Centre for International Governance Innovation

Digital Policy Hub

Digital Policy Hub – Working Paper

Digital Regulation and Innovation in Sweden, Korea and Canada

Shirley Anne Scharf

Winter 2024 cohort

About the Hub

The Digital Policy Hub at CIGI is a collaborative space for emerging scholars and innovative thinkers from the social, natural and applied sciences. It provides opportunities for undergraduate and graduate students and post-doctoral and visiting fellows to share and develop research on the rapid evolution and governance of transformative technologies. The Hub is founded on transdisciplinary approaches that seek to increase understanding of the socio-economic and technological impacts of digitalization and improve the quality and relevance of related research. Core research areas include data, economy and society; artificial intelligence; outer space; digitalization, security and democracy; and the environment and natural resources.

The Digital Policy Hub working papers are the product of research related to the Hub's identified themes prepared by participants during their fellowship.

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

Partners

Thank you to Mitacs for its partnership and support of Digital Policy Hub fellows through the Accelerate program. We would also like to acknowledge the many universities, governments and private sector partners for their involvement allowing CIGI to offer this holistic research environment.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Key Points

- This working paper examines digital regulation of citizens' personal information in Sweden, the Republic of Korea and Canada. It explores whether robust legislation precludes strong innovation performance on digital technologies.
- Sweden, through the European Union's General Data Protection Regulation (GDPR), is governed by particularly stringent legislation with respect to privacy rights, accountability systems and sanctions. Korea, governed through the Personal Information Protection Act (PIPA), has similarly comprehensive coverage.
- Canada's relevant legislation, the Personal Information Protection and Electronic Documents Act (PIPEDA), is now not only dated but also very modest in its protection of citizens' privacy rights.
- International innovation indicators on patents, venture capital (VC) investment and competitiveness do not indicate that rigorous digital legislation necessarily impedes innovation performance.
- Canada's digital legislation is very much in need of modernization. The GDPR and PIPA offer important models for protection of privacy rights and secure processing of data. These models need to inform any new Canadian legislation regarding data protection.

Introduction

In a highly digitalized world where personal data has been monetized, privacy rights of the individual compete with the global race for innovation and transnational data flows can be instantaneous, the capacity of the state to manoeuvre among these goals is deeply challenged. The regulation of digital technologies that a new age — and, essentially, a revolution — have ushered in, is particularly fraught. Public governance of those technologies must wrestle with the threat that regulation will smother the "creative destruction" (Schumpeter 1950) and dynamic capacity of firms, dampening the cycle that propels innovation, productivity and increased national wealth. This working paper seeks to examine this contested terrain from a comparative perspective, focusing on Sweden and the Republic of Korea — two innovation leaders (Organisation for Economic Co-operation and Development [OECD] 2016, 2023) — and Canada, a country with a much more problematic history on the innovation front (Scharf 2022, 2025, forthcoming 2025).

The paper examines whether robust regulatory frameworks for digitalization and citizen rights may impede innovation or whether the impact is more neutral. Thus, the governance issue addressed is not narrowed to a more unidimensional focus on growth and economic benefits. Rather, it is intended to embrace the implications of digitalization for larger issues around privacy and accountability — issues that contribute to and form fundamental building blocks of a nation's democratic health. For the purposes of this paper, digitalization refers to the economic and societal transformations that occur in the wake of the development, adoption and diffusion of digital technologies (such as massive computing power, machine-to-machine

connectivity, artificial intelligence [AI] and big data, among others), and the resulting interconnection.[1]

The paper unfolds in several parts. It briefly attends to theoretical considerations, situating this research within that context. But, primarily, the paper dives into an analysis that is twofold. It explores the robustness of digital legislation in Sweden, Korea and Canada through the respective dimensions of privacy rights, accountability and sanctions. The analysis centres around three seminal pieces of legislation in each country: the GDPR[2] that applies to Sweden; the PIPA[3] in Korea; and the PIPEDA[4] in Canada. It then examines innovation indicators that reflect these countries' standings on patents and investments related to key digital technologies, as well as their digital competitiveness. As such, the research question is: To what extent does digital regulation exist alongside, or preclude, high international rankings on innovation indicators associated with digital technologies? Policy conclusions follow.

Theoretical Framework

Dating back to Joseph A. Schumpeter (1950) and Kenneth J. Arrow (1962), the questions of market competitiveness, monopoly power and innovation have been an area of spirited debate and extensive empirical study. Nevertheless, the issue of regulation and technology innovation has become not only a much more contested arena, particularly riven by binary choices between suppressing technological change or unleashing the forces of innovation, but also where engagement on this question has been more underdeveloped. As Philippe Aghion, Antonin Bergeaud and John Van Reenen (2023, 2894) noted in terms of the economic discipline: "There is considerable literature on the economic impacts of regulations but relatively few studies on their impact on technological innovation."[5] The author of this working paper would add that the observation especially applies to digital technologies.

This issue has particularly resonated with Anu Bradford and her assessment of the debates around innovation in the United States and the European Union as being driven or hampered by "techno-libertarian" or "rights-driven models."[6] Recently, Bradford has moved these questions further, arguing that assumptions about a negative relationship between vigorous technological regulation and ensuing innovation need to be questioned. She maintains that debates have been cornered into a "false choice"

1 This definition draws from three concepts used in the OECD's (2019, 18) definition: digital technologies, data and interconnection.

2 EC, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJ, L 119/1 [*GDPR*], online: <https://eur-lex.europa.eu/eli/reg/2016/679/oj >.

3 *Personal Information Protection Act*, No 19234 (2011) (Republic of Korea) [*PIPA*], online: <https://elaw.klri.re.kr/eng_service/lawView.do?hseq=62389&lang=ENG>.

4 *Personal Information Protection and Electronic Documents Act* (SC 2000, c 5) [*PIPEDA*], online: <https://laws-lois.justice.gc.ca/eng/acts/p-8.6/FullText.html>.

5 With respect to seminal contributions on the relation between regulation and innovation, see Aghion et al. (2005); Aghion, Bergeaud and Van Reenen (2021); Amable, Demmou and Ledezma (2009); Blind, Petersen and Rillo (2017); Broughel and Hahn (2022); Chen, Frey and Presidente (2022); Johnson (2023); and Porcher (2013); also, on governance and innovation, Ugur (2013).

6 See Bradford (2024) on this issue and Bradford (2023) for her characterization of these digital regimes.

between digital regulation or innovation, with consequential assumptions that tech growth can only take root and thrive in a laissez-faire environment (Bradford 2024).

That said, there are grounds to suggest there is a theoretical space to further contribute to these questions. Examining the substantive nature of digital regulatory frameworks and focusing on nations where innovation has thrived (Sweden, Korea) or has had much less sustenance (Canada), can offer a meaningful path to advance these debates. This approach also goes beyond the concerns with superpowers, providing a more granular look at middle-nation-state experiences with regulatory efforts.

Sweden

The GDPR, under which Sweden (as a member state of the European Union) falls, has signalled a major shift in data privacy protection. Characterized as "the most extensive body of law aiming to regulate the activities involving personal data" (Bayamlıoğlu 2022, 1059), its import is unequivocal. The regulation came into force on May 24, 2016, and has applied to member countries since May 25, 2018. Central to its features and its significance are its defence of fundamental human rights, the rigour with which it governs privacy for the individual, the accountability structure it establishes and the sanctions in place for non-compliance.[7] Each of these is addressed in turn.

Governance and Privacy Protection

The "general provisions" of the GDPR are explicit as to purpose. The legislation protects the free flow of data among EU members (and the trade that necessarily involves), but its purpose is also grounded in the Charter of Fundamental Rights of the European Union, which lays out the "right to the protection of personal data."[8] Providing intent for the legislation, recital 1 of the GDPR lays out not only the attachment to the charter writ large but also to privacy protection for the individual. Article 1(2) in the legislation embeds the right in the body of the law, with the regulation going on to stipulate what this means and the conditions governing that protection.[9] There are several.

Personal data is to be "processed lawfully, fairly and in a transparent manner"[10] and is not to be the type of open-ended approach that leaves the individual's control over their data and their right to privacy compromised.[11] Rather, processing is to be transfixed to a specific purpose, limited in nature, maintained in an "accurate" manner, stored only as is necessary and secured with the appropriate systems in place.[12] So, too, are the

7 For useful accounts of the legislation, see Kuner, Bygrave and Docksey (2020), both on the articles and their historical origins; Hoofnagle, van der Sloot and Zuiderveen Borgesius (2019), particularly in relation to US law; Mondschein and Monda (2019); and GDPR.EU (https://gdpr.eu/what-is-gdpr/; also https://gdpr.eu/). On the robustness of this legislation, despite its complexity in balancing risks with human rights, Karen Yeung and Lee A. Bygrave (2022, 137) conclude that the GDPR is a resilient piece of legislation, with "in-built 'future-proofing.'"

8 *Charter of Fundamental Rights of the European Union*, [2012] OJ, C 326, art 8(1), online: <https://eur-lex.europa.eu/eli/treaty/char_2012/oj/eng>.

9 *GDPR*, *supra* note 2, art 1(2): "This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data."

10 *Ibid*, art 5(1)(a).

11 See Hoofnagle, van der Sloot and Zuiderveen Borgesius (2019) on the differences with US law.

12 *GDPR*, *supra* note 2, art 5(1)(b–f).

protections around the meaning of consent and the conditions under which it applies robust. The intent of consent is to be clearly specified and "distinguishable" from other matters.[13] The rights of the individual, or "data subject," are inclusive: to have access to the information collected about them;[14] to be able to correct that data[15] or erase it ("the right to be forgotten"[16]); to restrict processing of that data where relevant;[17] and, very significantly, to contest the processing[18] and, particularly, automated decision making when made without human supervision.[19] As well, the affected individual may essentially override that consent — "withdraw" it — at any time, in a manner that is not unduly burdensome.[20]

Two key aspects can be discerned in this. First, protection of the individual in maintaining their security and their right to privacy in the process is paramount. Second, as Yeung and Bygrave (2022, 139) point out, article 5 and the principles it articulates are "a central anchoring point" for the legislation and its governance.

Accountability

With respect to the accountabilities vested in the GDPR, these, too, are multifaceted in nature. Indeed, the GDPR broke new ground with respect to the responsibilities that now rest with the data controller (Kuner, Bygrave and Docksey 2020),[21] with the burden of responsibility being shifted away from the consumer (Hoofnagle, van der Sloot and Zuiderveen Borgesius 2019, 72). Some gaps are starting to emerge as the implications of the GDPR evolve (Dahi and Corrales Compagnucci 2022), but the accountability of the data controller to the data subject is exceedingly robust. As article 24 indicates, the controller is to take all necessary ("appropriate") action to "demonstrate that processing" is lawful and accords with the regulations.[22] Not only is the controller responsible to the individual or data subject, but they are also equally responsible for those who are "processing" the data and essentially under their purview.[23] The processor, in turn, must provide clear assurance ("guarantees") that the work undertaken aligns with the regulation. Thus, through the controller and those under their auspices, as it were, the rights of the individual are deemed to be protected. That is not all. This cascading series of responsibilities is to be further girded by systems established with the clear intent of meeting GDPR requirements. Systems set up by the data controller must, from the very beginning ("by design and by default"[24]), be embedded with means to protect the privacy and security of the individual within reasonable constraints concerning existing costs and infrastructure.

13 *Ibid*, art 7.

14 *Ibid*, arts 13–15.

15 *Ibid*, art 16.

16 *Ibid*, art 17.

17 *Ibid*, art 18.

18 *Ibid*, art 21.

19 *Ibid*, art 22.

20 *Ibid*, art 7(3): "It shall be as easy to withdraw as to give consent."

21 "Controller" is defined by the GDPR (article 4(7)) as the agency (including "natural or legal person") that "determines the purposes and means of the processing of personal data."

22 *GDPR*, *supra* note 2, art 24.

23 *Ibid*, art 28.

24 *Ibid*, art 25.

Novel to the GDPR is the data controller's accountability for fully automated decision making when working with personal data. Not only must the data controller be able to provide clear and "meaningful information about the logic involved,"[25] but an individual also has the right to object to such decisions when undertaken without human oversight or intervention.[26] This is indeed a contested area that begs all the questions around algorithmic opacity and the *ex post* explanations that may need to be used in dealing with algorithmic agency. Nonetheless, it introduces a whole new dimension of responsibility on the part of the data controller, providing the individual or "subject" with the right to object to this type of use of their data. Later developed more comprehensively in the EU Artificial Intelligence Act,[27] this provision has been a seminal development in digital law.

Sanctions

Finally, the GDPR stipulates heavy fines for non-compliance. Each country's supervisory authority has some flexibility in administering such fines. They may consider the scope and "gravity" of the infractions;[28] the intent with which wrongful processing was, or was not, undertaken;[29] and factors such as whether there is repeat behaviour.[30] However, for those who do not adhere to the overarching principles embedded in the legislation (namely, to be lawful, fair and transparent),[31] disregard the subject's rights[32] or who do not comply with an "order" by the relevant supervisory authority,[33] maximum fines may be levied. As article 83(5) lays out, these may be up to "20 000 000 EUR, or…up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher."[34] Equally critical, there are mechanisms for redress for individuals whose privacy has been violated, including the individual's right to compensation.[35]

In sum, if accountability rides not just on explanation to the subject or relevant party in question, but also on consequences when obligations are not fulfilled, the GDPR is extremely explicit on these matters. Sanctions here have mechanisms for enforcement and have real — and substantial — financial implications for both controllers and processors. Moreover, the GDPR is particularly robust legislation — its applications range from embedding regulatory governance with fundamental human rights to groundbreaking provisions regarding an individual's right to transparency and explanation.

25 *Ibid*, art 13(2)(f).

26 *Ibid*, art 22.

27 EC, *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)*, online: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>.

28 *GDPR*, *supra* note 2, art 83(2)(a).

29 *Ibid*, art 83(2)(b).

30 *Ibid*, art 83(2).

31 *Ibid*, art 83(5)(a).

32 *Ibid*, art 83(5)(b).

33 *Ibid*, art 83(6).

34 *Ibid*, art 83(5).

35 *Ibid*, arts 78, 79, 82.

Korea

In Korea, the seminal legislation involving privacy regulation (PIPA) has been in place since March 29, 2011 — certainly long enough to see any potential impacts on innovation indicators. Like the GDPR, the legislation is quite extensive and, together with accompanying laws dealing with information protection, has been characterized as "essentially rival[ling] those of Europe" (Choe, Son and Kim 2017, 1). There are key differences, but, in large part, PIPA asserts the rights of the individual, places the burden of responsibility on the data-processing controller, and has rigorous accountability and enforcement mechanisms in place. Notably, much of this was established well before the GDPR.

Governance and Privacy Protection

PIPA lays out the purpose of the legislation as "protect[ing] the freedom and rights of individuals."[36] But one critical difference from the GDPR hinges on the constitutionality of the right to privacy. Whereas the European Constitution unequivocally states that right, the Constitution of the Republic of Korea does not include such a provision. Nevertheless, in two critical cases (in 2005 and in 2015), the country's Constitutional Court declared that privacy rights may be "derived" (Ko et al. 2017, 107) from the right to a private life and to dignity and happiness, which are embedded in the constitution. Consequently, the court has determined that "personal information self-determination"[37] (ibid.) exists as a constitutional right and that the collection and use of personal information need to respect those boundaries.

There are other distinctions as well. Legal scholars have argued that the right to consent in the Korean case (unlike the GDPR) takes precedence over other interests (Park, Chae and Chang 2017). It is only when the interests of the controller are "manifestly superior"[38] to those of the subject that processing (without consent) may occur. While this is a more stringent requirement, since amendments of 2020, the meaning of consent in PIPA has also been loosened somewhat. Controllers may use data without the subject's agreement when it is "reasonably related to the initial purpose of the collection."[39]

Despite such differences, the GDPR and PIPA are very similar. The onus is on the personal information controller to handle citizens' data "lawfully and fairly," based on the principle of minimization.[40] Information is to be "accurate," timely and secured through systems that protect the individual's privacy.[41] So, too, are protections for the data subject well specified. The right to consent, to have access to the information being used, and to ensure corrections or, indeed, destroy the data, as needed: all are spelled out in the legislation.[42] As for the right to be forgotten present in the GDPR, this does not exist in PIPA. Nevertheless,

36 *PIPA*, *supra* note 3, art 1.

37 This is a direct quote from the court.

38 *PIPA*, *supra* note 3, art 15(1)(6).

39 *Ibid*, art 15(3).

40 *Ibid*, arts 3(1), 3(6).

41 *Ibid*, arts 3(3), 3(4).

42 *Ibid*, art 4.

there is provision for the individual's right to request destruction of personal data.[43] Thus, there is a kind of "default" mechanism that provides safeguards to citizen (Erdos and Garstka 2020, 294).

Accountability

Accountability provisions, while not fully equivalent to the GDPR, are not dissimilar. Most critically, the burden of proof for responsible data processing — and acquisition of consent by the data controller — are not placed upon the citizen or data subject but rather on the controller. For circumstances in which the data controller proceeds without consent, the controller must be able to demonstrate that such exceptional circumstances can be justified.[44] Equally, the data controller is responsible for establishing and maintaining control systems that ensure security of the data.[45] As for delegation of processing, the act is quite specific around the conditions of that "entrustment," including ensuring security of the data not beyond the intended purpose, clear notification of the arrangement to the data subject and supervision of the third party, as required.[46] Nor does this arrangement obviate the data controller from responsibility when there is a breach of security. In these circumstances, the entrusted or third party is deemed to be "an employee" of the data controller and, akin to the GDPR, comes within their purview. PIPA does not, however, specifically call for internal control systems for data protection to be built systematically from beginning to end with those protections as primal (i.e., "by design and default").

As for the important issue of automated processing, the act (as of 2023) now covers this dimension as well. Data subjects have the right not only to an "explanation" of automated decisions but also the right to refuse such a decision.[47]

Sanctions

For non-compliance, the "penalty provisions" in PIPA are explicit — and extensive.[48] In the case of personal information controllers who collect or use personal data or share it with a third party without the data subject's consent, they may be subject to fines of up to three percent of their total sales, with a hard cap of two billion won.[49] In contrast with the GDPR, criminal punishment can also be imposed, both for processors and for individual "persons" engaged in unlawful activities. Disruption of the workings of a public agency or collection of personal information through fraudulent means can garner up to 10 years in prison or a maximum fine of 100 million won.[50] Misuse of personal data that violates the consent of the data subject, including by third parties, can result in up to five years of imprisonment or a maximum fine of 50 million won.[51] Less egregious offences, such as processing of incorrect personal data, carry lesser

43 *Ibid*, art 4(4).

44 *Ibid*, art 22(3).

45 *Ibid*, c IV.

46 *Ibid*, art 26.

47 *Ibid*, art 4(6).

48 *Ibid*, c X.

49 *Ibid*, art 64(2).

50 *Ibid*, art 70.

51 *Ibid*, art 71.

penalties but still can involve fines of 20 million won or two years of imprisonment.[52] As with the GDPR, there are remedies available to the individual citizen.

Responsibility for the legislation is under the auspices of the Personal Information Protection Commission (PIPC), including enforcement authority regarding administrative fines[53] as well as guidelines for data processors that protect and secure privacy rights.[54] Previously, its authority had been more fractured, with enforcement split among different agencies (Ko et al. 2017; Lee & Ko 2020). With the 2020 amendments, the commission's authorities have been consolidated, although criminal activities do stand beyond its jurisdiction, with such matters referred to prosecutorial authorities or the police. Since 2020, there have also been several high-profile cases in which heavy fines were administered, including the case of an AI chatbot (Paulger 2022).

Canada

PIPEDA received royal assent in 2000. Despite its now dated nature, given the fact that the proposed Digital Charter[55] has been terminated with the prorogation of Parliament, it continues to stand as a key bulwark against breaches of privacy regarding use of personal data. The legislation has been overtaken by technological developments, particularly in the realm of AI.[56] Yet, even aside from the transformative changes swept in through a new digital age, the statute is rather modest in nature, both in its aspirations as well as the insulation it provides for individual privacy. Relative to the protections and rigour of the GDPR or of the Korean statute, it stands in sharp contrast.

PIPEDA does seek to protect "personal information that is collected, used or disclosed" in the pursuit of "electronic commerce," but therein lies the challenge.[57] While under the Constitution Act of 1867, section 92 assigns "Property and Civil Rights"[58] to provincial jurisdiction, "Regulation of Trade and Commerce"[59] falls within federal authority, with PIPEDA duly positioning its justification under those auspices. As such, the act specifically applies to organizations using personal data in their commerce, as well as to employees who fall within federal works. The jurisdictional authority has been challenged (by Quebec in 2003), but the Supreme Court has not resolved this issue.[60] While these earlier debates

52 *Ibid*, art 73.

53 *Ibid*, arts 7-8, 7-9.

54 Where lesser offences or concerns are involved, the PIPC may first determine to proceed with recommendations or "corrective orders" rather than escalating to the level of criminal sanctions. See www.dlapiperdataprotection.com/index.html?t=enforcement&c=KR.

55 *Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts*, 1st Sess, 44th Parl, 2022 (second reading 24 April 2023), online: <www.parl.ca/legisinfo/en/bill/44-1/c-27>. Parliament was prorogued January 6, 2025.

56 See Bolca (2020); Office of the Privacy Commissioner of Canada (OPC) (2020); Cofone (2020).

57 *PIPEDA*, *supra* note 4.

58 *Constitution Act, 1867* (UK), 30 & 31 Vict, c VI, s 92, 13, reprinted in RSC 1985, Appendix II.

59 *Ibid*, c VI, s 91(2).

60 On the quasi-constitutional status of PIPEDA, see the critical article by former Justice of the Supreme Court of Canada, Michel Bastarache (2012); also, Bolca (2020); Cofone (2020); House of Commons, *Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act* (February 2018) (Chair: Bob Zimmer) [*Towards Privacy by Design*], online: <www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9690701/ethirp12/ethirp12-e.pdf>; Jamal (2006); Nisker (2007); Scassa (2012, 2020, 2022).

have now ceased to resonate as loudly,[61] the legislation itself continues to rest in the more ambiguous territory of "quasi-constitutional" status.[62]

Governance and Privacy Protection

Given such constitutional complexity, the protection of human rights, including the right to privacy, is not unequivocally embedded in the legislation. The act does not link back to Charter rights as does the GDPR, nor to the unequivocal nature of this "self-determination" as decided through Korean jurisprudence. Rather, it "recognizes the right of privacy"[63] and brackets the use of personal data with two important caveats. Article 3 states that "the purpose of this Part is to establish…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*."[64]

This language is problematic on two fronts. With respect to the notion around reasonableness, the provision is quite broad and subject to much interpretation. Equally important, the protection of personal data is essentially subject to the "negotiat[ion]" or trade-offs involved with a business conducting commerce (Scassa 2020, 180). At minimum, it constitutes a balancing act between the individual's rights and the requisites of an organization's business model. The Standing Committee on Access to Information, Privacy and Ethics, the OPC and legal scholarship[65] have all critiqued PIPEDA — not just for the need to modernize but also, in terms of fundamentals, for being "narrowly" bounded (OPC 2019a, 11). As the OPC has observed, in speaking both to PIPEDA and the Privacy Act,[66] "neither law formally recognizes privacy as a right in and of itself" (ibid).

As well, the issue of meaningful and informed consent within PIPEDA is much more modestly positioned, not existing as "rights of the data subject" as within the GDPR.[67] Article 6(1) of PIPEDA invokes valid consent in terms of whether "it is reasonable" that the individual involved would "understand the nature, purpose and consequences of the [data] collection," rather than the more direct and specific language of the EU legislation.[68] True, the principles attached in schedule 1 of PIPEDA do speak to data collection and consent, but, even here, the burden on the organization is to "make a reasonable effort"[69] to ensure the data subject is properly informed before seeking consent. Schedule 1 also raises other concerns that diminish the effectiveness of the legislation. It has been argued that as schedule 1 is not located in the body of the law, its import is lessened in terms of judicial interpretation.[70] As for the "right to be forgotten," this does not exist within the current legislation.[71] All this to say, on these critical matters relating to rights and exercise of those

61 See Bolca's (2020, 87) comment that the "criticisms of PIPEDA's constitutionality have been subdued."

62 On this, see OPC (2019a, 11); see also the joint resolution by Canada's information and privacy commissioners (OPC 2019b) and Cofone (2020, fn 11).

63 *PIPEDA*, *supra* note 4, art 3.

64 *Ibid* [author's emphasis].

65 See, respectively, for the House of Commons, *Towards Privacy by Design*, *supra* note 60; for the OPC (2019a); and for legal scholarship, Bolca (2020), Cofone (2020) and Scassa (2020).

66 *Privacy Act*, RSC 1985, c P-21.

67 *GDPR*, *supra* note 2, c 3.

68 *PIPEDA*, *supra* note 4, art 6(1).

69 *Ibid*, schedule 1, principle 4(3)(2).

70 On schedule 1, see Cofone (2020) and OPC (2019a); although in the latter case, the argument is made in reference to rights.

71 See Rosenstock (2016, 133), who does argue, however, that the legislation "could support" this.

rights by the individual, the spirit, intent and language of PIPEDA are considerably weaker in contrast with the GDPR as well as with PIPA.

Accountability

With respect to accountability provisions, PIPEDA, with few exceptions, does not measure up to the standards set by the European Directive. Principle 4(1) in PIPEDA does speak to the issue, indicating that the organization that holds such personal data "is responsible for personal information under its control" and must name those accountable for "compliance."[72] This responsibility and a "comparable level of protection" also apply to processing undertaken by a third party.[73] And there must be "policies" and processes that can ensure privacy protection and obligations under the act.[74] However, there is no clause that the processes must provide guarantees as in the GDPR,[75] nor that the organization must be able to demonstrate compliance. Nor is there any requirement for data-processing systems to be developed with a built-in capacity to protect the individual's privacy that applies throughout the life cycle of processing, namely, "by design and by default."[76]

With respect to the Korean legislation, the Canadian standards around accountability are also different. PIPA specifically embeds the "duty of safeguards"[77] within the text of the legislation. In the Canadian case, accountability of the data processor to protect personal information rests not in the body of the act but within the schedule 1 principles, which carry lesser legal import.

As for AI, the early inception of PIPEDA precluded legislators from having to wrestle with the thorny issues around AI that now present themselves. Consequently, there are no provisions in the legislation regarding automated or, indeed, semi-automated decision making.

Sanctions

On the issue of sanctions, if it indeed may be called that in the Canadian case, PIPEDA stands in sharp contrast to both the GDPR and the Korean legislation. PIPEDA functions on an ombudsman model, with the OPC being the appropriate authority.[78] As such, this model does not equip the OPC with powers to enforce compliance with the act. If an individual registers a complaint, the OPC may investigate, calling witnesses and gathering evidence. It may also enter into negotiations with the organization involved and seek to attain compliance. But should no agreement be reached, and the data processor does not wish to comply, the OPC has no authority for "binding orders."[79] Nor can fines be levied. The aggrieved individuals may, at that time, proceed

72 *PIPEDA*, *supra* note 4, principle 4(1).

73 *Ibid*, art 4(1)(3).

74 *Ibid*, art 4(1)(4).

75 *GDPR*, *supra* note 2, art 5.2.

76 *Ibid*, art 25. These concerns have been of particular import to the OPC and parliamentarians studying these matters, with the OPC specifically putting proposals on the books to amend the act. See OPC (2013; 2019a; 2020).

77 *PIPA*, *supra* note 3, c IV; see especially art 29.

78 On the issue of PIPEDA, enforcement and remedies available, see in particular Bolca (2020); Cofone (2020); *Towards Privacy by Design*, *supra* note 60; OPC (2013); see also Austin (2006); Macnab (2021).

79 See *PIPEDA*, *supra* note 4, arts 12, 13, 17, for the relevant clauses; Cofone (2020, s 2.d).

to seek a remedy in the courts, and the OPC also has the option to proceed in seeking jurisprudence.[80] But the OPC has no capacity to force or order the offending organization into compliance. This has, of course, been a long-standing concern of the OPC, going back at least to 2013.[81] Observers have also noted that the courts, in this case, are not an effective means for compliance.

Innovation Indicators

Given the respective differences between the more stringent GDPR and PIPA and the more modest provisions of PIPEDA, one might well expect to find impacts that bleed into innovation indicators. Yet a comparison of Sweden, Korea and Canada on information and communications technology (ICT) patent applications to the World Intellectual Property Organization (WIPO) does not show particularly strong evidence of such differential implications (see Figure 1). It is Korea (not Canada) that shows the most robust performance, garnering an increase in patents of 854 percent over the time series. In fact, as of 2020, Korea's standing on this measure was *seven times* that of Canada. The comparison with Sweden does display more mixed results, with Korea's performance 4.9 times that of Sweden.

However, when it comes to the Swedish/Canadian comparison, the trend lines again run opposite to expectations. In the case of Sweden, there has been an increase of 53 percent over the full time series, with Canada, in fact, coming in just under this number at 49 percent. Further, in 2020, it is Sweden's performance on ICT patent applications that was 1.4 times that of Canada. There is a relatively modest deceleration in Sweden's patents, which started after 2017 (the year before the GDPR was introduced) and continues, but with an uptick in 2019. But on balance, given the much weaker legislative standards in the Canadian case, as well as the stability of that legislation over decades, this more liberal context has not generated a particularly strong performance for Canada. Indeed, this may well be more suggestive of the lack of a vigorous ICT ecosystem that could sustain a higher level — and growth — in patents. Interestingly, although not directly applicable, statistics from the European Patent Office on total patents for Sweden, which extend to 2021, do show a modest upswing.[82]

The VC investments in AI borne out in the author's previously published DPH working paper (Scharf 2025) also attest to thriving Korean and Swedish innovation. Figure 2 reproduces the earlier data. While all countries had experienced a drop in VC investments by 2023 from earlier highs, these dips left Korea standing at US$2.2 billion and Sweden at US$2.0 billion — both significantly above Canada at US$1.85 billion. Most remarkable in this data, however, is Sweden's vaunt in investment from 2020 to 2022 — well after the introduction of the GDPR and occurring during COVID-19 pandemic years. It is also notable that a more liberal environment regarding privacy protections has not insulated Canada from a significant decrease in AI VC after earlier gains.

80 *PIPEDA*, *supra* note 4, arts 14(1), 17(2).

81 *Towards Privacy by Design*, *supra* note 60 at 52–56; OPC (2013; 2018).

82 See https://data-explorer.oecd.org/vis?df[ds]=DisseminateFinalDMZ&df[id]=DSD_PATENTS%40DF_PATENTS&df[ag]=OECD.STI.PIE&dq=6F0.A.AP.PATN.PRIORITY...INVENTOR..._T&pd=2000%2C2021&to[TIME_PERIOD]=false&vw=tb.

Interestingly, as this paper goes to print, all three countries have experienced declines in AI VC for 2024, with Sweden holding slightly stronger on this measure than Canada or Korea.[83] Clearly, simple assumptions between strengthened privacy legislation and a chilling effect on the most disruptive and innovative technologies found in AI must be questioned. Clearly, other factors are influencing the VC performance and, in this case, the AI ecosystems.

In the case of patents, the data is constrained by the limited time series, stopping in 2020, and later indicators might well show different trajectories. There is also a lagged effect on investment and research and development, which legislation may be causing, that would not yet be demonstrable. However, based on the evidence available, both for patents and for VC, the argument that more stringent regulatory standards have — and will — necessarily hamper innovation is not definitively borne out. As for the indicator relating to digital competitiveness, here, too, the potentially negative impacts associated with innovation are not manifest. The 2024 World Digital Competitiveness Ranking places Sweden and Korea well above Canada, at fifth and sixth, respectively, with Canada coming in quite far below at thirteenth (IMD 2024).

Conclusion

In addressing the question of the relationship between digital regulation and innovation, several dimensions need to be highlighted. The GDPR, on one hand, is an exceedingly rigorous piece of legislation, premised on the protection of human rights and tight regulations regarding the use and collection of personal data. PIPA, while not directly equivalent, is similarly robust. PIPEDA, on the other hand, given its age, rather contorted constitutional design and an ombudsman model predicated on obligations rather than rights, does not compare with the same rigour.

That said, what are not seen are highly distinguishable results on the innovation front. The evidence is by no means unequivocal, but it does make for some compelling conclusions. Despite a very liberally constructed legislation in the Canadian context that has lasted over the better part of two decades, this regulation has not unleashed digital innovation and growth.

All of this speaks to the complex and dynamic nature of innovation. The robustness of national innovation ecosystems, their degree of internal integration, and public policies that can provide consistent priority setting and enable that dynamism: these all factor into innovation potential. In this context, the choice between regulation and innovation is not only “false” but also misplaced. The stringency or dearth of digital regulation cannot be the singular means by which to engage in the highly competitive and globally contested race for innovation, productivity and growth. For Canada, regulatory modernization and protection of privacy rights in this new digital age are long overdue, and it should not be viewed as an impediment to engendering prosperity. Nor should it be cast as a bulwark against facing down the country’s historical challenges with innovation.

83 See OECD.AI (https://oecd.ai/en/data?selectedArea=investments-in-ai-and-data&selectedVisualization=vc-investments-in-ai-by-country, data from Preqin, last updated February 18, 2025, accessed on May 14, 2025).

Recommendations

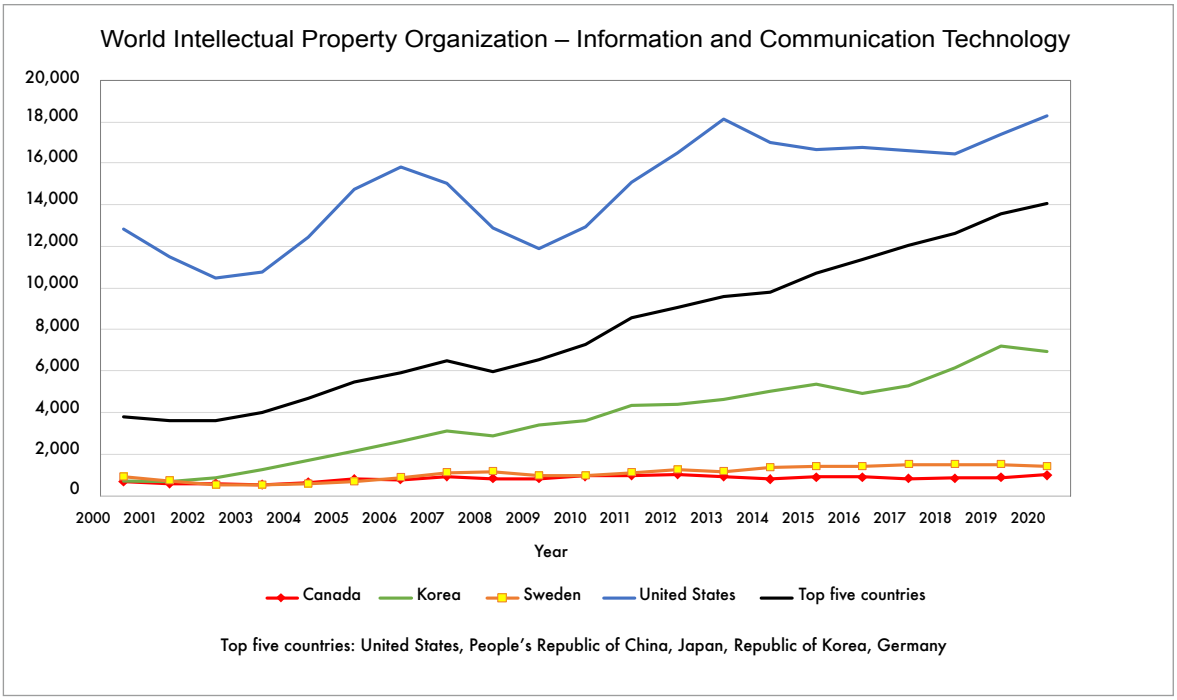
- Canada continues to struggle with digitalization and creating innovation in a robust ICT ecosystem. Governing digital legislation in the Canadian case should not be viewed as a critical element contributing to this.
- PIPEDA is very much in need of modernization — on many fronts. The GDPR and PIPA offer important models for protection of privacy rights and secure processing of data.
- Embedding of privacy rights, vigorous accountability systems and sanctions for non-compliance are key elements that should inform any new Canadian legislation regarding data protection.

Acknowledgements

I would like to extend my sincere appreciation to my academic supervisors, Patrick Leblond and David Wolfe, for their invaluable guidance and engagement on this work. I also wish to thank Daniel Araya for his critical insights on policy and digital regulation. My sincere thanks go out as well to my Digital Policy Hub peers, Jamie Duncan, Matthew da Mota and Michael Murphy, as well as to the Digital Policy Hub team.

Figure 1: ICT Patent Applications to WIPO

Dataset: Patents by Technology	
Patent authorities	World Intellectual Property Organization – Information and Communication Technology – ICT
Measure	Patent applications
Reference date	Priority date
Agent role	Inventor
Selected OECD policy domain	ICT

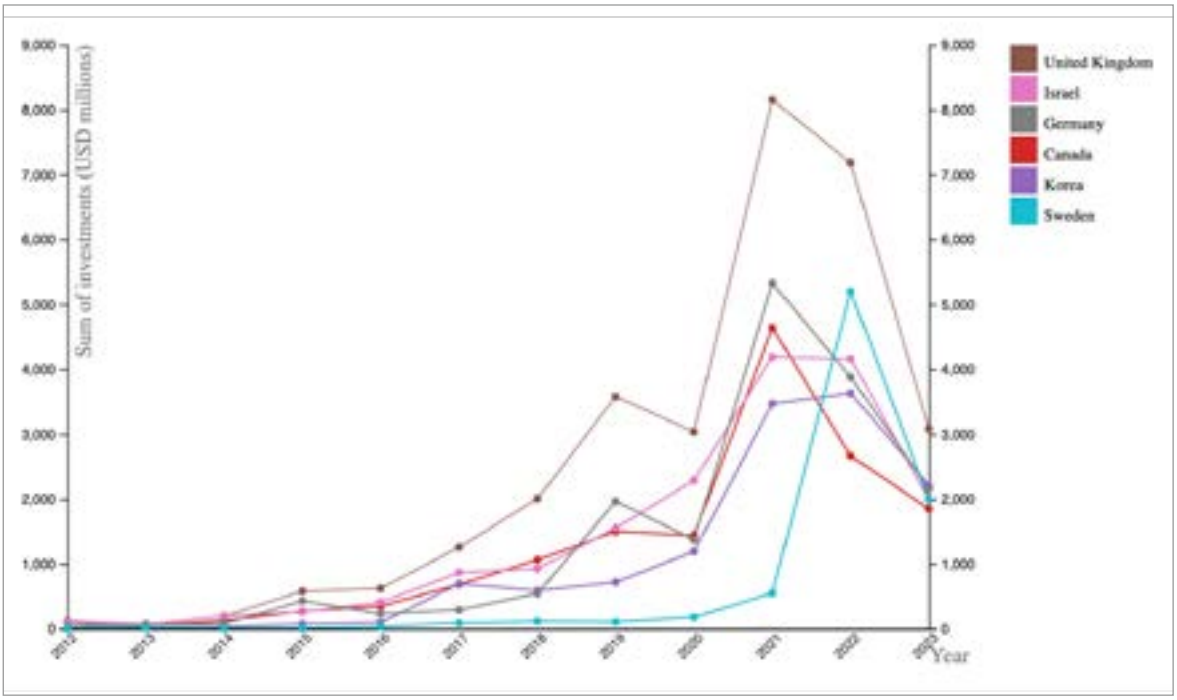


Data source: OECD, https://data-explorer.oecd.org/vis?df[ds]=DisseminateFinalDMZ&df[id]=DSD_PATENTS%40DF_PATENTS&df[ag]=OECD.STI.PIE&dq=9P50_1.A.AP.PATN.PRIORITY...INVENTOR...ICT&pd=2000%2C2021&to[TIME_PERIOD]=false&vw=tb.
Data accessed on November 11, 2024.

About the Author

Shirley Anne Scharf is a former Digital Policy Hub postdoctoral fellow at the Centre for International Governance Innovation in Waterloo, Ontario. She is also a visiting researcher with the CN-Paul M. Tellier Chair on Business and Public Policy at the University of Ottawa, as well as a post-doctoral fellow with the Innovation Policy Lab, Munk School of Global Affairs and Public Policy, University of Toronto. Shirley Anne has a Ph.D. in public administration from the University of Ottawa, where her dissertation was titled "Canadian Innovation Policy: The Continuing Challenge" (2022). Her current research focuses on innovation policy from two innovation leaders — the Republic of Korea and Sweden — and the comparative lessons Canada may learn from these countries. Other research interests include industrial policy, governance and technological change.

Figure 2: VC Investments in AI by Country (by Year)



Data source: OECD, https://oecd.ai/en/data?selectedArea=investments-in-ai-and-data&selectedVisualization=vc-investments-in-ai-by-country. Data accessed on July 21, 2024.

Acronyms and Abbreviations

AI	artificial intelligence
GDPR	General Data Protection Regulation
ICT	information and communications technology
OECD	Organisation for Economic Co-operation and Development
OPC	Office of the Privacy Commissioner of Canada
PIPA	Personal Information Protection Act
PIPC	Personal Information Protection Commission
PIPEDA	Personal Information Protection and Electronic Documents Act
VC	venture capital
WIPO	World Intellectual Property Organization

Works Cited

Aghion, Philippe, Antonin Bergeaud and John Van Reenen. 2021. “The Impact of Regulation on Innovation.” National Bureau of Economic Research Working Paper Series, Working Paper 28381. January. Cambridge, MA: National Bureau of Economic Research. www. nber. org/system/files/working_papers/w28381/w28381.pdf.

– – –. 2023. “The Impact of Regulation on Innovation.” *American Economic Review* 113 (11): 2894–936. www.aeaweb.org/articles?id=10.1257/aer.20210107.

Aghion, Philippe, Nick Bloom, Richard Blundell, Rachel Griffith and Peter Howitt. 2005. “Competition and Innovation: an Inverted-U Relationship.” *Quarterly Journal of Economics* 120 (2): 701–28. https://doi.org/10.1093/qje/120.2.701.

Amable, Bruno, Lilas Demmou and Ivan Ledezma. 2009. “Product market regulation, innovation, and distance to frontier.” *Industrial and Corporate Change* 19 (1): 117–59. https://doi.org/10.1093/icc/dtp037.

Arrow, Kenneth J. 1962. “Economic Welfare and the Allocation of Resources for Invention.” In *The Rate and Direction of Inventive Activity: Economic and Social Factors*, edited by H. M. Groves, 609–26. Princeton, NJ: Princeton University Press.

Austin, Lisa M. 2006. “Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices.” *Canadian Business Law Journal* 44: 21–53. https://ssrn.com/abstract=1169162.

Bastarache, Michel. 2012. “The Constitutionality of PIPEDA: A Re-consideration in the Wake of the Supreme Court of Canada’s *Reference re Securities Act*.” June. Montreal, QC: Heenan Blaikie LLP. https://barrysookman.com/wp-content/uploads/2021/03/SCC-39396_COMPUFINDER_REPLY-RECORD_SUITABLE-FOR-POSTING.pdf.

Bayamlıoğlu, Emre. 2022. “The right to contest automated decisions under the General Data Protection Regulation: Beyond the so-called ‘right to explanation.’” *Regulation & Governance* 16 (4): 1058–78. https://doi.org/10.1111/rego.12391.

Blind, Knut, Sören S. Petersen and Cesare A. F. Rillo. 2017. “The impact of standards and regulation on innovation in uncertain markets.” *Research Policy* 46 (1): 249–64. https://doi.org/10.1016/j.respol.2016.11.003.

Bolca, Tunca. 2020. “Can PIPEDA ‘Face’ the Challenge? An Analysis of the Adequacy of Canada’s Private Sector Privacy Legislation against Facial Recognition Technology.” *Canadian Journal of Law and Technology* 18 (1): 51–90. https://digitalcommons.schulichlaw.dal.ca/cgi/viewcontent.cgi?article=1262&context=cjlt.

Bradford, Anu. 2023. *Digital Empires: The Global Battle to Regulate Technology*. New York, NY: Oxford University Press.

– – –. 2024. “The False Choice Between Digital Regulation and Innovation.” *Northwestern University Law Review* 119 (2): 377–452. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4753107.

Broughel, James and Robert W. Hahn. 2022. “The impact of economic regulation on growth: Survey and synthesis.” *Regulation & Governance* 16 (2): 448–69. https://onlinelibrary.wiley.com/doi/abs/10.1111/rego.12376.

Chen, Chinchih, Carl Benedikt Frey and Giorgio Presidente. 2022. “Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally.” Oxford Martin Working Paper Series on Technological and Economic Change, Working Paper No. 2022-1. www.oxfordmartin.ox.ac.uk/publications/privacy-regulation-and-firm-performance-estimating-the-gdpr-effect-globally.

Choe, Jeong Yeol, Doil Son and Sejin Kim. 2017. “The Limitations on the Use of Big Data Pursuant to Data Privacy Regulations in Korea.” *Journal of Korean Law* 17 (1): 1–32. https://s-space.snu.ac.kr/handle/10371/168345.

Cofone, Ignacio. 2020. *Policy Proposals for PIPEDA Reform to Address Artificial Intelligence*. Report. November. Gatineau, QC: OPC. www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pol-ai_202011/.

Dahi, Alan and Marcelo Corrales Compagnucci. 2022. “Device manufacturers as controllers – Expanding the concept of ‘controllership’ in the GDPR.” *Computer Law & Security Review* 47: 1–18. https://doi.org/10.1016/j.clsr.2022.105762.

Erdos, David and Krzysztof Garstka. 2020. “The ‘right to be forgotten’ online within G20 statutory data protection frameworks.” *International Data Privacy Law* 10 (4): 294–313. https://doi.org/10.1093/idpl/ipaa012.

Hoofnagle, Chris Jay, Bart van der Sloot and Frederik Zuiderveen Borgesius. 2019. “The European Union general data protection regulation: what it is and what it means.” *Information & Communications Technology Law* 28 (1): 65–98. https://doi.org/10.1080/13600834.2019.1573501.

IMD. 2024. *IMD World Digital Competitiveness Ranking 2024. The digital divide: risks and opportunities*. November. Lausanne, Switzerland: IMD. https://imd.widen.net/s/xvhldkrrkw/20241111-wcc-digital-report-2024-wip.

Jamal, Mahmud. 2006. “Is PIPEDA Constitutional?” *Canadian Business Law Journal* 43 (3): 434–54. https://heinonline.org/HOL/LandingPage?handle=hein.journals/canadbus43&div=31&id=&page=.

Johnson, Garrett A. 2023. “Economic Research on Privacy Regulation: Lessons from the GDPR and Beyond.” In *The Economics of Privacy*, edited by Avi Goldfarb and Catherine E. Tucker. Chicago, IL: University of Chicago Press. https://dx.doi.org/10.2139/ssrn.4290849.

Ko, Haksoo, John M. Leitner, Eunsoo Kim and Jong-Gu Jung. 2017. “Structure and enforcement of data privacy law in South Korea.” *International Data Privacy Law* 7 (2): 100–14. https://academic.oup.com/idpl/article-abstract/7/2/100/3749605?redirectedFrom=PDF.

Kuner, Christopher, Lee A. Bygrave and Christopher Docksey. 2020. “Background and Evolution of the EU General Data Protection Regulation (GDPR).” In *The EU General Data Protection Regulation (GDPR): A Commentary*, edited by Christopher Kuner, Lee A. Bygrave, Christopher Docksey and Laura Drechsler, 1–47. New York, NY: Oxford Academic. https://doi.org/10.1093/oso/9780198826491.003.0001.

Lee & Ko. 2020. “Major Amendment to the Personal Information Protection Act Passed by National Assembly.” Legal 500, January 15. www.legal500.com/developments/thought-leadership/major-amendment-to-the-personal-information-protection-act-passed-by-national-assembly/.

Macnab, Aidan. 2021. “Federal Court decision a step towards determining whether Canada will have a right to be forgotten.” *Canadian Lawyer*, July 21. www.canadianlawyermag.com/practice-areas/privacy-and-data/federal-court-decision-a-step-towards-determining-whether-canada-will-have-a-right-to-be-forgotten/358306.

Mondschein, Christopher F. and Cosimo Monda. 2019. “The EU’s General Data Protection Regulation (GDPR) in a Research Context.” In *Fundamentals of Clinical Data Science*, edited by Pieter Kubben, Michel Dumontier and Andre Dekker, 55–71. Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-319-99713-1_5.

Nisker, Josh. 2007. “PIPEDA: A Constitutional Analysis.” *The Canadian Bar Review* 85 (2): 317–43. https://cbr.cba.org/index.php/cbr/article/view/4053.

OECD. 2016. *OECD Reviews of Innovation Policy: Sweden 2016*. Paris, France: OECD Publishing. www.oecd.org/en/publications/oecd-reviews-of-innovation-policy-sweden-2016_9789264250000-en.html.

– – –. 2019. *Going Digital: Shaping Policies, Improving Lives*. Paris, France: OECD Publishing. www.oecd-ilibrary.org/science-and-technology/going-digital-shaping-policies-improving-lives_9789264312012-en.

– – –. 2023. *OECD Reviews of Innovation Policy: Korea 2023*. Paris, France: OECD Publishing. www.oecd.org/en/publications/2023/07/oecd-reviews-of-innovation-policy-korea-2023_6517d469.html.

OPC. 2013. "The Case for Reforming the *Personal Information Protection and Electronic Documents Act*." May. www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_r/pipeda_r_201305/.

– – –. 2018. *Trust but verify: Rebuilding trust in the digital economy through effective, independent oversight*. 2017–18 Annual Report to Parliament on the *Personal Information Protection and Electronic Documents Act* and the *Privacy Act*. Gatineau, QC: OPC. www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201718/ar_201718/.

– – –. 2019a. *Privacy Law Reform: A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy*. 2018–2019 Annual Report to Parliament on the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*. Gatineau, QC: OPC. www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201819/ar_201819/.

– – –. 2019b. "Effective privacy and access to information legislation in a data driven society." Resolution of the Federal, Provincial and Territorial Information and Privacy Commissioners, Charlottetown, PEI, October 1–2. www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_191001/.

– – –. 2020. "A Regulatory Framework for AI: Recommendations for PIPEDA Reform." November. www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/reg-fw_202011/.

Park, Kwang Bae, Sunghee Chae and Jaeyoung Chang. 2017. "Main Issues in Korea Regarding Consent for the Processing of Personal Information, with Emphasis on Recent Supreme Court Cases." *Journal of Korean Law* 17: 53–77.

Paulger, Dominic. 2022. *South Korea: Status of Consent for Processing Personal Data*. ABLI-FPF Convergence Series. June. Asian Business Law Institute and Future of Privacy Forum. https://fpf.org/wp-content/uploads/2022/06/ABLI-FPF-Consent-Project-South-Korea-Jurisdiction-Report.pdf.

Porcher, Simon. 2013. "Regulation and ICT capital input: empirical evidence from 10 OECD countries." In *Governance, Regulation and Innovation: Theory and Evidence from Firms and Nations*, edited by Mehmet Ugur, 182–96. Cheltenham, UK: Edward Elgar.

Rosenstock, Michael. 2016. "Is There a 'Right to be Forgotten' in Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)?" *Canadian Journal of Law and Technology* 14 (1): 131–55. https://digitalcommons.schulichlaw.dal.ca/cjlt/vol14/iss1/6/.

Scassa, Teresa. 2012. "Fresh Questions about the Constitutionality of PIPEDA?" *Teresa Scassa* (blog), January 17. www.teresascassa.ca/index.php?option=com_k2&view=item&id=96:fresh-questions-about-the-constitutionality-of-pipeda?&Itemid=80.

– – –. 2020. “A Human Rights-Based Approach to Data Protection in Canada.” In *Citizenship in a Connected Canada: A Research and Policy Agenda*, edited by Elizabeth Dubois and Florian Martin-Bariteau, 173–88. Ottawa, ON: University of Ottawa Press. www.uottawa.ca/research-innovation/centre-law-technology-society/connected-canada/book.

– – –. 2022. “Bill C-27 and a human rights-based approach to data protection.” *Teresa Scassa* (blog), August 2. www.teresascassa.ca/index.php?option=com_k2&view=item&id=361:bill-c-27-and-a-human-rights-based-approach-to-data-protection&Itemid=80.

Scharf, Shirley Anne. 2022. “Canadian Innovation Policy: The Continuing Challenge.” Ph.D. dissertation (unpublished), University of Ottawa. https://ruor.uottawa.ca/items/21c09975-d9df-4080-8eb0-0edfc9fe2113.

– – –. 2025. “Artificial Intelligence and Innovation Policy: A Comparative Perspective.” Digital Policy Hub Working Paper. Waterloo, ON: CIGI. www.cigionline.org/publications/artificial-intelligence-and-innovation-policy-a-comparative-perspective/.

– – –. Forthcoming 2025. “Innovation Policy and Venture Capital: Korea, Sweden and Canada.” Digital Policy Hub Working Paper. Waterloo, ON: CIGI.

Schumpeter, Joseph A. 1950. *Capitalism, Socialism, and Democracy*. 3rd ed. New York, NY: Harper & Row.

Ugur, Mehmet. 2013. “Governance, regulation and innovation: new perspectives and evidence.” In *Governance, Regulation and Innovation: Theory and Evidence from Firms and Nations*, edited by Mehmet Ugur, 1–24. Cheltenham, UK: Edward Elgar. https://doi.org/10.4337/9781782540663.00008.

Yeung, Karen and Lee A. Bygrave. 2022. “Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship.” *Regulation & Governance* 16 (1): 137–55. https://doi.org/10.1111/rego.12401.