketing productivity through more effective acquisition, retention, and development of customers."[62] This historical step led to the increasing accumulation of consumer data.[63] Once the Internet became widely accessible, it was only a matter of time before the practice grew and progressively achieved ever-greater segmentations and precision as it honed in further on its multifaceted targets.[64] New Internet technologies, including AI, now allow advertisers to track users on an ongoing basis and use the accrued data to extrapolate patterns from their online behaviour to target ads with ever greater precision and efficiency.[65]

On the Internet, advertising revenues are usually based on a *cost-per-click* (whereby the advertiser is paid according to the number of clicks an ad receives from Internet users) or *cost-per-conversion* (where the advertiser is paid according to the number of times that an Internet user clicks on an ad redirecting them to

---

58 *Ibid.*

59 See Stucke & Grunes, *supra* note 27 at 54.

60 Julia Zukina, "Accountability in a Smoke-Filled Room: The Inadequacy of Self-Regulation Within the Internet Behavioral Advertising Industry" (2012) 7 Brooklyn J Corporate, Financial & Commercial L 277 at 277.

61 See Zuiderveen Borgesius, *supra* note 38 at 17.

62 *Ibid.* at 18.

63 *Ibid.*

64 *Ibid.*

65 *Ibid.* at 1.

an advertising client's website and performs a pre-determined action) basis. As a result of these models, an advertiser or advertising network's[66] success depends entirely on an advertisement's persuasion and effectiveness.[67] With most major SNSs being usually available to consumers for free, given that these services require the maintenance of an expensive web architecture and supporting institutions, monetizing the very capital they generate — personal data — was a natural course of action for SNSs to take. Combining their platform's undeniable popularity — and the consequently wide user base continually producing troves of personal data — with perpetually refined technologies in order to generate insightful behavioural accounts of large swaths of the population made them the perfect contenders in the race to become the most powerful advertisers on the Internet.

(i) Overview of Online Behavioural Advertising and Data Practices of Major SNSs

For this study, we looked at the privacy policies of six major SNSs: Facebook, Instagram, Twitter, LinkedIn, Google + and YouTube (the latter two being owned by Google and therefore falling under the purview of the Google Privacy Policy).[68] The advertising practices of SNSs mostly share similar characteristics, with some exceptions that mostly relate to partnerships with other advertising and analytics firms. These practices, from a data protection standpoint, can have major implications, which, in turn, raise important questions as to how effective SNSs are at regulating themselves as regards the personal data of their users.

Each of the SNSs studied offers their own advertising interface through which firms can place an ad on their respective social media platform.[69] Firms

---

[66] An advertising network, sometimes shortened to "ad network," is a company that connects advertisers to website publishers in order to serve ads on websites. *Ibid.* at 16.

[67] *Ibid.* at 18.

[68] See Facebook, "Data Policy" (19 April 2018), online: *Facebook* <www.facebook.com/policy.php> [Facebook Privacy Policy]; Facebook, "Cookies and Other Storage Technologies" (4 April 2018), online: *Facebook* <www.facebook.com/policies/cookies/> [Facebook Cookies Policy]; Twitter, "Privacy Policy" (25 May 2018), online: *Twitter* <twitter.com/en/privacy> [Twitter Privacy Policy]; LinkedIn, "Privacy Policy" (8 May 2018), online: *LinkedIn* <www.linkedin.com/legal/privacy-policy> [LinkedIn Privacy Policy]; LinkedIn, "Cookies Policy" (8 May 2018), online: *LinkedIn* <www.linkedin.com/legal/cookie-policy> [LinkedIn Cookie Policy]; Instagram, "Privacy Policy" (19 January 2013), online: *Instagram* <help.instagram.com/155833707900388>; Instagram, "Data Policy" (19 April 2018), online: *Instagram* <help.instagram.com/519522125107875> [Instagram Data Policy]; Google, "Google Privacy Policy" (25 May 2018), online: *Google* <policies.google.com/privacy?hl=en> [Google Privacy Policy].

[69] See Facebook, "Facebook Ads" (11 August 2018), online: *Facebook* <www.facebook.com/business/products/ads>; Twitter, "Twitter Ads" (11 August 2018), online: *Twitter* <ads.twitter.com/campaign/>; Instagram, "Advertising on Instagram" (11 August 2018), online: *Instagram* <business.instagram.com/advertising/>; LinkedIn, "Linke-

can customize their ad depending on the type of marketing campaign they envisage and choose specific targeting parameters, including demographics, behaviours, and interests, to circumscribe the ad's audience. These parameters can be very broad (for instance, "the United Kingdom") or finely tuned (for example, "interested in BBC's 1995 TV adaptation of *Pride and Prejudice*"). They can also be a combination of individual user characteristics such as "People in Brazil who like high-value goods."[70] Through the process of manufacturing the ad, firms do not have direct access to personal data accumulated by the SNS. They only tell the SNS who to target with their ad and the SNS does it for them.[71]

At this point, SNSs' use of personal data is arguably reasonable. In exchange for providing a service — one that, manifestly, consumers greatly appreciate — user-generated content and other freely-disclosed information are used by the SNS in order to profit from advertising that will generally be of some interest to users. Consumers have an opportunity to read terms of services, including the SNS's legislatively mandated privacy policy, which gives them the opportunity to decline to engage in the service if they are not satisfied with its terms.[72] Moreover, at the end of the day, both consumer and service provider benefit from their respective actions. Furthermore, if access to personal data by third-parties is limited to prevent any considerable risk of identification and appropriate privacy protection measures are taken to preserve users' personal

---

dIn Ads" (11 August 2018), online: *LinkedIn* < business.linkedin.com/marketing-solutions/ads > ; Youtube, "YouTube Advertising" (11 August 2018), online: *Youtube* < www.youtube.com/yt/advertise/ > ; Google, "Google Ads — Google + " (11 August 2018), online: *Google* + < plus.google.com/ + GoogleAds > .

70 These examples were taken directly from Facebook's ad interface. See Facebook, "Ads Manager" (29 July 2018), online: *Facebook* < www.facebook.com/adsmanager/creation?act = 191051970974205&filter_set > .

71 This aspect of the advertising process on social media has been the cause of acute unease on the part of the public, which has led many SNSs to clarify that they "do not sell their data." See e.g. Facebook, "Does Facebook sell my information" (2018), online: *Facebook Help Centre* < www.facebook.com/help/152637448140583?helpref = related > . This exact point was reiterated by Facebook CEO Mark Zuckerberg in his testimony before Congress. See Kaleigh Rogers, "Let's Talk About Mark Zuckerberg's Claim that Facebook 'Doesn't Sell Data'", *Motherboard* (11 April 2018), online: < motherboard.vice.com/en_us/article/8xkdz4/does-facebook-sell-data > .

72 While the extent to which a consumer should be expected to read boilerplate legalese or terms of services in general can be debated, we agree with multiple scholars that they nonetheless have an obligation to take actions to protect their privacy, including their personal data. See e.g. Anita L Allen, "Protecting One's Own Privacy in a Big Data Economy" (2016) 130 Harv L Rev F 71; Eugene E Hutchinson, "Keeping Your Personal Information Personal: Trouble for the Modern Consumer" (2015) 43 Hofstra L Rev 1151. See also Daniel J Solove, "Introduction: Privacy Self-Management and the Consent Dilemma" (2013) 126 Harv L Rev 1880 (arguing that consenting to data collection and sharing practices is not enough, as it does not grant people meaningful control over their data).

data from privacy breaches, then a compromise between privacy and reasonable use of personal data for economic purposes might be struck.

The current situation is not so rosy, however. First, SNSs use *cookies*, that is, small text files that a server can send to an Internet browser. Cookies allow a website publisher or a third party to track people's actions on the Internet[73] and to monitor consumers' interests and browsing patterns outside of their respective ecosystems.[74] Even more shocking is the fact that SNSs stalk consumers on the web whether or not they have an account with them.[75] This is normally done through plugins allowing users to share a given webpage on different SNSs. In such cases, the website publisher has approved the plugin's addition and includes it as part of its cookie policy, which users are normally prompted to approve when they visit the website.[76] Already, this poses a major problem as regards informed consent, which is crucial for this sort of data collection to be in any way legitimate. For one, consumers who do not subscribe to an SNS have no genuine way of consenting to the collection of their information in the first place. Moreover, even subscribed consumers could not be said to have consented to the aggregation of their information outside an SNS. A regular customer would most likely not imagine that an SNS's tracking practices extend this far, for one. Furthermore, tracking practices are not clearly highlighted in many privacy policies — one has to dig deep to find the information hidden in an SNS's privacy policy.[77]

Second, SNSs often collaborate with third-party advertising networks to place advertisements using SNS-gathered data outside of their respective SNS ecosystem. This practice is problematic. First, it relies on enhanced tracking

---

[73] See Zuiderveen Borgesius, *supra* note 38 at 17.

[74] Far from being a veiled practice, many SNSs admit to doing so in their Privacy Policy. See e.g. LinkedIn Privacy Policy, *supra* note 68 at 1.8; Facebook Cookies Policy, *supra* note 68; Twitter, "Privacy Control for Personalized Ads" (29 July 2018), online: *Twitter* < help.twitter.com/en/safety-and-security/privacy-controls-for-tailored-ads > .

[75] See Adam Wright, "Twitter, Facebook and LinkedIn Offer New Ways for Advertisers to Reach Users: The World's Leading Social Media Platforms Have Expanded Their Advertising Offerings Beyond Their Own Platforms as They Seek to Compete With Google" (25 March 2015), *The Guardian* (accessed through LexisNexis Quicklaw); Kurt Wagner, "This is How Facebook Collects Data Even if You Don't Have an Account" (20 April 2018), online: *Recode* < www.recode.net/2018/4/20/17254312/facebook-shadow-profiles-data-collection-non-users-mark-zuckerberg > .

[76] See Wagner, *supra* note 75 (on SNSs tracking users outside their platform using plugins). See also Claude Castelluccia & Arvind Narayanan, "Privacy Considerations of Online Behavioural Tracking" (Athens, Greece: European Network and Information Security Agency, 2012) at 9 (22% of Internet pages have a Facebook "Like" button, 7.5% a "Twitter Re-Tweet" button, and 10.4% contain a "Google + share" button).

[77] Facebook, Instagram, and LinkedIn include this information about halfway through their privacy policies. See Facebook Privacy Policy, *supra* note 68; Instagram Data Policy, *supra* note 68; LinkedIn Privacy Policy, *supra* note 68. Twitter's privacy policy is silent on the subject and it is not clear whether or not it uses such plugins to collect information.

technologies that are even more intrusive than cookies to follow SNS users around the web.[78] Second, it requires third parties to share information with SNSs that they themselves have acquired about single users. That users do not get the chance to give informed consent regarding the collection of their data only scratches the surface of the problem. Here, not only are users tracked across the Internet, with networks of advertisers combining their efforts to follow users everywhere they go, but personal data is being exchanged with their originating user having absolutely no control over its propagation. Whereas cookies, despite their possible intrusiveness, can be removed by a user or altogether blocked on given Internet browsers, the same is not true of some of the technologies used like Facebook's "persistent ID," which can track a given user across devices.[79]

In summary, online behavioural advertising opens consumers to grave violations of privacy and personal integrity through individualized tracking in and outside SNSs. A crucial problem related to this practice is that it allows individual SNSs to track consumers all over the Internet without adequately securing their consent. Moreover, this practice has the potential to remove consumers from being in any position where they can fully exercise their choice and autonomy as to the dispersion of their personal data on the Internet.

(ii) Wider Effects of Behavioural Advertising

Online behavioural advertising has several large-scale effects. First, a potential chilling effect results from unmoderated online behavioural advertising. The Internet is not only a place where people engage in economic transactions with various service providers — it is also a place to look for information on important subjects, from health to politics to law,[80] and serves as a medium for identity formation.[81] Knowledge of SNSs' and advertising networks' extensive tracking practices can lead some to skepticism and wariness when using the Internet. Faced with a significant information asymmetry between them and SNSs, users may recognize their lack of control over their personal information and become less willing to use the Internet as a result.[82]

---

[78] See Wright, *supra* note 75. For example, Facebook developed a partnership with Atlas, which tracks Facebook's persistent ID, thereby allowing the tracking of users across devices and for the full customer journey, from clicking on an ad to buying a product. Similarly, LinkedIn partnered with AppNexus to target LinkedIn users on third-party websites.

[79] See Zach Rogers, "With Atlas Relaunch, Facebook Advances New Cross Device ID Based on Logged-In Users", (28 September 2014), online: *Ad Exchanger* < adexchanger.com/platforms/with-atlas-relaunch-facebook-advances-new-cross-device-id-based-on-logged-in-users/ > .

[80] See Castelluccia and Narayanan, *supra* note 76 at 9 (noting the presence of SNS plugins on many health websites).

[81] See Zuiderveen Borgesius, *supra* note 38 at 74. A line of scholarship has notably argued that one justification for privacy is autonomy and self-development. See Julie E Cohen, "Examined Lives: Informational Privacy and the Subject as Object" (2000) 52:5 Stanford L Rev 1373.

Second, online behavioural advertising can be so effective that it effectively allows for manipulation of people's thoughts and behaviours.[83] This could be done in two major ways. First, firms could detect certain weaknesses in people from tracking them extensively and take advantage of these weaknesses to gain an unfair advantage.[84] Firms could also decide to use online behavioural advertising to steer consumers toward certain beliefs and behaviours.[85] To take our earlier example, a consumer who has never considered becoming vegetarian may slowly be induced to adopt this diet through targeted advertising online, notably ads extolling the virtues of vegetarianism.[86]

Third, online behavioural advertising opens up the possibility of differential treatment according to personal characteristics, which can lead to abusive or questionable practices. For example, advertisers could organize marketing campaigns according to a consumer's affluence and offer certain discounts that would not otherwise be available to someone whose browsing history reflects precarity. Conversely, someone whose browsing seems to indicate indigence could be targeted with ads for nefarious lending schemes.[87]

(d) Third-Party Disclosures of Data

Having described the perils of online behavioural advertising as applied to social media, we now turn to third-party data sharing. Third-party data sharing can occur in a number of contexts, not all of which are necessarily illegitimate. All SNSs studied state that they share data for various purposes with third parties in their privacy policies. However, these policies are most often unclear as to the exact nature and purpose of the data shared. Ultimately, two major

---

82 See Jerry Kang, "Information Privacy in Cyberspace Transactions" (1998) 50 Stan L Rev 1193 at 1253; Zuiderveen Borgesius, *supra* note 38 at 78-79 (describing how people are often confronted with take-it-or-leave-it choices when looking into engaging in a new service on the Internet).

83 *Ibid.* at 83.

84 See Ryan Calo, "Digital Market Manipulation" (2014) 82:4 Geo Wash L Rev 995 (notably giving the example of scientific studies indicating women feel "less attractive" on Monday mornings, making this a "prime vulnerability moment" during which targeted advertising risks being more successful).

85 *Ibid.* See also Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019). In the context of politics, see Anthony Nadler, Matthew Crain & Joan Donovan, "Weaponizing the Digital Influence Machine: The Political Perils of Online Ad Tech" (2018), online (pdf): *Data & Society Research Institute* <datasociety.net/wp-content/uploads/2018/10/DS_Digital_Influence_Machine.pdf>; Colin J Bennett & David Lyon, "Data-driven elections: implications and challenges for democratic societies" (2019) 8:4 Internet Pol'y Rev 3; Tal Z Zarsky, "'Mine Your Own Business!': Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion" (2002) 5:1 Yale JL & Tech 1 at 40.

86 See Zuiderveen Borgesius, *supra* note 38 at 83.

87 *Ibid.* at 81.

problems arise from this ambiguity. First of all, data sharing will most often be done without the express consent of SNS users. Second, once a user's personal data has been shared, they have no way of knowing how their data is being used and who has access to it.[88] Moreover, once their personal data is in the hands of a third party, it is possible for that third party to share it with another one, thereby preventing further monitoring by either the SNS or the consumer.[89]

We have mentioned earlier how SNSs often do not give consumers a reasonable chance to give informed consent to data collection and tracking practices. The information asymmetry noted earlier between users and SNSs is equally applicable to third-party data sharing. Every privacy policy consulted states that its originating SNS uses and shares personal data for such things as "providing our services" or "improving [them]."[90] There is great uncertainty in such a formulation. The SNS could mean that it is sharing personal data internally, in which case it is easier to keep track of it, and security measures can be taken to prevent data breaches. Conversely, the SNS could also mean that data is shared externally, in which case tracking the data is harder for users.

SNSs usually share personal data with third parties to provide analytics and measurement services, notably for companies using the SNS's built-in business tools. As such, they provide aggregate statistics and non-personally identifiable information ("non-PII") to businesses and advertisers to understand their ad's performance.[91] While aggregate statistics are not the most concerning, the same cannot be said for non-PII. For one, despite being at the centre of multiple laws and regulations, PII has yet to be decisively defined.[92] Schwartz and Solove underscore this fact by outlining three definitions commonly used for PII.[93] It can either be information that identifies a person,[94] information that is not publicly accessible or that is purely statistical,[95] or specific categories of information enumerated in a statute about a class of individuals.[96] In short,

---

[88] See Clark D Asay, "Consumer Information Privacy and the Problem(s) of Third-Party Disclosures" (2013) 11:5 Nw J Tech & Intell Prop 321 at 322 (outlining the two problems of third-party disclosures of consumer information as the Incognito problem, or the fact that consumers do not know how their data will be used, and the Onward Transfer problem, which refers to the fact that once a consumer's personal data is in the hands of a third party, the consumer has simply no means of monitoring the use of his personal data); Natalie Kim, "Three's a Crowd: Towards Contextual Integrity in Third-Party Data Sharing" (2014) 28:1 Harv JL & Tech 325 at 327 ("the typical user only has control over first-node sharing between user and data controller [. . .] in contrast, contextual integrity in the second node is unclear at best").

[89] See LaMagna, *supra* note 11.

[90] See *supra* note 68.

[91] *Ibid.*

[92] See Yuen Yi Chung, "Goodbye PII: Contextual Regulation for Online Behavioural Targeting" (2014) 14:2 J High Tech L 413 at 418.

[93] See Schwartz & Solove, *supra* note 42 at 1828-30.

[94] *Ibid.* at 1829 (presenting this approach as the so-called "tautological approach").

[95] *Ibid.* at 1829-30 (presenting this approach as the so-called "non-public approach").

difficulty in defining non-PII takes teeth out of privacy policies' efforts to protect users' personal data. Moreover, the possibility of cross-referencing data sets to re-identify individuals after data has been anonymized significantly dilutes any promises made by SNSs that sharing only non-PII adequately protects users' personal data.[97]

Some SNSs state that they also disclose personal data to academics for research purposes or to authorities for legal reasons.[98] While these might seem less problematic, it is important not to downplay these as possible channels through which privacy rights can be violated. As any third party, academics can share their data sets with others and thus remove personal data from under the control of SNS users, as was done in the case of Cambridge Analytica.[99] Moreover, as revealed by Edward Snowden in 2013, massive government surveillance programs exist that can amass personal data on billions of people worldwide with little to no due process.[100] Given the breadth of information possessed by SNS on the citizenry, personal data disclosures for legal reasons, like any disclosure of personal data, should be questioned and examined openly.

In addition to SNS-bound disclosures of personal data, users may also voluntarily share information with third parties, notably when using third-party apps on a given SNS. Here, users are again faced with the problems described above. While there is no question that third-party apps can sometimes require some personal data in order to provide their service, their privacy notices are usually too vague to give users a genuine idea of why and how certain data is used. Moreover, as the Cambridge Analytica scandal underscored, third-party apps can, without any real barrier, collect data unrelated to its purposes, which it

---

96 *Ibid*. at 1831 (presenting the so-called "specific-types approach").

97 This issue has long been underscored by scholars, leading to a plethora of proposed solutions. See e.g. Ira S Rubinstein, Ronald D Lee & Paul M Schwartz, "Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches" (2008) 75 U Chicago L Rev 261 at 268 (describing how data reduction can serve to anonymize personal data); Ohm, *supra* note 42 at 1742 (suggesting slowing down the flow of information on the Internet and in society altogether to avoid a "whack-a-mole" situation wherein any attempt at defining PII eventually proves futile as hitherto unaddressed aspects of this extremely difficult problem eventually appear, demanding constant re-definition of the problem); Schwartz and Solove, *supra* note 42 at 1865ff (responding to Ohm's argument by proposing new definitions of the basic elements of PII with greater flexibility and durability); Chung, *supra* note 92 at 440 (suggesting the abandonment of the PII/non-PII dichotomy to emphasize contextual integrity with a comprehensive regulatory scheme setting ground norms for privacy regulation).

98 See Facebook Privacy Policy, *supra* note 68 (academic and legal requests); Instagram Data Policy, *supra* note 68 (academic and legal requests); Twitter Privacy Policy, *supra* note 68 (legal requests only); LinkedIn Privacy Policy, *supra* note 68 at 3.6 (legal requests only); Google Privacy Policy, *supra* note 68 (legal requests only).

99 See Merelli, *supra* note 10.

100 See Glenn Greenwald, "NSA collecting phone records of millions of Verizon customers daily", *The Guardian* (6 June 2013), online: < www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order > .

can then share with other third parties with no user control over the spread of their personal data. The personality quiz-dispensing app at the origin of the collection of the information of over 80 million user profiles only managed to gather such a mind-boggling amount of information because it collected not only its users' personal data, but their friends' too.[101] In short, the value of consent for third-party sharing of personal data to SNS apps is very dubious. Not only is consent uninformed, but no monitoring of personal data is possible once the information has been transferred to third parties.

(e) SNS Efforts at Self-Regulation

For the most part, all of the SNSs studied regulate their actions with regards to advertising and third-party data sharing through their own policies and without reference to any outside rules. While they occasionally provide rights equivalent to certain self-regulatory principles in their policies, asserting these rights often proves confusing and challenging.

On advertising, Facebook, Instagram, Google+ and YouTube do not explicitly disclose any adherence to self-regulatory principles or require the adherence of advertising partners. Twitter discloses neither adherence to nor requirement of such principles, but it provides opt-out tools for interest-based advertising, hidden in one page of its help centre.[102] LinkedIn is the only SNS studied to explicitly adhere to self-regulatory principles, namely the American *Digital Advertising Alliance*, the Canadian *Digital Advertising Alliance of Canada*, and the European Union's *European Interactive Digital Advertising Alliance*, the opt-out tools of which it provides hyperlinks.[103]

Other SNSs do provide some opportunity to opt out of targeted advertising, but only from individual advertisers.[104] This form of opting out has serious drawbacks. First, consumers are unable to refuse to be subject to targeted

---

[101] See Alex Hern & Carol Calwalladr, "Revealed: Aleksandr Kogan collected Facebook users' direct messages", *The Guardian* (13 April 2018), online: < www.theguardian.com/uk-news/2018/apr/13/revealed-aleksandr-kogan-collected-facebook-users-direct-messages > .

[102] Opt-out tools for online behavioural advertising are provided by self-regulatory initiatives and allow an Internet user to request that participating advertising networks stop tracking them with cookies. See Twitter, "Our Use of Cookies and Similar Tracking Technologies" (14 August 2018), online: *Twitter* < help.twitter.com/en/rules-and-policies/twitter-cookies > ; "Your AdChoices" (14 August 2018), online: *Digital Advertising Alliance* lang = EN > ; "Opt Out of Interest-Based Advertising" (14 August 2018), online: *National Advertising Initiative* < optout.networkadvertising.org/?c = 1#!/ > .

[103] See LinkedIn, "Manage Advertising Preferences" (14 August 2018), online: *LinkedIn* < www.linkedin.com/help/linkedin/answer/62931?query = managing%20ad%20preferences > .

[104] See Facebook, "Can I opt out of seeing ads because I'm included in a Custom Audience?" (14 August 2018), online: *Facebook* < www.facebook.com/business/help/1415256572060999 > .

advertising, meaning their personal data will still be used to target advertising at them. Furthermore, under this scheme, consumers can only opt out of a given advertiser when they encounter their advertisement online. As such, their personal data may still be used in targeted advertising until they eventually encounter this advertiser's ad. In any case, asking consumers to personally opt out of every single targeted advertisement they encounter, given how utility is the main driving factor behind SNS use,[105] is simply unrealistic.

With regards to data sharing, aside from general principles provided by governments,[106] SNSs generally craft their own rules. The rules are basically the same for each SNS: consumers must agree to the SNS's terms of service, which include its privacy rules, when creating their account. Thereafter, SNSs may collect any user-generated content on the site. It is up to consumers to decide whether to disclose more data, such as by posting pictures, videos, status updates, etc. In the fallout of the Cambridge Analytica scandal, SNSs have started offering users the chance to download the "archive" an SNS keeps on them.[107] The overall process of downloading this archive (which requires finding one's way through a labyrinth of help pages) is fairly straightforward. However, it is of little consequence. SNSs still hold each user's personal data and generally give limited options to correct and delete it, taking the approach that as long as personal data is not removed from the site by the user, the SNS may still use it for its own purposes. To their credit, LinkedIn and Facebook have created special tools to simplify the removal of personal data by users.[108] As far as we know, other SNSs provide no such tool. As a result, it is practically impossible to fully remove one's personal data from most SNSs studied.

In any case, such tools remain antithetical to the very nature of SNSs, whose nature is oriented towards information disclosure, and SNSs therefore necessarily discourage users from using them. After all, it makes little sense to remove the very content through which the core purpose of SNSs, that is, interacting with one's social circle, is achieved. Rather than requiring users to sacrifice their enjoyment of the service, it would be considerably better if SNSs addressed data protection concerns transparently and by design.

In short, self-regulatory measures taken by SNS are ineffective and fail to address major privacy concerns of online behavioural advertising and data sharing. SNSs give little clarity as to their uses of data and protection measures. As a result, consumers' rights are at great risk when using these sites.

---

[105] See Milanesi, *supra* note 52 (and accompanying text).

[106] See FTC 2012 Report, *infra* note 129; PIPEDA, *infra* note 137 at Schedule 1.

[107] See Dwight Silverman, "How to download your data from Google, Twitter, LinkedIn, Snapchat", *Houston Chronicle* (15 August 2018), online: < www.houstonchronicle.com/techburger/article/How-to-download-your-data-from-Google-Twitter-12789357.php > .

[108] See LinkedIn, "Delete Your Personal Data from LinkedIn" (15 August 2018), online: *LinkedIn* < www.linkedin.com/help/linkedin/answer/93500?query = delete%20data > .

Part II: *DATA PROTECTION LAW OF THE UNITED STATES, CANADA, AND THE EUROPEAN UNION*

In this Part, we look at the data protection framework enacted in the United States, Canada, and the European Union ("EU"). The picture we draw in this section serves as the basis for the theoretical discussion we entertain in Part III. The United States, Canada, and the EU each represent distinct regulatory philosophies, which admit greater or lesser levels of self-regulation. Indeed, the United States accepts an important margin of self-regulation with respect to the personal data protection.[109] Canada and the EU, on the other hand, possess unified statutory frameworks with general and concrete obligations.[110]

(a) United States

The United States does not have national law on data privacy standards.[111] Rather, various interweaving state and federal sectoral laws create a patchwork of rules that impose certain obligations on corporations with regards to data processing.[112] These are fashioned according to the specific industries and types of data they aim to regulate.[113] Notable examples include the *Gramm-Leach-Bliley Act*[114] and the *Health Insurance Portability and Accountability Act*,[115] which respectively apply to financial services and health insurance companies. Privacy obligations under these statutes include confidentiality of non-public personal information,[116] notice and choice procedures to inform a user about the uses and disclosures affecting their personal information,[117] and the creation of a privacy policy for consumers.[118] According to one author, under United States

[109] We note, at this point, that the literature is far from clear as to the frontier between self-regulation and co-regulation. Furthermore, as noted by a number of scholars, regulatory schemes characterized as self-regulatory often admit some form of government involvement. See Florian Saurwein, "Regulatory Choice for Alternative Modes of Regulation: How Context Matters" (2011) 33 L & Pol'y 334 at 336. See also Hirsch, "The Law," *supra* note 7; Bert-Jaap Koops et al, "Should Self-Regulation Be the Starting Point" in Bert-Jaap Koops et al, eds, *Starting Points for ICT Regulation* (The Hague: Springer, 2006).

[110] See Joanna Kulesza, *International Internet Law* (London: Routledge, 2012) at 55: "US legal academics and commentators assume that government interference in this regulatory field is unnecessary. The US model ensures only a few positive rights. The intention is that self-regulation and market forces jointly are to establish the protection of data and privacy. The European model, however, assumes that the government is responsible for privacy protection for nationals, and to this end it is the government that should demonstrate active involvement."

[111] See Jeff Kosseff, *Cybersecurity Law* (Hoboken, NJ: John Wiley & Sons, 2017) at 1.

[112] *Ibid.* at 318.

[113] *Ibid.*

[114] See Pub L No 106-102, 113 Stat 1338 (1999).

[115] See Pub L No 104-191, 110 Stat 1936 (1996).

[116] See 15 USC § 6801 (1999) (confidentiality of personal information collected by financial services).

law, privacy is considered not so much a conceptually fulsome *right* so much as a *good*. As such, privacy protections function as carve-outs: a firm can collect all the data it wants except that excluded by statute.[119]

The Federal Trade Commission (FTC) most closely approaches the role of centralized privacy regulator in the United States.[120] Its authority extends over any company engaged in interstate and international commerce.[121] Section 5 of the Act, prohibiting "unfair or deceptive practices" affecting commerce, allows the FTC to order a company to cease and desist certain practices that do not provide sufficient data protection to their customers and subsequently fine them if they fail to abide by the order.[122] It also allows the FTC to commence enquiries and civil proceedings against major Internet-related companies, notably SNSs.[123] In each of its cases, the FTC takes an individualized approach to determine whether a company's privacy practices are "unfair or deceptive."[124] In addition to its investigative powers and standing before US courts in proceedings relating to its statute, the FTC may promulgate quasi-judicial orders (called "consent orders")[125] compelling acts and imposing certain conditions respecting a company's continued operation after it has been found to have engaged in unfair or deceptive practices, [126] which the FTC vigorously enforces.[127] Finally, the FTC may also promulgate regulations in furtherance of its statutory objectives.[128]

Beyond its legislative and judicial capacities, the FTC is also involved in monitoring the market and monitoring its evolutions. As such, it has published

---

[117] *Ibid.* at § 6802 (use and disclosure in the financial services industry); 45 CFR § 164.502 (use and disclosure of personal health information).

[118] See 15 USC, *supra* note 116 at § 6803; 45 CFR, *supra* note 117 at § 164.520.

[119] See Lindsey Barrett, "Confiding in Con Men: US Privacy Law, the GDPR, and Information Fiduciaries" (2019) 42 Seattle UL Rev 1057 at 1068.

[120] Other federal agencies, like the Federal Communications Commission or the Department of Health and Services, may also act as a form of centralized data regulator. The FTC's reach, however, is much broader. See Kosseff, *supra* note 111 at 2.

[121] See *Federal Trade Commission Act,* Pub L No 63-203, § 4, 38 Stat 717 (1914) (codified as amended at 15 USC § 41) [*FTC Act*].

[122] *Ibid.* at 15 USC § 45. See also Michael L Rustad, *Global Internet Law in a Nutshell* (St. Paul: Westgate Academic Publishing, 2016) at 203 (on resorting to Section 5 of the *FTC Act* to enforce data protection).

[123] See Rustad *supra* note 122 at 203.

[124] See Kosseff, *supra* note 111 at 320.

[125] See *ibid.* at 6.

[126] See e.g. "In re Facebook, Inc, Decision and Order" (27 July 2012), online: *FTC* <www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf>; Google, Inc, 152 FTC 345 (2001).

[127] Google was notably sanctioned to pay USD 22.5 million for violating a consent order already imposed by the FTC in the Google Buzz case. See Kosseff, *supra* note 111 at 320.

[128] See *FTC Act*, *supra* note 121 at § 15.

numerous reports and recommendations on data protection. To this point, these have been mainly aimed at self-regulation, thus reflecting the economic paradigm in the United States.[129] As regards data protection, the FTC has reiterated several self-regulatory principles that businesses should adopt:[130]

- *Notice*, meaning "those collecting data must disclose their information practices before collecting from consumers";[131]
- *Access*, meaning consumers must be given options to direct how their personal information may be used for purposes other than those to which they originally consented;[132]
- *Consumer education,* meaning "companies should educate consumers about their privacy practices";[133]
- *Security*, meaning "data collectors must take reasonable steps to assure info collected from consumers is secure from public use";
- *Privacy by design*, meaning "companies should incorporate privacy protections for consumers at each stage of product development";[134]
- *Enforcement*, meaning "the core principles of privacy protection can only be effective through enforcement mechanisms including: industry self-regulation, the creation of private rights of action, and government enforcement through civil and criminal penalties";
- *Simplified consumer choices*, meaning "companies should provide consumers with the option to decide what information is shared about them, and with whom";[135]
- *Transparency*, meaning "companies should disclose details about the collection and use of consumers' information, as well as providing access to that data."[136]

(b) Canada

Canada has enacted data protection obligations at the federal level through the *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*").[137] *PIPEDA* was passed in response to the 1998 European Union's Data Protection Directive. One of the Directive's major aspects was

---

[129] See e.g. United States, Federal Trade Commission, *Protecting Consumers in an Era of Rapid Change* (Washington, DC: FTC, 2012) [FTC 2012 Report]; United States, Federal Trade Commission, *Self-Regulatory Principles for Online Behavioral Advertising* (Washington, DC: FTC, 2009) [FTC 2009 Report]; United States, Federal Trade Commission, *Self-Regulation and Privacy Online: A Report to Congress* (Washington, DC: FTC, 1999).

[130] Definitions are taken from Kosseff, *supra* note 111 at 162.

[131] See FTC 2012 Report, *supra* note 129 at 61-64.

[132] *Ibid*. at 64-71.

[133] *Ibid*. at 71-72.

[134] *Ibid*. at 22-35.

[135] *Ibid*. at 35-60.

[136] *Ibid*. at 60-72.

that EU Member States had to ensure adequate levels of privacy protection for data transfers in another jurisdiction. *PIPEDA* was therefore enacted to ensure that Canadian firms provided an adequate level of protection for data coming from the EU.[138]

PIPEDA operates under the federal government's competence in trade and commerce under s 91(2) of the *Constitution Act*, *1867*.[139] Given that Canadian provinces can pass laws respecting property and civil rights in the province under s 92(13)[140] of the *Constitution Act, 1867*, and local or private matters under s 92(16)[141] of the same, they can enact their own laws respecting data protection.[142] However, since commercial activity involving interprovincial and international personal data flows is regulated by *PIPEDA*, this legislation sets the data protection benchmark for most Internet-related firms.[143]

PIPEDA sets out broad principles in relation to personal information flows, which are all set out in Schedule 1 of the Act:

- *Accountability*, meaning "[a]n organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles."[144]
- *Identifying purposes*, meaning "[t]he purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected."[145]
- *Consent*, meaning "[t]he knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate."[146]

---

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

[138] See Michael Power, *The Law of Privacy* (Toronto: LexisNexis, 2017) at 65.

[139] See *Constitution Act, 1867* (UK), 30 & 31 Vict, c 3, s 91(2), reprinted in RSC 1985, Appendix II, No 5.

[140] *Ibid*., s 92(13).

[141] *Ibid*., s 92(16).

[142] See Power, *supra* note 138 at 7-11 (enumeration of all federal and provincial statutes respecting privacy in Canada).

[143] Only a few general data protection statutes applicable to private entities within a province have been enacted. See *Personal Information Protection Act*, SBC 2003, c 63; *Personal Information Protection Act*, SA 2003, c P-6.5; *An Act respecting the protection of personal information in the private sector*, CQLR, c P-39.1. Provincial data protection laws otherwise apply only to specific sectors and types of data, like health, or to the provincial public sector. See e.g. *Health Information Act*, RSA 2000, c H-5 (legislating data protection rules in the Alberta healthcare system); *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165 (legislating data protection rules in the British Columbia public sector).

[144] See *PIPEDA*, supra note 137 at Schedule 1, s 4.1.

[145] *Ibid*. at Schedule 1, s 4.2.

[146] *Ibid*. at Schedule 1, s 4.3.

- *Limiting collection*, meaning "[t]he collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means."[147]
- *Limiting use*, *disclosure, and retention*, meaning "[p]ersonal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes."[148]
- *Accuracy*, meaning "[p]ersonal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used."[149]
- *Safeguards*, meaning "[p]ersonal information shall be protected by security safeguards appropriate to the sensitivity of the information."[150]
- *Openness*, meaning "[a]n organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information."[151]
- *Individual access*, meaning "[u]pon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate."[152]
- *Challenging compliance*, meaning "[a]n individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance."[153]

Each principle is enriched by more specific obligations under it. *PIPEDA* provides a few exceptions to these obligations.[154] *PIPEDA* directs a *balancing of interests* philosophy[155] to interpret the scope of the principles in different situations.[156] This philosophy aims to take notice of the context under which *PIPEDA* takes effect — a data economy, where business objectives are tightly

---

[147] *Ibid.* at Schedule 1, s 4.4.

[148] *Ibid.* at Schedule 1, s 4.5.

[149] *Ibid.* at Schedule 1, s 4.6.

[150] *Ibid.* at Schedule 1, s 4.7.

[151] *Ibid.* at Schedule 1, s 4.8.

[152] *Ibid.* at Schedule 1, s 4.9.

[153] *Ibid.* at Schedule 1, s 4.10.

[154] *Ibid.*, ss 7-11.

[155] *Ibid.*, s 3: The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

linked with the collection, use, and disclosure of data — and the need to protect citizens' personal integrity.[157] In contextualizing data protection, the Privacy Commissioner also monitors the market and privacy innovations and produces research reports for businesses and the public.[158]

Complaints can be filed with the federal Privacy Commissioner under s 11 of *PIPEDA*. The Commissioner has to then investigate the complaint[159] and eventually either dismisses it[160] or publishes a report outlining findings and recommendations.[161] The Commissioner may then enter into a compliance agreement with the respondent[162] or initiate proceedings before the Federal Court to ultimately have that Court order remedies and other measures aimed at remedying a breach of the Act.[163] Finally, the Privacy Commissioner may audit the data protection practices of a company if they have "reasonable grounds to believe that the organization has contravened" the Act.[164] Contrary to its United States and EU counterparts, the Privacy Commissioner does not have the power to impose fines or make orders directly, something that its head has criticized.[165]

(c) European Union

Until May 2018, the European Union's data protection legislation was the Data Protection Directive. The General Data Protection Regulation ("GDPR") that has since come into force replaces the Directive and updates its various obligations. The Regulation is comprehensive and enumerates obligations that are binding on a *data controller* — meaning the entity who "alone or jointly with others, determines the purposes and means of the processing of personal data"[166]

---

[156] See e.g. *Englander v. Telus Communications Inc.*, 2004 FCA 387, 2004 CarswellNat 4119, 2004 CarswellNat 5422 (F.C.A.) at para. 46:

> All of this to say that, even though Part 1 and Schedule 1 of the Act purport to protect the right of privacy, they also purport to facilitate the collection, use and disclosure of personal information by the private sector. In interpreting this legislation, the Court must strike a balance between two competing interests. Furthermore, because of its non-legal drafting, Schedule 1 does not lend itself to typical rigorous construction. In these circumstances, flexibility, common sense and pragmatism will best guide the Court.

[157] See Power, *supra* note 138 at 75.

[158] See *PIPEDA*, *supra* note 137, s 24.

[159] *Ibid.*, s 12.

[160] *Ibid.*, s 12.2.

[161] *Ibid.*, s 13.

[162] *Ibid.*, s 17.1.

[163] *Ibid.*, s 15.

[164] *Ibid.*, s 18.

[165] See Canada, Office of the Privacy Commissioner, "Facebook Allegations Underscore Deficiencies in Canada's Privacy Laws" (Ottawa: Office of the Privacy Commissioner, 2018), online: <www.priv.gc.ca/en/opc-news/news-and-announcements/2018/oped_180326/> [Office of the Privacy Commissioner Op-ed].

[166] 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*

— and *data processor* — meaning the entity "which processes personal data on behalf of the controller."[167]

Data processing, under the GDPR, is governed by the guiding principles, which are expanded in later provisions of the Regulation. Contrary to the United States and Canadian law, under the GDPR, a data controller has the burden of demonstrating their adherence to the principles:[168]

- *Lawfulness, fairness, and transparency*, meaning personal data must be "processed lawfully, fairly and in a transparent manner in relation to the data subject";[169]
- *Purpose limitation*, meaning personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes";[170]
- *Data minimization*, meaning personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed";[171]
- *Accuracy*, meaning personal data must be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay";[172]
- *Storage limitation*, meaning personal data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed";[173]

---

data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ, L 119/1 at art 4(7) [GDPR].

[167] *Ibid*., art 4(8).

[168] *Ibid*., art 5(2). See also Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Cham: Springer International Publishing, 2017); Zuiderveen Borgesius, *supra* note 38 at 99-102 (analysis of GDPR principles).

[169] See GDPR, *supra* note 166, art 6 ("Lawfulness of processing," including the obligation to ascertain consent or necessity to data processing), art 7 ("Conditions for consent"), art 12 ("Transparent information, communication and modalities for the exercise of the rights of the data subject"), art 13 ("Information to be provided where personal data are collected from the data subject"), art 14 ("Information to be provided where personal data have not been obtained from the data subject"), art 15 ("Right of access by the data subject"), art 30 ("Records of processing activities"), art 33 ("Notification of a personal data breach to the supervisory authority"), Chapter 4, s 4 ("Data protection officer").

[170] *Ibid*., art 21 ("Right to object"), art 22 ("Automated individual decision-making, including profiling").

[171] *Ibid*., art 9 ("Processing of special categories of personal data"), art 18 ("Right to restriction of processing").

[172] *Ibid*., art 16 ("Right to rectification"), art 18 ("Right to restriction of processing").

[173] *Ibid*., art 17 ("Right to erasure ('right to be forgotten')"), art 18 ("Right to restriction of processing").

- *Integrity and confidentiality*, meaning personal data must be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."[174]

Similar to the United States and Canada, *privacy by design* — the idea that technologies should be designed with ensuring privacy as a primary consideration — is included in the GDPR.[175] The Regulation also prescribes that Member States must establish a "supervisory authority" empowered to monitor the application of its various rules.[176] Additionally, a supervisory authority can act proactively in various respects. Notably, it can monitor relevant data protection developments,[177] give advice as to best practices, and adopt standard contractual clauses for firms to use in their privacy policies.[178] The Regulation also favours the adoption of industry codes[179] and certifications[180] as possible regulatory tools to be monitored by another competent authority.

The Regulation orders that supervisory authorities be granted sometimes far-reaching investigative powers, which include the power to carry out data protection audits and obtain access "to any premises [. . .] including to any data processing equipment and means."[181] Additionally, they may issue warnings and reprimands and order performance of various acts by a data controller or processor.[182] Finally, a data subject may submit a complaint to the supervisory authority in the Member State where they reside.[183] This might lead a supervisory authority to issue an order, or a fine.[184] The Regulation, however, does not bind authorities to represent the complainant in court to obtain a remedy.

---

[174] *Ibid*., art 22 ("[Right to be free from] automated individual decision-making, including profiling"), art 24 ("Responsibility of the controller"), art 25 ("Data protection by design and by default"), art 32 ("Security of processing"), art 35 ("Data protection impact assessment"), art 36 ("Prior consultation"), ch 5 ("Transfers of personal data to third countries or international organisations").

[175] *Ibid*., art 25.

[176] *Ibid*. at ch 6.

[177] *Ibid*., art 57(i).

[178] *Ibid*., art 57(j)

[179] *Ibid*., art 41.

[180] *Ibid*., art 42

[181] *Ibid*., art 58(1).

[182] *Ibid*., art 58(2).

[183] *Ibid*., art 80.

[184] *Ibid*., art 83. As underscored in Part III, fines can be very significant.

(d) Comparing the US, Canada, and the EU's Data Protection Framework

To bring to light the different choices made by each jurisdiction, we compare their data protection framework through three angles: regulatory design, the place of industry codes, and enforcement powers.

(i) Regulatory Design

Of the three jurisdictions studied, the United States has the data protection regime that places the most emphasis on self-regulation. At the other end, the EU takes the most interventionist approach to data protection, with comprehensive data regulations binding on member states. Canada has recently adopted amendments to *PIPEDA* that bring it closer to the GDPR, although the powers of the Privacy Commissioner are not as strong as those under the GDPR.

Although the FTC has greatly promoted industry codes since the early Internet,[185] and although many such codes remain in use,[186] this has not stopped the FTC from intervening under its competence to investigate unfair and deceptive practices, which is now subject to a full-fledged legal test.[187] As such, the FTC framework should theoretically achieve, albeit through greater legal exegesis, a good ambit of protection, similar to other jurisdictions, despite its broadness.[188] Its publications clarifying data protection principles and constant enforcement actions against companies ultimately delineate clear obligations by which corporations need to abide.[189] The FTC's attempts to draw out principles of data protection ultimately serve a role similar to Schedule 1 of *PIPEDA* or Article 4 of the GDPR (although we should underscore that the GDPR principles are expanded to create full-fledged obligations in other provisions of the Regulation). The added benefit of this approach is that the American regulatory scheme is more flexible and can follow industry developments more closely. This, however, is done at the expense of clarity, as the degree to which the industry can effectively adhere to clear and sufficiently precise standards becomes reduced. As a result, corporations are less certain what their obligations are — or consumers, their rights. The opposite is true in the EU, whose comprehensive Regulation establishes clear standards and duties on both

---

[185] See Hirsch, "The Law," *supra* note 7 at 459 (historical overview of data protection and self-regulation in the United States). See also FTC 1999 Report, *supra* note 129; FTC 2009 Report, *supra* note 129.

[186] See e.g. "Guidelines for Online Privacy Policies" (7 August 2018), online: *Online Privacy Alliance* < www.privacyalliance.org/resources/ppguidelines/ >; "NAI 2018 Code of Conduct" (7 August 2018), online (pdf): *Network Advertising Alliance* < https://www.networkadvertising.org/sites/default/files/nai_code2018.pdf >.

[187] See Kosseff, *supra* note 111 at 4-5 (describing a three-part test for determining unfair or deceptive practices).

[188] Moreover, the FTC's authority over data protection was confirmed quite clearly by the U.S. Court of Appeals for the Third Circuit. See *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir., 2015).

[189] See *supra* note 129.

controller and *processor* — something Canada somewhat provides, but not the United States.

(ii) Place of Industry Codes

All three jurisdictions encourage industry codes as part of their data protection framework.[190] In all three cases, the regulator shows interest in seeing certain (perhaps more fastidious) aspects of data protection being self-regulated with sectoral rules that address privacy issues with greater precision. What then distinguishes industry codes according to each jurisdiction is the general framework within which they exist and the enforcement mechanisms backing them. The general framework within which industry codes exist affects them insofar as they create the basic rules that are then substantiated by industry codes.

For example, in the United States, where the only legislative guidance on data protection is the broad duty arising under Section 5 of the FTC Act, voluntary codes inject content into the general obligation. In Canada and the EU, on the other hand, industry codes are drafted in response to laid-out and relatively precise obligations under the law, especially in the context of the GDPR. Industry codes are then not *jurisgenerative* or *boundary-setting* so much as they may express legal rules in a more contextualized way. Their function is therefore less significant than in the United States, though they can still be very useful.

Since industry rules are adopted by industry members and their teeth depend on members' active and continuous adherence to them, they are more difficult to enforce, whereas statutory rules can be enforced through state sanction. The United States and Canada take a completely hands-off approach to monitoring industry codes.[191] Indeed, the FTC and the Privacy Commissioner encourage industry codes, but they do not take part in their enforcement, contrary to the EU, which authorizes specially-appointed bodies to monitor their compliance and take measures to lead parties into compliance.[192]

(iii) Enforcement

Agencies in charge of enforcing data protection legislation have different powers to enforce their rules. The FTC can autonomously impose a fine on a defaulting party only after it fails to comply with a cease-and-desist order. The fines cannot exceed USD 10,000.[193] For this reason, the FTC will normally enter into consent orders with firms, and the breach of these orders can be sanctioned by a court with millions of dollars in penalties.[194] The Canadian Privacy

---

[190] *Ibid.*; *PIPEDA*, *supra* note 137, s 24; GDPR, *supra* note 166, art 40.

[191] See *supra* note 129.

[192] See GDPR, *supra* note 166, art 41.

[193] See FTC Act, *supra* note 121 at § 45.

[194] *Ibid.*

Commissioner works similarly but cannot impose fines or make orders. As such, the Commissioner is entirely reliant on the Federal Court to issue and enforce compliance orders.[195] Conversely, the EU GDPR empowers supervisory authorities with much greater powers to order fines and compel certain actions. Supervisory authorities can autonomously impose fines as high "20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher"[196] and make various orders to make a controller or processor comply with the provisions of the GDPR.[197]

Thus, EU supervisory authorities, under the GDPR, have the most direct power over non-compliant firms. Since the FTC and the Canadian Privacy Commissioner cannot directly fine a firm for insufficient data protection practices, their ability to intervene in each case is limited. As a result, they will often settle with the non-compliant firm rather than going through full-fledged court proceedings to induce compliance and order remedies for serious violations of data privacy.[198] The Canadian Privacy Commissioner has himself expressed multiple times that he would like his office to have more investigative and inspection powers of company data protection practices to keep private firms in check.[199]

(e) Criticisms

Several criticisms can be formulated for each data protection framework. These put in perspective the challenges of balancing adequate data protection with encouraging businesses to reap the benefits of Big Data to innovate.

The United States, as we have described, has a very fractured data protection framework. Privacy is protected through a patchwork of statutory provisions in each state and at the federal level, providing for privacy in discrete contexts, but no universally applicable protection exists at the statutory or constitutional level.[200] This leads to the creation of a "consumer privacy regime primarily concerned with ease of compliance for companies, and [shielded from] more consumer-protective modifications."[201] Accordingly,

---

[195] See *PIPEDA*, *supra* note 137, s 24.

[196] See GDPR, *supra* note 166, art 83.

[197] *Ibid.,* art 58(2).

[198] See Kosseff, *supra* note 111 at 320.

[199] See Office of the Privacy Commissioner Op-ed, *supra* note 165; Canada, Office of the Privacy Commissioner, "Appearance before the Standing Committee on Access to Information, Privacy and Ethics (ETHI) on the Study of the *Personal Information Protection and Electronic Documents Act* (PIPEDA)" (Ottawa: Office of the Privacy Commissioner, 2017) [Appearance before the Standing Committee].

[200] See Barrett, *supra* note 119 at 1068.

[201] *Ibid.*

> the patchy protections of sectoral regulation, the failures of notice and choice without strong enforcement to compensate for them, and the narrow definition of what kind of harms merit judicial or administrative redress reflect this conceptual and legal diminishment of privacy, and often keep protections for it from being effective.[202]

Furthermore, actions to prevent data breaches by the FTC are often unclear, as the FTC often does not comment on its decisions, and unsatisfying, as its enforcement actions are often limited or even absent.[203]

The interventionist framework of the EU's GDPR, whose approach most closely aligns with the government regulation approach among the three jurisdictions studied, entails that national data protection agencies in charge of regulating data protection have a lot more oversight and power. These are seen by the EU as necessary to protect the privacy of Internet users. Adopted in 2016, the GDPR entered into force only in May 2018 to give companies time to adjust to the major changes that the Regulation would bring about.[204] Two years in, it is difficult to estimate the law's long-term effects. The Regulation addresses many of the problems that experts found in its predecessor, the Data Protection Directive.[205] However, as noted by multiple observers, the GDPR has had several negative consequences in the short term.[206] For example, a survey of mergers and acquisitions professionals from Europe, Africa, and the Middle East from July 2018 revealed that 55% declared having worked on transactions that did not go through due to concerns about companies' compliance with the GDPR.[207] Furthermore, 56% of respondents in a survey from October 2018 of data protection professionals at organizations subject to the GDPR said their organizations are far from complying with the GDPR or will never comply.[208] Finally, French and UK (which was still a member of the EU at the time) data protection agencies expressed being overwhelmed by the demands brought on by the Regulation and concerned about not having enough resources to enforce

---

[202] *Ibid.*

[203] *Ibid.* at 1075 — 76.

[204] See He Li, Lu Yu, and Wu He, "The Impact of GDPR on Global Technology Development" (2019) 22:1 J Global Information Technology Management 1 at 1.

[205] See Neil Robinson et al, *Review of the European Data Protection Directive* (Santa Monica, CA: RAND Corporation, 2009) at 38-39.

[206] See Eline Chivot & Daniel Castro, "What the Evidence Shows About the Impact of the GDPR After One Year" (17 June 2019), online (pdf): *Center for Data Innovation* <www2.datainnovation.org/2019-gdpr-one-year.pdf>.

[207] See Merrill Corporation, "GDPR Burdens Hinder M&A Transactions in the EMEA Region, According to Merrill Corporation Survey" (13 November 2018), online: *Merrill Corporation* <www.merrillcorp.com/us/en/company/news/press-releases/gdpr-burdens-hinder-m-a-transactions-in-the-emea-region.html>.

[208] See IAPP and Ernst & Young, "Annual Governance Report 2018", online: *IAPP and Ernst & Young* <iapp.org/resources/article/iapp-ey-annual-governance-report-2018/>.

it.[209] Hence, while expansive regulation ensures that a consumer's rights are protected on paper, it does not mean that the data protection agency will be efficient or effective in practice.

Canada falls between the United States and the EU in terms of regulation. While establishing guiding principles and distinct obligations, it does not go as far as the EU in terms of the obligations imposed on firms handling personal data and the powers vested in the regulator to take action in each case. This means that while data protection obligations under Canadian law are better defined, the means to enforce them are deficient in significant respects. Like in the United States, the statutory framework presumes that firms will govern themselves or can simply be nudged into compliance.

PART III: *PROACTIVE CO-REGULATION AS THE PATH FORWARD FOR DATA PROTECTION ON SOCIAL NETWORKING SITES*

The discussion so far shows that there is a real concern with respect to the nature of data protection regulation and the effects of that framework in each jurisdiction. Elements of self-regulation and government regulation have their advantages and disadvantages from a regulatory perspective. While excessive reliance on self-regulation, as in the United States, points to several major shortcomings, heavy regulation, as can be found in the EU, can also burden the industry and can sometimes be difficult for even a local regulator to apply. At the same time, an incomplete set of tools limits the range of solutions a regulatory agency can pursue in each case. As such, we aim to argue in this Part that in searching for a regulatory approach that bridges these concerns, legislators should adopt elements of both self- and government regulation, an approach which has been named "co-regulation."[210] In particular, regulators should consider regulatory negotiations as one of the most powerful tools to create rules that are effective and adapted to business reality.

(a) Government, Self- and Co-Regulation: Pros and Cons

Self-regulation has been adopted and is still favoured by several on the assumption that, as a regulatory framework, it procures several benefits that cannot be achieved through government regulation. For example, proponents of self-regulation argue that it (a) "overcome[s] the problem of information deficits

---

[209] See Chivot & Castro, *supra* note 206 at 6.

[210] It is important to note that definitional frontiers of co-regulation are blurry. As such, co-regulation may be an umbrella term for a multitude of regulatory arrangements. See Hirsch, "The Law," *supra* note 7 at 465; Ira S Rubinstein, "The Future of Self-Regulation is Co-Regulation" in Evan Selinger, Jules Polonetsky & Omer Tene, *The Cambridge Handbook of Consumer Privacy* (Cambridge, UK: Cambridge University Press, 2018) [Rubinstein, "The Future"]; Ira S Rubinstein, "Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes" (2011) 6 ISJLP 355 at 371 [Rubinstein, "Privacy"].

of state regulation because [private actors] benefit from greater expertise and special skills within the industry"; (b) "[is] faster and more flexible than state regulation, mostly because [it is] not bound by statutory procedures to the same extent as state regulation"; (c) "reduce[s] regulatory cost to the state's arid implementation costs in general, especially because profit-driven companies are supposed to carry out the self-regulatory process more cost efficiently"; and (d) "[is] applicable in areas sensitive to state regulation," such as where regulation might impede on protected freedoms.[211] In the context of data protection, arguments are also presented to the effect that competition should push Internet-centred firms to ensure their users' data is protected.[212]

Co-regulation and government regulation advocates argue that these benefits, while theoretically potent, fail in practice. They argue self-regulation (a) "provide[s] symbolic policy with weak standards, ineffective enforcement, mild sanctions and limited reach, because [it] often appl[ies] only to those who voluntarily participate and not to all members of an industry"; (b) "result[s] in self-service by the industry, with public interests being neglected vis-à-vis private interests, and the outsourcing of regulation may also result in a loss of know-how on the part of regulators, thus exacerbating existing information asymmetries"; (c) "entail[s] the danger of cartels and other anticompetitive behaviour, resulting from close cooperation between companies in self- and co-regulatory regimes and the dominance of large, long-established companies in self- and co-regulation may produce solutions that discriminate against smaller enterprises and newcomers"; and (d) "decrease[s] the democratic quality of regulation, especially owing to lack of accountability, transparency, legal certainty and the like."[213]

While stressing that there is no one form of co-regulation,[214] its proponents consistently argue that the collaborative relationship it fosters between government, industry, and other stakeholders will encourage firms to share insider knowledge of the industry more than if the government were drafting rules alone.[215] Ultimately, co-regulation would achieve cost-effectiveness, efficiency, effective enforcement, and enough flexibility to evolve along with the business landscape, which government regulation and self-regulation cannot achieve on their own.[216] Government and business would ultimately enjoy improved relations, sparking more creative and innovative responses to social problems, as well as making each party accountable to the other.[217]

---

[211] See Michael Latzer, Natascha Just & Florian Saurwein, "Self- and Co-regulation: Evidence, Legitimacy and Governance Choice" in Monroe E Price, Stefaan Verhulst & Libby Morgan, *Handbook of Media Law* (London: Routledge, 2013) 373 at 375.

[212] See Hirsch, "The Law," *supra* note 7 at 455.

[213] *Ibid.*

[214] See *supra* note 210.

[215] See Rubinstein, "Privacy," *supra* note 210 at 378.

[216] See Hirsch, "The Law," *supra* note 7 at 466-67.

On the other hand, co-regulation also has its criticisms. Detractors first argue that the industry, conscious of the knowledge imbalance that exists between itself, the regulator, and the public, will use its advantageous position to broker weaker standards. Secondly, co-regulation risks taking negotiations between government and industry behind closed doors, which prevents criticism from civil society from influencing public policy. Thirdly, co-regulation still does not address the problem of enforcement, whereby firms may still be allowed a degree of leniency if they have to enforce rules against themselves. Fourthly, ultimately, rather than bringing a collaborative spirit to business-government relations, legal obligations to shareholders will often overshadow good faith attempts at responding to societal concerns.[218]

Co-regulation has nevertheless been the subject of a number of compelling case studies, which give insight into its possibilities and effectiveness.[219] A notable one is Dennis Hirsch's study of Dutch privacy codes.[220] Through its *Personal Data Protection Act*, the Netherlands has adopted a comprehensive statutory scheme that implements the broad principles of the EU Data Protection Directive and allows industries to adopt their own codes that specify how the statutory requirements will apply in their particular context. These codes have been adopted in twenty sectors, including financial services. They are approved by the Dutch Data Protection Authority and enforced as a binding administrative decision.[221] Rubinstein summarizes Hirsch's conclusions regarding the codes as follows:

> (1) the need to clarify the broad terms of the PDPA as they applied to specific sectors and in some cases to forestall direct government regulation created sufficient incentives for companies to participate; also, the negotiation process (2) built sufficient trust between regulators and industry to promote both information sharing and joint problem solving between them, thereby taking advantage of industry expertise, and (3) led to more tailored, workable, and cost-effective rules.[222]

Thus, while bearing in mind that co-regulation is not a magic bullet and is only as effective as its design makes it, there is great promise in promoting context-specific regulation and information-sharing among the regulator, regulated firms, and other stakeholders.[223] As we will argue shortly, the form of regulatory

---

[217] *Ibid*. at 466.

[218] *Ibid*. at 468.

[219] See e.g. Kenneth A Bamberger & Deirdre K Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (Cambridge, Mass: MIT Press, 2015); Dennis D Hirsch, "Going Dutch? Collaborative Dutch Privacy Regulation and the Lessons It Holds for U.S. Privacy Law" (2013) Mich State L Rev 83 [Hirsch, "Going Dutch"].

[220] Hirsch, "Going Dutch," *supra* note 219.

[221] *Ibid*. at 119-120.

[222] Rubinstein, "The Future," *supra* note 210 at 521.

negotiations embodied in Dutch privacy codes offers the best solution to regulate data protection on SNSs.

(b) Transparency and Accountability: Why the Self-Regulation of SNSS Failed

In the context of SNSs, self-regulation failed to provide adequate data protection due to its substantial deficiencies in transparency and accountability.[224] It has failed in transparency because neither the regulator nor consumers can verify that SNSs are complying with privacy obligations.[225] As shown in Part I, consumers are in an extremely unbalanced relationship with SNSs. Rarely are they aware of how their information is collected and used, and they are even less aware of the amount of information. Furthermore, information regarding a firm's data practices has usually been sanitized in documentation provided in help sections and privacy policies or is written with so much imprecision it is impossible to concretely grasp what is, in fact, being described.[226] In short, consumers have scarce control over how their data is collected. This, along with the general lack of information about the internal workings of a company, ultimately makes protecting consumers' personal data very difficult for the regulator and protecting one's own privacy very difficult for consumers.

Moreover, at least in the United States and in Canada, accountability mechanisms greatly lack in teeth as the regulator's powers to make orders and impose fines are limited, which makes their oversight less effective and efficient.[227] Furthermore, under the American and Canadian regimes, the regulator does not have powers to audit without reasonable grounds to believe that the SNS has infringed the law[228] or conduct unannounced inspections on SNS premises to ascertain their compliance with privacy standards. In the absence of sufficient market incentives to adopt and implement robust privacy practices, the regulator's supervisory function becomes especially crucial. While proponents of the free market claimed that consumers would gravitate towards products with better privacy protections and that competition would promote

---

[223] Hirsch also notes problems with the Dutch framework for regulatory negotiations and offers suggestions to improve it. See Hirsch, "Going Dutch," *supra* note 219 at 118, 152-53.

[224] See Zukina, *supra* note 60 at 296; Rubinstein, "Privacy," *supra* note 210 at 356.

[225] See Part I above.

[226] See *supra* note 68.

[227] See Canada, Office of the Privacy Commissioner, "Powers and Functions of the Ombudsman in the *Personal Information Protection and Electronic Documents Act*: An Effectiveness Study" by France Houle & Lorne Sossin (Ottawa: Office of the Privacy Commissioner, 2010) at 166 ("the ability to levy fines and other order-making capabilities can lead to additional compliance and serve as an important deterrent even if not used often.").

[228] See *PIPEDA*, *supra* note 137, s 18; *FTC Act*, *supra* note 121 at § 45.

the progressive sharpening of privacy tools by the industry, thus creating an Internet landscape with robust protections of personal data, this is not what happened in fact.[229] As outlined in Part I, consumers, despite their claims to greatly caring about their privacy, are unwilling to switch to SNSs with stronger privacy practices if their social network does not also migrate to it. As a result, the innovative impulse at the root of competition and underlying the self-regulatory paradigm is severely undermined.[230]

Accountability, as several authors have pointed out, has been further hindered by the fact that industry codes have failed to produce an effective regulatory framework.[231] Rules set by industry codes are often lenient and not aimed at instilling long-term changes in practices in the biggest firms.[232] Moreover, given that these codes are based on voluntary compliance and major firms have no compelling reason to take on additional obligations, their proposed rules ultimately receive lax implementation.[233] Additionally, industry codes are limited in scope and thus only cover certain activities, while leaving others in a regulatory gap. For example, SNSs might voluntarily adhere to an advertising industry code, but other activities with business partners, for example, data aggregation, might not be covered under an existing industry code, leaving SNSs free from even self-generated constraints. This opens the door to unscrupulous practices, as well as diminishes the value of industry codes and their purported oversight.

(c) Co-Regulation as the Path Forward for Data Protection on SNSS: A Few Principles and Ideas for the Future

To fill current gaps in transparency and accountability, as well as craft regulation that can be implemented effectively in practice, it is necessary, more than ever, to craft regulation that achieves its objectives in the most efficient manner possible. This can only be achieved through co-regulation characterized by intense collaboration between the regulator and regulated firms. Indeed, some of the main difficulties in regulating data protection on SNSs is their complexity and opacity. Each SNS platform is unique, as is its interaction with third parties. Furthermore, information about each SNS's internal operations is limited. Thus, while SNSs benefit from an oligopolistic position in the market, their complexity and the lack of public information about them make context-specific regulations characterized by significant information-sharing appropriate and necessary. Due

---

[229] See Stucke & Grunes, *supra* note 27 at ch 5.

[230] *Ibid*. See also Lauren E Willis, "Why Not Privacy by Default?" (2014) 29 BTLJ 61 at 67.

[231] See Cody, *supra* note 19 at 1223.

[232] See Kim, *supra* note 88 at 335-36; Asay, *supra* note 88 at 331-32; Zukina, *supra* note 60 at 291.

[233] For example, Twitter and LinkedIn have withdrawn from Do Not Track rules, which are voluntary rules aimed at limiting tracking using cookies by the online behavioural advertising industry. See Twitter Privacy Policy, *supra* note 68; LinkedIn Cookie Policy, *supra* note 68.

to inherent complexity of the subject, a one-size-fits all approach is more likely to be ineffective.[234]

To this end, the legislator should first adopt a framework legislation setting out clear obligations. Concurrently, an industry code governing data protection on SNSs that specifies and supplements the obligations contained in the framework legislation for their particular context should be adopted following regulatory negotiations involving the regulator, regulated firms, and other stakeholders.

(i) Co-Regulating SNSs: A Proposal

An adequate co-regulatory model aimed at data protection must exist under a framework law that clearly sets out the various principles, rights, and obligations that are necessary to ensure minimum levels of transparency and accountability to consumers. These include, among others, adequate requirements for consent, as well as provisions of information on how to assert rights with regards to one's personal data, namely the right to know who has access to one's data and what that person or entity is using it for, the right to secure data processing and to hold accountable people along the data chain, and the right to restrict data processing. As well, persons and entities collecting data must have clear obligations to limit their collection only to what the consumer has explicitly consented to (accordingly, pre-emptive data collection, that is, collecting data only on the assumption that it will have some use in the future, should be forbidden), to use adequate technological safeguards to prevent breaches while storing personal data, and to keep records of processing activities and ensure third-party processing of data is done with sufficient measures to protect data's confidentiality during processing. On their end, third parties that process data must have a stated obligation to be open and transparent with consumers and the data collector. In addition to this, they should only process data as necessary to achieve the objectives to which a consumer has consented. These rules would serve as benchmarks for protecting consumers' data, thus creating a basic protection that consumers can always fall back on in the absence of clear regulation on the subject.[235] They should be set out in a way similar to the GDPR, codifying certain obligations that, while relatively precise, still allow room for the industry and other stakeholders, such as consumer protection associations, to determine the specific acts by which the industry will be deemed to have complied with its obligations under the law via regulatory negotiation. For example, while the framework law would clearly outline under what circumstances consent to the collection of one's personal data would be valid, the parties would still have some freedom to determine what tools and mechanisms are to be used to obtain a consumer's consent and what features these can have

---

[234] See Asay, *supra* note 88 at 323.

[235] See Hirsch, "The Law," *supra* note 7 at 465-66.

to limit the risks of confusion and misinformation, in conjunction with other market stakeholders.

Legislating certain fundamental data rights, following the approach taken notably in the EU,[236] ensures that consumers are treated fairly throughout the use of their data and provides them with adequate ability to verify how their data is being used and to retain control over it.[237] At the very least, it gives them a clear and solid legal basis to assert their rights before SNSs using their data. Enacting minimum transparency rules also proves an effective way of increasing accountability.[238] Because effective transparency obligations lead to the exposure of careless practices, SNSs become more at risk of legal liability, which incentivizes more assiduous privacy self-enforcement practices, to the benefit of consumers.[239]

Transparency and accountability can also be increased through empowering the regulator with more extensive powers to audit and inspect firms, including SNSs, as well as make orders and issue fines to keep Internet firms accountable.[240] For one, this would ensure greater ease of regulatory enforcement and would facilitate accountability of Internet firms before consumers. One major problem of self-regulation to this day, and which has led to its recurrent inefficiency in enforcement, is the fact that sanctioning a firm's negligent data practices once in a blue moon is insufficient to ensure self-regulated industries remain accountable. Past examples show that when the regulator chastises a firm for breach of privacy in a self-regulatory industry, the firm will immediately trigger reactive measures and give multiple assurances that it recognizes its mistake and has implemented robust protocols to prevent similar regulatory failure from happening in the future. However, once the public eye has moved on and the firm is no longer scrutinized, with no more incentive to follow rigorous guidelines, the firm will often end up drifting back to its negligent practices.[241] As a result, in addition to ramping up transparency regarding data processing activities of SNSs, it is also important that firms see continuous monitoring to ensure compliance with privacy obligations. To this end, privacy audits and unannounced inspections have been recommended as potential means to keep companies in check.[242] Both methods are relatively inexpensive, and,

---

[236] See Barrett, *supra* note 119.

[237] See Lievens and Valcke, *supra* note 15 at 564.

[238] See Zuiderveen Borgesius, *supra* note 38 at 100.

[239] *Ibid*.

[240] See Office of the Privacy Commissioner Op-ed, *supra* note 165; Appearance before the Standing Committee, *supra* note 199; Houle & Sossin, *supra* note 227 at 160, 165-66.

[241] See Hirsch, "The Law," *supra* note 7 at 467.

[242] See e.g. Appearance before the Standing Committee, *supra* note 199 (the Privacy Commissioner referred to submissions made by various stakeholders across Canada, including, among other suggestions, that proactive methods such as audits be employed).

when done periodically, they can push a company to uphold rigorous data protection standards.

SNSs' role within this framework is at the technical level, where their role is to aid in determining implementation. Here, we see a process of regulatory negotiations being used to achieve efficiency in cooperation with other stakeholders, such as consumer advocacy groups and other actors in the technology sector.[243] Regulatory negotiations (or "negotiated rulemaking") is a "statutorily-defined process by which agencies formally negotiate rules with regulated industry and other stakeholders as an alternative to conventional notice-and-comment rulemaking."[244] Contrary to conventional rulemaking, in which the government drafts legislation, then solicits testimonies from industry representatives and other interest groups, regulatory negotiations envisage a regulatory process in which various parties work toward a consensus on how to regulate a given subject matter.[245] Regulatory negotiations have already been discussed at length in academic literature since their initial proposal and have been applied notably to devise environmental regulation.[246] Several legal scholars have endorsed using these in the context of data protection.[247]

Regulatory negotiations are noted for five main strengths.[248] First, they are oriented towards problem-solving as they lead to the engagement of various parties with one another, which produces new and innovative solutions. Parties in a negotiation are induced into disclosing information they would not otherwise share in order to present their views and counter the other side's arguments, thus allowing for the proposition of sharper, more sophisticated and informed arguments and filling informational gaps.[249] Facing other viewpoints leads to zeroing in on each party's respective interests and developing more

---

[243] The original proposal for regulatory negotiations by Philip J Harter lays the theoretical groundwork and goes through the envisaged process, responding to various practical and theoretical concerns. See Philip J Harter, "Negotiating Regulations: A Cure for Malaise" (1982) 71 Geo LJ 1.

[244] Rubinstein, "Privacy," *supra* note 210 at 377. See also *Negotiated Rulemaking Act of 1990,* Pub L No 101-648, 104 Stat 4969 (codified at 5 USC §§ 561-570).

[245] See Harter, *supra* note 243 at 7.

[246] See e.g. Harter, *supra* note 243; Jody Freeman, "Collaborative Governance in the Administrative State" 45 UCLA L Rev 1; Nicholas A Ashford & Charles C Caldart, "Negotiated Regulation, Implementation and Compliance in the United States" in Eduardo Croci, ed, *The Handbook of Environmental Voluntary Agreements* (Dordrecht: Springer, 2005) 135; Ehren K Wade, "Just What the Doctor Ordered?: Heath Care Reform, the IRS, and Negotiated Rulemaking" (2014) 66:1 Admin L Rev 199; Cary Coglianese, "Assessing Consensus: The Promise and Performance of Negotiated Rulemaking" (1997) 46 Duke LJ 1255; Laura I Langbein & Cornelius M Kerwin, "Regulatory Negotiation versus Conventional Rule Making: Claims, Counterclaims, and Empirical Evidence" (2000) 10:3 J Public Administration Research & Theory 599.

[247] See Rubinstein, "The Future," *supra* note 210; Hirsch, "Going Dutch," *supra* note 219.

[248] See Freeman, *supra* note 246 at 21-33.

[249] *Ibid*. at 22-27.

creative solutions, as parties are encouraged to see rule-drafting not as a zero-sum game, but as a problem that can be solved to the benefit of everyone at the table.[250] A sub-product of this is that rules are generally arrived at more quickly and more cost-effectively.[251]

Second, regulatory negotiations allow for participation of interested and affected parties. By bringing in different interest groups in the regulatory process, the information base used to create the rule is more complete, which leads to a better appraisal of the reality of the problem and a greater likelihood of the adequacy of the proposed rule.[252] The confluence of different parties ensures that different expertise will be brought to the negotiating table. For example, a consumer rights advocate and an industry representative bring vastly different perspectives. The former can speak to the effects of corporate policies and practices on the lives of ordinary consumers and how best to protect their interests, while the latter brings a vast amount of knowledge, not only on their type of product, but also on the industry, how its actors behave, and how it is likely to evolve in the coming years. They may also offer insight as to the practical and technical realities which might hinder the implementation of certain rules.[253]

Third, the rules arrived at following regulatory negotiations are provisional in that they are temporary and subject to periodic revision. This ensures that rules can be tailored and responsive to the specific context for which they are drafted, and thus more effective. After being approved, rules are continually monitored so that parties can assess their effectiveness on an ongoing basis and either improve them or make adjustments to account for new developments in the industry and other relevant factors. [254] This characteristic entails long-term effectiveness and increased ability to react and adapt to innovations and changing conditions related to the subject matter of the regulation.[255] A further corollary is that such provisionalism requires continuous disclosure of information, which further enhances transparency.

Fourth, regulatory negotiations allow for accountability that transcends traditional public and private roles in governance. Depending on the role the

---

[250] See Carrie Menkel-Meadow, "Toward Another View of Legal Negotiation: The Structure of Problem-Solving" (1984) 31 UCLA L Rev 754 at 760.

[251] Some empirical studies have been ambivalent as to the cost-effectiveness and rapidity of regulatory negotiations. Overall the literature seems to suggest that if regulatory negotiations are not quicker or more cost-effective, they are at least not more costly and time-consuming than traditional rule-making. See e.g. Coglianese, *supra* note 246.

[252] See Harter, *supra* note 243 at 24; Freeman, *supra* note 246 at 27.

[253] Regulatory negotiations put greater emphasis on practical implementation of rules. See Ashford & Caldart, *supra* note 246 at 140 (noting an EPA representative's testimony that the agency had never before "been able to grapple with the economic and technological issues" addressed by the rule).

[254] See Freeman, *supra* note 246 at 29.

[255] *Ibid.*

regulator takes in the negotiation and in the framework law underpinning the negotiation, it is possible for parties to agree on alternative accountability mechanisms, insofar that they are allowed by law or the regulator, such as auditing, standard-setting organizations, or certification of bodies themselves certified by the regulator.[256]

Fifth, regulatory negotiations allow the regulator to be both engaged and flexible. Depending on the role that the regulator wants to take, they can act either as "a minimal standard-setter," "a convenor-facilitator of multi-party negotiations that are designed to produce goals, standards, and the measures necessary to judge whether they have been attained," or "a capacity-builder of institutions capable of partnerships in coregulation."[257] Despite the emphasis that regulatory negotiations put on private parties, the regulator still plays a role in shaping outcomes, which allows for the public interest, nonetheless, to remain represented during the negotiation. Engaging in a negotiation process, contrary to claims by some scholars, does not undermine the regulator's authority.[258] Ultimately, they retain the final authority to impose their rules to shape the negotiation process and enact regulations if discussions ultimately fail.[259]

The collaborative governance offered by regulatory negotiations, overall, proves more desirable than government regulation. Traditional rulemaking is characterized by great power imbalance: the very actor soliciting comments ultimately has all the power to determine what is enacted as law.[260] As a result, the adversarial component of rulemaking is exacerbated, and parties tend to adopt extreme positions in order to influence policy.[261] Additionally, under traditional adversarial rulemaking, parties might be less forthcoming and open to disclosing certain information which may undermine their bargaining position.[262] Regulatory negotiation seeks to overcome these challenges by bringing together affected groups and having them negotiate applicable rules for a given situation. Such negotiations are ultimately effective because they are in parties' best interests:[263] the subject area at the heart of the negotiation is either already government-regulated, or soon will be,[264] which means the industry has a compelling interest in influencing the drafting of the regulation. In the past, regulatory negotiations have notably been used in the environmental context to bind polluters to sustainability goals, thereby achieving better results than might

---

[256] *Ibid.*

[257] *Ibid.* at 31.

[258] See William Funk, "Bargaining Toward the New Millenium: Regulatory Negotiation and the Subversion of the Public Interest" (1997) 46 Duke LJ 1351 at 1374-87.

[259] See Freeman, *supra* note 246 at 32.

[260] See Rubinstein, "Privacy," *supra* note 210 at 377.

[261] See Harter, *supra* note 243 at 19.

[262] *Ibid.*

[263] *Ibid.* at 42.

[264] See Hirsch, "The Law," *supra* note 7 at 377.

otherwise be politically achievable under traditional rulemaking.[265] As a result of this process, the regulation that is eventually given binding force by the regulator also has more legitimacy and is thus easier to enforce.[266] Moreover, in addition to enforcement by the regulator, parties can also enforce the negotiated rule through alternative means, like privately-funded "certified observers," who independently monitor the industry's compliance with the rule.[267] Finally, regulatory negotiations ultimately prove much more flexible and responsive to specific conditions than other means of drafting and implementing regulation, thus allowing for more rapid policy improvements.[268]

This process should prove attractive to SNSs as it allows them to advance their economic self-interest while responding to public demands for accountability and privacy assurances, and it allows them to have a real impact on the formation of new industry rules. Given SNSs' great proficiency in technological innovations, including AI, they are in a prime position to advise other stakeholders on possible technological avenues that could allow them to comply with their obligations more efficiently. This is beneficial for consumers as well. SNSs know their product and the industry the best. They possess the most valuable insight into how technological innovation is likely to progress in the years to come.[269] For example, AI technologies, which are becoming increasingly widespread in online behavioural advertising, are a technology that could be regulated through regulatory negotiations. Due to the immense benefits this technology offers through automation and the significant impacts it can have on consumers' commercial activity, it is only fruitful that industry and consumer protection groups come together to address its regulation moving forward. The industry's knowledge, when brought into a negotiation conference, can allow for privacy measures that, while effective, can be more readily implemented as their greater flexibility and pragmatism will more closely fit business realities.

Concurrently, bringing in inputs from consumer groups regarding technological innovations can ultimately further the adoption of privacy by design. As stakeholders engage in a collaborative discourse regarding new technologies and the practical implementation of data protection standards, ensuring technologies at the epicentre of industry developments comply with these standards will naturally flow from the discussion. To take our earlier example, discussions on the requirements for consent will necessarily arrive at questions of "just-in-time" disclosures, opt-in consent, one-stop dashboards for opting out of targeted advertising, and other technologies that facilitate privacy

---

[265] See Rubinstein, "Privacy," *supra* note 210 at 373. See also Ashford & Caldart, *supra* note 246 at 140.

[266] See Rubinstein, "Privacy," *supra* note 210 at 378; Freeman, *supra* note 246 at 23.

[267] See Ashford & Caldart, *supra* note 246 at 143.

[268] See Rubinstein, "Privacy," *supra* note 210 at 373.

[269] *Ibid.*

self-management.[270] As a result of being part of a negotiation process, SNSs are more likely to effectively incorporate these privacy features into their interface.

Finally, collaborative governance, which is central to the co-regulatory model presented here, is most effective when it is accompanied by the political will to mandate administrative agencies to firmly tackle a given problem. Thus, absent a willingness to significantly change the current regulatory paradigm and meaningfully sanction abuses of personal data, the industry may have much less incentive to take part in the negotiation process. Fortunately, however, firms have historically been willing to adopt voluntary codes of conduct when faced with the possibility of stricter regulation.[271] Thus, despite their shortcomings, there may be a future for industry codes under co-regulation.

CONCLUSION

This article aimed to demonstrate the shortcomings of self-regulation as a regulatory paradigm for SNSs and argue for the adoption of a co-regulatory model that allows for proper balancing of both economic prosperity and consumer protection. As the role that SNSs play in people's daily lives increases dramatically, and as vast amounts of personal data are collected without regard for consumer integrity, the current model has failed to adequately protect consumers' privacy and make SNSs accountable for their actions. Given the significant amounts of personal data each SNS possesses on its users, and given the competitive value of this data, SNSs are in a powerful position in today's economy, as Big Data and AI are extracting considerable value out of this data. Moreover, SNSs have wide powers to collect and process personal data within and outside their ecosystem, unbeknownst to consumers. While proponents of self-regulation argued that competition would lead the market to develop better privacy practices as consumers would choose services with better privacy options, insights from behavioural economics show that this has simply not been the case. All of this showcases SNSs' unequal relationship with their users.

We looked at the data protection law of three jurisdictions: the United States, Canada, and the European Union. The United States possesses the most self-regulated data protection landscape, with a broad rule encompassing most subject matters and a regulatory architecture that favours settlements with companies at fault. Canada is slightly more regulated, offering data protection principles, but with similar powers as its United States counterpart. The EU, on the other hand, has the most rigorous data protection framework of the three, with comprehensive data protection regulation and powerful enforcement tools.

After looking at the benefits and shortcomings of government regulation, self-regulation, and co-regulation, we examined why self-regulation is ineffective for SNSs and proposed a co-regulatory model based around regulatory negotiations and clear data protection obligations to be used in the place of

---

[270] See Kosseff, *supra* note 111 at 320.

[271] See Rubinstein, "The Future of Self-Regulation," *supra* note 210 at 519.

self-regulation. We argued that such a model would respond to two major shortcomings of self-regulation, namely lack of transparency and accountability, and would promote a cost-effective, innovative, and tailored regulatory approach to SNSs. At the same time it would provide a focused regulatory solution and foster a greater exchange of information between the regulator, SNSs, and stakeholders.