Canadian Journal of Law and Technology

Volume 16 | Number 2 Article 3

1-1-2016

Legitimate Invasions: What Ontario can Learn from the History of the Consumer Reporting Act

Eliie Marshall
Faculty of Law, University of Toronto

Legitimate Invasions: Lessons from the History of Canadian Consumer Reporting Legislation

Ellie Marshall*

INTRODUCTION

The growth of modern surveillance has attracted great public and scholarly interest. As Justice Abella recently noted in *Douez v. Facebook*, the Internet has transformed the potential harms flowing from an unjustified invasion of one's personal information.[1] Most analyses of the associated risks, however, imply that the techniques and motivations for surveillance are new. In fact, tactics for collecting and exchanging information about individuals to gain power over those individuals are well documented since time immemorial.[2] From William the Conquerer's *Domesday Book* to IBM's first census tabulating machine, the advantage gained through data sharing has greatly benefited the state.[3] The history of surveillance, however, is not solely a history of government surveillance. The explosion of commercial and consumer credit, the "vital air of the system of commerce," in the 19th century transformed surveillance by perfecting the process of flattening an individual's identity into a monetizable reputation.[4] Collecting and exchanging personal information became the artillery of the private sector, a necessity for growth and market saturation. Today, we are deeply accustomed to having our identities tested and our personal stories collected in commercial settings, taking for granted the infrastructures that trade them, and their justifications for doing so. In our highly mediated, digital economy, there is often no alternative to these legitimate invasions.[5]

---

* J.D. University of Toronto, Faculty of Law; M.Sc. Social Science of the Internet, University of Oxford. The author wishes to thank Simon Stern for supervising the first draft of this article as a Directed Research project at the University of Toronto. The author would also like to thank the editors of the Canadian Journal of Law and Technology for their helpful feedback and input.

1 *Douez v. Facebook, Inc.*, 2017 SCC 33, 2017 CarswellBC 17663, 2017 CarswellBC 1664, [2017] 1 S.C.R. 751, 411 D.L.R. (4th) 434 (S.C.C.) [*Douez*].

2 Diane Rowland, Uta Kohl & Andrew Charlesworth, *Information Technology Law* (New York: Routledge, 2017) at 331.

3 *Ibid*, citing UK, HL, *Parliamentary Debates*, vol 549, col 37 (11 October 1993) (Earl Ferrers).

4 Josh Lauer, *Creditworthy: A History of Consumer Surveillance and Financial Identity in America* (New York: Columbia University Press, 2017) at 27, citing Senator David Webster, "The Continuance of the Bank Charter" in *The Writings and Speeches of David Webster* (Boston: Little, Brown, 1834).

5 *Douez, supra* note 1, at para 111, citing Cheryl B Preston, "'Please Note: You Have Waived Everything': Can Notice Redeem Online Contracts?" (2015) 64 Am U L Rev 535 at 554.

Many suggestions for protecting individuals from the harms posed by our "always-on" lifestyles focus on interventions from privacy law. However, the post-Internet-era fixation on privacy is problematic because without a clear definition of what privacy means, the discussion often becomes about "protecting privacy for privacy's sake."[6] A privacy-only approach is also a-historic. The interests protected under the umbrella term of privacy have historically been addressed through multiple legal schemes, such as regulating eavesdropping, trade, statistics, labour relations, and even psychiatry. One particularly overlooked area of law by those interested in the recent rise of "platform capitalism" is consumer protection.[7] Reviving an interest in consumer protection is essential, as it can help us understand a critical problem with modern surveillance where privacy law has failed: how to provide meaningful choice to individuals whose data is collected by commercial platforms and shared with third parties.[8]

To highlight the need for a renewed commitment to consumer protection, this paper traces the history of consumer reporting legislation in Ontario and connects the debates surrounding its enactment to current power imbalances and limitations in Canadian data protection laws. Although consumer reporting statutes are quite similar across Canada, Ontario is a helpful case study given the high concentration of both technology companies and people in the province.[9] This exercise is also helpful because there are few histories of consumer surveillance in Canada.[10] History, and legal history in particular, enables us to "excavate the past" to discover that there is nothing inherent or essential about

---

6 Edward Ryan, *Report on protection of privacy in Ontario* (Toronto: Ontario Law Reform Commission, 1968) at 6.

7 This paper adopts the definition of "platform capitalism" in Nick Srnicek, *Platform Capitalism* (Cambridge: Polity Press, 2017) at 6 ("The platform has emerged as a new business model, capable of extracting and controlling immense amounts of data, and with this shift we have seen the rise of large monopolistic firms. Today the capitalism of the high- and middle-income economies is increasingly dominated by [platforms]); See also Lauer, *supra* note 4 at 298: while the gravity of current events make it difficult to view contemporary surveillance in its broader historical context, inattention to historic modes of data protection is curious given the field's grounding in the works of Max Weber and Michel Foucault.

8 Frank Pasquale, "Reforming the Law of Reputation" (2016) 47 Loy U Chicago LJ 515 at 516.

9 See, e.g., "Ontario tech sector booms as Trudeau's innovation strategy starts taking shape," *Financial Post* (4 April 2017), online: < business.financialpost.com/technology/ontario-tech-sector-booms-as-trudeaus-innovation-strategy-starts-taking-shape > .

10 There is no academic publishing on the topic of consumer surveillance in Canada before computerization. For an excellent treatment of the impact of contemporary surveillance on Canadians, see Colin Bennett et al, eds, *Transparent Lives: Surveillance in Canada* (Edmonton: Athabasca University Press, 2014). The most recent academic treatment of Ontario's *Consumer Reporting Act* was written in 2009 and does not provide historical context. See Kent Glowinski, "Don't Get Enough Credit – The Need for an Impartial Consumer Credit Report Appeal Tribunal in Ontario" (2009) 22 J L & Soc Pol'y 5.

technology and that there are "legitimately different ways to think about things, including legal order."[11] Focusing only on recent and emerging strategies — algorithmic decision-making, the proliferation of sensors, blockchain — risks taking the current distribution of rights in society for granted. This is important because modern surveillance raises not only privacy problems, but other human rights concerns, such as sorting already marginalized populations by predictions of risk[12] and limiting public participation in decision-making processes.[13] Further, a consumer law approach to the challenges posed by modern data sharing practices allows us to see that the concepts underpinning privacy, such as the right to be left alone, are not only about controlling access to core biographical information. The principles underlying our human rights frameworks also support a right to not conform to a unitary mode of capitalism.[14] Strong consumer protection frameworks are needed (alongside privacy law) to recognize economic pluralism and to protect autonomy.

To explore this proposition, Part I outlines the rise of consumer reporting in North America and describes the legislative history of Ontario's *Consumer Reporting Act,*[15] which imported the imprecise "legitimate business need" standard to justify the commercialization of identity in the context of social anxiety over computerization in the 1960s. Part II discusses the current gap in Ontario created by the federal private-sector privacy regime and the lack of enforcement of provincial consumer protection law, using unregulated Canadian artificial intelligence companies that score potential tenants as an example. Part III applies lessons from this history to potential legal solutions to strengthen the *Consumer Reporting Act,* highlighting the multiplicity of opportunities for provincial legislatures to intervene and provide democratic legitimacy to the practice of platform capitalism. The paper concludes by emphasizing how privacy, consumer protection, and other areas of law must intersect and inform each other in the pursuit of stronger statutory protections of human rights in the twenty-first century.

---

[11] Jim Phillips, "Why Legal History Matters" (Lecture delivered at the Faculty of Law, Victoria University of Wellington, 24 June 2010), (2010) 41 VUWLR 293 at 309

[12] Danielle Keats Citron & Frank Pasquale, "The Scored Society: Due Process for Automated Predictions" (2014) 89:1 Wash L Rev 1.

[13] See, e.g., "Algorithmic Transparency: End Secret Profiling," *Electronic Privacy Information Centre,* online: <www.epic.org/algorithmic-transparency/>.

[14] Government of Canada, "Canada's approach to advancing human rights," online: <international.gc.ca/world-monde/issues_development-enjeux_developpement/human_rights-droits_homme/advancing_rights-promouvoir_droits.aspx?lang=eng> ("Pluralism and Diversity: Our policies are guided by the belief that economic prosperity, responsible governance and social well-being are all enhanced by efforts to build inclusive and pluralistic societies that respect diversity.").

[15] R.S.O. 1990, c. C 33 [*Consumer Reporting Act*].

I. HISTORY OF CONSUMER REPORTING LEGISLATION IN ONTARIO

Jim Phillips explains that legal history teaches us four things about the law: it is contingent on specific social contexts; it is capable of resisting dominant interests; there is nothing inevitable or preordained about our legal order; and there are many ways to think about law.[16] In the case of consumer surveillance, history allows us to understand how modern data protection laws connect rationally and logically to the social, economic, and technological forces which catalyzed the rise of consumer reporting.[17] This history, however, is comprised of many diverse problems, such as consumer discipline, the financialization of debt, and bankruptcy, which are outside the scope of this paper. Instead, the purpose here is to explain how the legal framework around the collection, use, and disclosure of data about individuals in the consumer context developed. What emerges from this history is an understanding that the enactors of consumer reporting legislation faced three specific challenges, all of which remain today: how to define the entities that collect, use, and disclose consumer data; what level of transparency these entities owe their data subjects; and what degree of privilege should be afforded to these commercial activities.[18]

A. Rise of Consumer Reporting in North America

19th Century

The history of compiling and selling access to the reputations and financial standings of Canadians is deeply intertwined with the American experience. Until the mid-19th century, credit evaluation was informal and personal.[19] A creditor could surveil his neighbours and lean on community opinion to determine to whom to grant credit, but separating out "honest" debtors was difficult. This issue was exposed in the financial crisis of 1837, when a "cascade of defaulted debts" following major industrial expansion crippled the American economy.[20] In response, Lewis Tappan launched the Mercantile Agency in 1841 with the sole purpose of overcoming the problems of distance and depersonalization in commercial credit.[21] Tappan's agency converted social

---

16 Phillips, *supra* note 11 at 295.

17 Lawrence Lessig's pathetic dot theory posits that individuals are regulated by four forces: law, social norms, the market, and technical infrastructures. See Lawrence Lessig, *Code: And Other Laws of Cyberspace, Version 2* (New York: Basic Books, 2006).

18 It is important to remember that data subjects are unlikely to be customers of data brokerage.

19 This paper treats "consumer reports," "credit evaluation," "credit reports," and "credit scores" as synonyms for the collection, analysis, and disclose of personal information to support consumerism. This is an oversimplification simplification of the development of the industry and the issues which scoring itself poses.

20 Lauer, *supra* note 4 at 29.

21 *Ibid.*

relationships into "disembodied and increasingly abstract forms of data" through which individuals acquired a new identity: financial identity.[22] Like modern platform capitalists, Tappan transformed collected knowledge into a centralized, subscription-based reporting service. Also, similar to modern data-rich companies, the agency tightly controlled access to its data. Subscribers had to travel to the agency's offices where a clerk would summarize information from ledgers without providing a copy.[23]

Despite Tappan's best efforts, his agency and its competitors were subject to leaks.[24] This exposed the industry not only to reduced revenues, but a bigger threat: libel suits. The industry successfully lobbied for their reports to be treated as privileged communication between agency and subscriber.[25] Strict confidentiality and lack of deliberate malice immunized the industry from civil liability for defamation, even where its data was inaccurate. This immunity empowered the retail industry to take up the innovations of the commercial credit reporting agency in the 1870s. Early consumer reporting organizations also published highly confidential information in closely guarded "credit rating books."[26] One of the first companies to do this, the Retail Credit Company (now Equifax) would go door-to-door to collect information about consumers and sold their complied data in "Merchant Guides" for $25.[27] Consumer reporting, however, added the direct experience of a retailer's interactions with the customer to an individual's profile.[28] When pooled with records from other retailers, these insights created patterns of promptness, or struggle, with credit obligations.

20th Century

By the early 20th century, consumer reporting agencies used an array of techniques, including interviews, to extract and manage data, bringing individuals "into networks of communication over which they had little control or knowledge."[29] Entrance into this system was not optional. Further,

---

22 *Ibid* at 32.

23 *Ibid* at 33.

24 This issue, of course, continues to plague the industry. See Stacy Cowley & Tara Siegel Bernard, "As Equifax Amassed Ever More Data, Safety Was a Sales Pitch" *New York Times* (23 September 2017), online: < www.nytimes.com/2017/09/23/business/equifax-data-breach.html?mcubz = 0 > .

25 The first major libel suit occurred in 1851 where a husband claimed he was barred from purchasing goods because a local correspondent informed the Mercantile Agency that his wife was about to file for divorce and alimony, reducing his assets. An agency employee was jailed for failing to provide the identity of the data collector. See *Reports of the Four Leading Cases Against the Mercantile Agency for Slander and Libel* (New York: Dun, Barlow & Vo, 1873).

26 Lauer, *supra* note 4 at 66.

27 Cowley & Siegel Bernard, *supra* note 24.

28 Lauer, *supra* note 4 at 69.

the information obtained by consumer reporting agencies was increasingly augmented by other forms of data.[30] Linking these datasets was not a mistake or simple technological affordance. The credit reporting industry purposefully set out to "preach the doctrine that credit is character," sustaining the future of their business by embedding themselves in the moral fabric of capitalism.[31]

Josh Lauer writes that one of the most striking aspects of early consumer reporting was that it generated so little public reaction.[32] This may be because credit surveillance was presented as a socially redeeming technology, commended for its democratic approach to the treatment of customers. Individuals "assumed equal rights" under the law of objective credit reporting and scoring.[33]

As post-war debt soared, new credit instruments such as retail store charge cards and universal credit cards created immense demand for up-to-date credit information.[34] One of the biggest problems facing the industry, however, was ensuring accuracy. Potential sources of inaccuracies included clerical errors in books of creditors, unreliable gossip, malicious reports, confusion between similar identities, consumer disputes reported as defaults, material mistakenly placed in the wrong files by careless file-clerks, and errors missed by a busy telephone reporter.[35] Computerization was the industry's answer. Sophisticated digital scoring systems first emerged in the late 1950s.[36] The subsequent efficiencies and power gained by the industry was enormous. However, unlike the first 90-odd years of the consumer reporting industry, this change did not go unnoticed.

B. Public Response to Computerization

By the end of the 1960s, the reporting industry found itself "at the centre of a public firestorm that left its benevolent self-image in tatters."[37] In 1966, a

---

29 *Ibid* at 125.

30 *Ibid* at 115. By late 1930s, the accumulated newspaper clippings of some credit bureaus were considered a valuable resource in their own right. In 1938, Reader's Digest confirmed that "every possible source of information is used to keep this great reference library alive."

31 *Ibid* at 126.

32 *Ibid* 136.

33 *Ibid* at 131.

34 In 1965, the total indebtedness for all forms of consumer credit amounted to $7 billion, an over eight-fold increase over 1948. See Jacob S Ziegel, "Consumer Credit Regulation: A Canadian Consumer-Oriented Viewpoint" (1968) 68:3 Colum L Rev 488 at n 1.

35 Dale Gibson & John Sharp, *Privacy and commercial reporting agencies* (Winnipeg: Legal Research Institute of the University of Manitoba, 1968) at 15.

36 Lauer, *supra* note 4 at 185. Interestingly, the banking industry was better positioned, financially and technologically, to lead computerization of credit data, but did not because the industry's attitude toward personal information was much more conservative.

37 *Ibid* at 212.

congressional committee was established to investigate the privacy risks of a central government database on citizens. It was through publicity of this inquiry that the majority of Americans, and Canadians, discovered that the private-sector databases which tracked their consumption were already online.[38] The reach of the industry shocked lawmakers throughout North America, and even in the United Kingdom.[39] As Lauer writes, "big brother had not arrived in the guise of Orwellian technocrats, but rather as a business system for controlling consumers."[40]

By the end of the 1960s, Canadian consumers were equally concerned as their American counterparts about the rise of computerized credit reporting and scoring.[41] For instance, a 1969 *Toronto Daily Star* article entitled "How your credit rating follows you — everywhere," raised alarm at the scale and speed at which the industry operated.[42] Despite the fact that the comparatively under-resourced Canadian consumer reporting agencies were still far from computerization,[43] similar legislative committees and royal commissions on privacy were established across Canada. The federal and provincial legislatures quickly responded by enacting a "veritable cornucopia of new legislation."[44]

C. Legal Responses to Computerized Consumer Reporting

Ontario's first attempt to legislate in response to growing privacy concerns was 1965's *Private Investigators and Security Guards Act*, which enforced a licensing regime on "private investigators."[45] Disappointingly, despite defining

---

[38] At the 1966 hearings of the congressional subcommittee on computers and privacy, the testimony of RAND Corporation's Paul Baran, who pioneered the packet switching technology underpinning internet protocols, shocked the committee. While explaining that the bits and pieces of separate automated information systems the private sector was already building were more dangerous than the single data bank the government was only just contemplating, Baran was interrupted by Rep. Benjamin Rosenthal: "So the point you make is that even though the Government has not put their stamp of approval on building this system it is growing on its own because various groups are independently developing its starting points?" Baran responded: "Precisely."

[39] The 1972 Younger Committee on Privacy identified three specific areas of concern: the use of computers to compile personal profiles; their capacity to correlate information; and the ease with which unauthorized access to data could be obtained, often from remote sites. See Rowland, Kohl & Charlesworth, *supra* note 2 at 331.

[40] Lauer, *supra* note 4 at 221.

[41] The loss of privacy was dismissed by the *Toronto Daily Star's* Financial Editor Jack McArthur as a "journalistic fad," in a 1964 article. McArthur, like modern platform capitalists, suggested concerned citizens could simply choose not to participate: "If you really want to protect your "privacy," you can do it by not borrowing or buying on time." See Jack McArthur, "You can get too private," *Toronto Daily Star* (6 June 1964).

[42] Sue Howden, "How your credit rating follows you — everywhere," *Toronto Daily Star* (21 June 1969) 76.

[43] Jacob S Ziegel, "Canadian Consumer Reporting Legislation: Trends and Problems" (1973) 11:3 Osgoode Hall LJ 503 at 503.

[44] Ziegel, "Consumer Credit Regulation," *supra* note 34 at 498.

investigations to include information into personal character, the statute specifically exempted investigators who search for and disclose credit, employment, or insurance information.[46] In 1966, the Ontario Law Reform Commission initiated a preliminary study into the nature of existing and growing problems respecting the "right to privacy."[47] The resulting Ryan Report drew heavily on the work of Alan Westin and framed privacy as a basic human psychological and physiological need. Summarizing the anxiety of the time, it warned against the "trend towards de-individualization" and predicted reduced strength in claims based in privacy.[48] The Ryan Report criticized the consumer reporting industry's invasive methods of data collection, noting that these activities are carried out not to invade privacy but to serve economic interests, "which in turn afford the fundamental rationalization of "service to the general prosperity."[49] Informed by the burgeoning consumer protection movement, the Ryan Report centered the importance of economic pluralism:

> The interests in not being made object of commercial advertising, the interest in not being made an unwilling factor in market research, the interest in not owning a car or telephone set or the interest generally in being economically individualistic without being subject to either major social disadvantage or the pressure of being thought to be eccentric by a peer group.[50]

It also challenged the logic of the "general headings" under which the "assault on privacy" was justified; economic efficiency, police efficiency, government efficiency and social utility all represented an overwhelming pressure on "a reordering of human values."[51]

---

[45] R.S.O. 1965, c. 102, s. 2 (defined as "a person who investigates and furnishes information for hire or reward, including a person who searches for and furnishes information as to the personal character or actions of a person, or the character of business or occupation of a person.").

[46] At a 1970 conference in London, University of Manitoba Professor John Sharp criticized the Act's fragmented approach to privacy and suggested that *"every* data bank should be subject to a licensing requirement regardless of whether it is operated by a government agency, insurance, finance or credit reporting company or other person." See JM Sharp, "Some proposals for legislation in Canada" in RC Rowe, ed, *Privacy, Computers and You* (Manchester: National Computing Centre Limited, 1972) at 130.

[47] Ryan, *supra* note 6 at 1. The Law Reform Commission's introduction described the problem resulting from the potential use of data banks as: "the grave threat posed to all free men and democratic institutions by modern technology and well-intentioned government and commercial practices that expose the individual to public and institutional scrutiny; that record and collate all his transactions; and that treat him as an object to be manipulated in the attainment of public, social and economic goals."

[48] *Ibid* at 3.

[49] *Ibid* at 4.

[50] *Ibid*.

[51] *Ibid* at 10. Impressively, the Ryan Report also commented on the contextual nature of information, noting that standards of privacy are relativistic, such that it is hard to know

Federalism Debate

The Ryan Report explicitly called for legislative reform: "absent legal regulation, dynamic norms of economic positivism almost invariably prevail over the static norms of manners."[52] This pre-*Charter* review unsurprisingly spent significant time mapping the federalism issue facing a provincial intervention. Until this point, Ontario was reticent to participate in the growing challenge posed by technology.[53] Attorney-General Arthur Wishart indicated that the province *could* legislate eavesdropping and the electronic items used for such activities, but adhered to the position that wiretapping and electronic surveillance should be handled at the federal level, as it is closely related to criminal law.[54] The Ryan Report, however, dismissed the objection to the exercise of provincial powers, noting that, contrary to a prior report, eavesdropping was not a crime at common law transferred to Parliament at Confederation.[55]

The Ryan Report noted that none of the federal schemes purporting to protect consumers were grounded in a view of privacy as a unified concept.[56] The Report concluded that the province had the power to intervene if legislation was framed as directed at suppressing conditions calculated to favour the development of crime, rather than at the actual punishment of crime. If concerned with the quality of life, actions must equal the scope of the right at stake:

> If the objective is to grant protection to privacy that is reasonable under the circumstances of any given case, then legislation must not only limit the claim to privacy by this formula, but should also limit those competing claims that are based upon considerations of public interest, economic well-being, commercial expedience, control of anti-social activities, and all the rest. Without creating parallel norms, particularly in those areas with either a strong laissez-faire tradition or an established set of distinctive institutional values, then the exceptions

---

what will actually "invade someone's privacy." For a comprehensive treatment of the concept of privacy as contextual, see Helen Nissenbaum, "Privacy as Contextual Integrity" (2004) 79 Wash L Rev 119.

52 Ryan, *supra* note 6 at 4.

53 *Ibid.*

54 *Ibid* at 16. See also Howden, *supra* note 42. Wishart was operating under the assumption that then-Justice Minister John Turner would legislate in the area of consumer privacy.

55 Ryan, *supra* note 6 at 17. Eavesdropping was brought within cognizance of the courts by *Justices of the Peace Act 1361*. In *Re MacKenzie*, 1945 CarswellOnt 63, [1945] O.R. 787, [1946] 1 D.L.R. 584, 85 C.C.C. 233 (Ont. C.A.): King's Counsel concluded that the power to administer preventive justice to deal with the nuisance of eavesdroppers is vested in magistrates and Justices of the Peace in Ontario.

56 The Ryan Report review included criminal provisions regarding trespass and intimidation, the *Bell Telephone Act of 1880*, the *Statistics Act,* the *Radio Act*, the *Telegraphs Act*, and the *Railway Act*.

> inherent to granting protection to privacy that is "reasonable under all the circumstances" may eat up the rule.[57]

Among the Report's 20 recommendations were establishing controls over private sector acquisition, use, and disclosure of personal information; personal remedies; a system of consent; and controls over invasion of privacy related to employment and other institutions whose legitimate activities establish a threat to privacy. These recommendations were ultimately picked up by lawmakers in Ontario. However, the Report's chief requests, standalone privacy legislation and the creation of a privacy tort, were ignored.[58]

American Influence

The consumer reporting industry in America had been operating with virtual impunity and believed itself to be an outstanding protector of individual privacy. To a congressional hearing in 1968, a reporting industry executive told members: "We have protected privacy for the past 60 years [. . .] and frankly, gentlemen, we believe we can do it with computers."[59] However, privacy scholar Alan Westin's well-publicized testimony from 1966 remained a direct challenge to this proposition. Westin illustrated the lax control over personal information for the congressional subcommittee by obtaining, in one day, the "report of character" of his female research assistant, detailing not only her financial standing but information on her "character, habits, and morals."[60]

In response to both the attention on the 1966 subcommittee on computers and privacy and the growing influence of the consumer protection movement, Congress enacted the *Fair Credit Reporting Act* (FCRA) in October 1970.[61] This legislation became the model for both state and provincial action. Consumers gained rights to notification in the case of employment and investigative report requests, and were provided the credit bureau's contact information when denied credit, insurance, or employment benefits, or when their interest rates were increased on the basis on an adverse report. Adverse items on reports were to be deleted after seven years. Most importantly, consumers gained the right to review, correct, and monitor the circulation of their personal information, but without a right to inspect the report directly. Otherwise, consumer reports could be furnished in response to a court order, for providing government benefits, for employment or insurance purposes, or to a person with a "legitimate business need" to use the information.

---

57 Ryan, *supra* note 6 at 73.

58 In 1968, British Columbia passed its *Privacy Act*, making it "a tort, actionable without proof of damage, for a person wilfully and without a claim of right to violate the privacy of another." No substantial guidance was given as to the meaning or content of this baldly stated cause of action.

59 Lauer, *supra* note 4 at 218.

60 *Ibid* at 219.

61 *Fair Credit Reporting Act*, 15 USC § 1681 (2016).

Importantly, the FCRA created civil liability for non-compliance. As Augusta Wilson writes, "the wall of silence and secrecy, the refusals because 'we don't think it feasible at this time,' the 'privilege' to ruin a person's career or credit because of negligence" were destroyed by the FCRA.[62] However, the FCRA model was immediately criticized for two major deficiencies. First, without direct inspection, the industry was allowed to revert to the secretive methods of 19th century mercantile agencies, obfuscating what information they did share with consumers when required by law.[63] Second, the vague "legitimate business need" stipulation was a catchall.[64] Allowing information about business transactions involving the consumer to flow to any persons who have a legitimate need for that information meant the protections were limited by what was normatively viewed as legitimate business operations.[65] This framework inherently favours the private sector over consumers because it is the industry-defined business need that triggers the disclosure of a credit report, not the individual's consent.[66]

D. Ontario's Consumer Reporting Act

Legislative History

While Ontario struggled to mobilize in response to the FCRA, its counterparts in Manitoba, Saskatchewan, and Nova Scotia enacted legislation based on the American model. After the Ryan Report, Professor Jacob Ziegel lobbied for credit reporting reform in the province. Ziegel dismissed the business community's "Panglossian frame of mind" which critiqued consumer law as a

---

[62] Augusta E Wilson, "The Future of Common-Law Libel Actions under the Fair Credit Reporting Act" (1971) 21:1 Cath U L Rev 201 at 202 ("Since the common-law requirements for establishing malice are so stringent, and since 15 U.S.C. 168(1)(e) prohibits actions for defamation unless the false information has been published with malice, most consumers will probably proceed in the future under Section 168(1)(o), which allows actual damages for negligent noncompliance," or under § 168(1)(n), which permits both actual and punitive damages for willful noncompliance with the statute).

[63] Lauer, *supra* note 4 at 226-227.

[64] See *Fair Credit Reporting Act*, *supra* note 61, § 604.

[65] In 1996, the "legitimate business needs" test abandoned the "involving the consumer" formulation and replaced it with "initiated by the consumer" to clarify that there is no permissible purpose for using a consumer report unless the consumer is already a customer of the business. See US, Federal Trade Commission, Advisory Opinion, "Advisory Opinion to Tatelbaum" (26 July 2000), online: <www.ftc.gov/policy/advisory-opinions/advisory-opinion-tatelbaum-07-26-00>. Further, a FTC Staff Opinion notes that Congress intended the "permissible purposes" provisions of the Act to cover, primarily, eligibility issues. See US, Federal Trade Commission, Advisory Opinion, "Advisory Opinion to Buchman" (2 March 1998), online: <www.ftc.gov/policy/advisory-opinions/advisory-opinion-buchman-03-02-98>.

[66] See, e.g., US, Federal Trade Commission, Advisory Opinion, "Advisory Opinion to Coffey" (11 February 1998), online: <www.ftc.gov/policy/advisory-opinions/advisory-opinion-coffey-02-11-98>.

leftist conspiracy. He instead relied on overwhelming proof of disparity in bargaining power and the work of Henry Maine to emphasize the lack of meaningful *consensus ad idem* in credit reports: modern society was reversing its progress towards a society based on contract instead of status.[67] Further, Ziegel criticized the judiciary's "painfully" slow pace at responding to the problems posed by consumer reporting, noting that the "fiction of freely arrived at bargains still haunts the judicial corridors."[68]

A private members bill to protect privacy from invasion by the credit rating industry was introduced on October 2, 1969, but did not receive debate.[69] In October 1972, then Minister of Financial and Consumer Affairs, Arthur Wishart, introduced Bill 23, *An Act to provide for the Control of Credit Reporting Agencies, the Collection of Credit Information and Credit Reporting*. Bill 23 was poorly drafted, and Bill Davis' Conservatives allowed it to lapse. In early 1971, the new Minister, John Clement, introduced a rewritten bill, *An Act to Control the Storage and Supply of Personal Information for Rating Purposes*. Unlike Bill 23 before it, this legislation would regulate not only credit reporting but the "all-important field of personal information."[70] Bill 229 received a second reading and was debated thoroughly, however, it fell subject to the legislative timetable. In the next session, Clement reintroduced the legislation as Bill 101, which subsequently received assent to on October 30, 1973 as the *Consumer Reporting Act*.[71]

The Act requires all consumer reporting agencies to register with the Registrar of Consumer Reporting Agencies and requires all persons seeking a consumer report to notify applicants about their intention. Individuals are granted the right to know whether or not a report has been obtained. If a benefit was refused because of an adverse report, the recipient of the report must tell the consumer. Consumers were also given the right to know what information an agency had collected and from whom, the right to have the agency correct errors drawn to its attention, and the right to see a copy of their reports. Yet, the resulting legislation suffered from the same deficiencies as the FCRA. As a result of the publicity of Alan Westin's testimony before the congressional committee, most Canadian legislation about consumer reporting included considerable detail about the types of persons to whom a consumer report may be released.[72]

---

67 Ziegel "Consumer Credit Regulation," *supra* note 34 at 491.

68 *Ibid* at 492.

69 Ontario, Legislative Assembly, *Official Report of Debates (Hansard)*, 28th Parl, 1st Sess (2 October 1969) at 6523 (Douglas Kennedy) ("An Act to provide for the protection of personal privacy prohibits violation of privacy including electronic eavesdropping and the collection and use of economic commercial and social data without consent. It also provides for the machinery for supervision and control.").

70 Ontario, Legislative Assembly, *Official Report of Debates (Hansard)*, 29th Parl, 2nd Sess (6 December 1972) at 5194 (DM Deacon).

71 See *Consumer Reporting Act*, *supra* note 15.

72 See *ibid* s. 8.

However, this detail boiled down to the same unprincipled "legitimate business reason" test found in the FCRA.[73]

The source of these deficiencies can be explained by three all-too-familiar themes which emerged during the debates over Bill 229 and Bill 101. First, the legislature struggled to define the problem they were tasked with solving. Similarly, facing pressure from industry but lacking an understanding of computerization, lawmakers did not clearly conceptualize the degree of transparency to be granted to the consumer. Finally, and most interestingly, there was debate over whether legislating the qualified privilege historically afforded to the industry was necessary at all.

Theme 1: Definitional Problems

A major flaw identified before Bill 229 was tabled was defining the scope of the legislation. The debate in the Legislature was influenced by the 1968 report of Dale Gibson and John Sharp that explained that there were two types of reporting agencies causing concern: information exchanges between groups of merchants, and information exchanges which actively search for information on behalf of their members or customers.[74] For descriptive and functional purposes, a distinction was drawn between the two in Bill 229.[75] In debate, however, opposition member Donald Deacon suggested that the definition of "personal reporting agency" was too narrow, applying only to those furnishing consumer reports, and excluding purposes of investigation like insurance.[76] Instead, Patrick Lawlor called for separate legislation modeled on British Columbia's *Privacy Act*.[77] Without clear definitions of exactly what activity was regulated and why, the unchecked power of the industry could continue to grow.

Theme 2: Transparency Debate

Gibson and Sharp identified two serious risks to the privacy of individuals: inaccurate or misleading information being reported, and accurate information used for unjustifiable purposes.[78] This problem troubled Ontario's lawmakers more than other jurisdictions as they debated whether to exclude uncorroborated information from agency reports.[79] Bill 229 included a provision excluding the information unless its lack of corroboration was noted in the report. In Bill 101,

---

[73] *Fair Credit Reporting Act*, *supra* note 61, s. 8(1)(d)(vi).

[74] Gibson & Sharp, *supra* note 35 at 9. Their report, which focused on privacy implications, also emphasized the risks posed by supplementing data collected with public records and newspaper clippings.

[75] Ziegel, "Canadian Consumer Reporting Legislation," *supra* note 43 at 507.

[76] Ontario, Legislative Assembly, *Official Report of Debates (Hansard)*, 29th Parl, 2nd Sess (6 December 1972) at 5195 (DM Deacon).

[77] Ontario, Legislative Assembly, *Official Report of Debates (Hansard)*, 29th Parl, 2nd Sess (6 December 1972) at 5198 (PD Lawlor).

[78] Gibson & Sharp, *supra* note 45 at 13.

[79] *Ibid* at 511. See also Sharp, *supra* note 46 at 130 where he raises this issue.

only uncorroborated *adverse* information needed to be noted. Agencies could use uncorroborated evidence so long as they adopted "reasonable procedures" to ensure the accuracy of their records.

The right to transparency was strongly resisted by the industry because of the potential exposure to libel action.[80] Jacob Ziegel also criticized Bill 101's notification requirement for being too onerous in application, as it required individuals who would never think they were subject to the legislation to notify consumers. His examples included a professor rejecting a research assistant because of a poor recommendation, a lawyer who interviews an articling student, or a landlady who declines a room.[81] This concern was picked up in legislative debate in October 1973. Curiously, Bill 101 was the only legislation of the era to include a provision that a credit grantor may not disclose to others information about their transactions or experiences with the consumer without consent. Ziegel questioned whether this 180-degree turn from industry norms would actually be taken up. He opined: "is it really a meaningful step towards protecting the consumer's privacy in a domain where publicity and the free dissemination of information has long been the rule?"[82] Despite public criticism, the Legislature ultimately deleted the clause protecting the disclosure of information by one credit grantor to another, implicitly supporting industry.[83]

Theme 3: Legitimating Intrusion

Alan Westin's 1966 testimony made its way directly into debate over Bill 229 when Lawlor raised the example of how easy it is to get an individual's report. Lawlor criticized the bill for intending to protect privacy but providing no preventative mechanism. Echoing the Ryan Report, Jim Renwick argued at the Standing Committee:

> . . . the right to privacy that we are talking about is the need for a citizen's protection against the intrusion of his privacy regardless of whether statement which are made are true or false. What we are concerned about in our society is the need to protect people against the true statement which is involved in terms of his own private life which is just nobody's business[84]

Renwick went on to express concern about the methods of observation used by credit reporting agencies which to the ordinary citizen are "the least ungentlemanly if not reprehensible."

Further, Renwick challenged the very purpose of the legislation in debate on both Bill 229 and Bill 101.[85] Renwick suggested the financial industry's need for

---

[80] Ziegel, "Canadian Consumer Reporting Legislation," *supra* note 43 at 506.

[81] *Ibid* at 509.

[82] *Ibid* at 510.

[83] "Another defeat for the right to privacy," *The Globe and Mail* (5 October 1973) 6.

[84] Ontario, Legislative Assembly, *Official Report of Debates (Hansard)*, 29th Parl, 2nd Sess (6 December 1972) at 5205 (JA Renwick).

consumer information was overstated: "it seems to me what we are doing here is institutionalizing a credit reporting industry which had its origin in the assumed need of financial institutions in the province to get information about individual citizens"[86] Raising Warren and Brandeis's famous 1891 essay on the right to privacy Renwick explained that the right is not just to prevent inaccurate portrayal of private life, but to prevent its being depicted at all:

> . . . we cannot support this bill which appears to legitimize the right of credit reporting agencies to collect personal information, meaning information about a consumer's character, reputation, health, physical or personal character or mode of living.[87]

Interestingly, Bill 229 did not extend qualified privilege to the agency when obliged to open its files, opening the agency to civil litigation. Clement intended to allow the common law of defamation to protect credit reporting, arguably defeating the purpose of intervening in the industry at all. Ziegel criticized the legislature for this oversight and noted that the Manitoba Act provided the immunity expressly.[88] Lawlor pointed out the Legislature ought to understand the difference in American law on qualified privilege and Canadian law. In the United States, absent gross negligence, nuisance or trespass, credit agencies were able to disseminate information broadly. In Canada, qualified privilege only related to the internal dissemination of the information — leaks were subject to damages and to injunctions with the onus on the information collector to prove they were not negligent.[89] Yet, this difference was not entrenched in the Bill in any way. Ultimately, Renwick concluded that the "Bill is not a step forward because of the scope of the information collected." The lack of express qualified privilege indicated a lack of purpose to the legislation which opened up a significant gap in Ontario's data protection law. What is the public interest in a consumer protection statute that only implicitly affirms the common law and industry norms?

---

85 *Ibid* at 4844.

86 *Ibid* at 5198.

87 *Ibid* at 5207.

88 See Ziegel, "Canadian Consumer Reporting Legislation," *supra* note 43 at 513 ("If a reporting agency is obliged to open its files to the consumer fairness would seem to suggest that it should also be protected against libel suits, at least in those cases where the agency has exercised reasonable care in the collection and dissemination of the information on its files and has acted without malice."). In the Manitoba legislation, an express privilege was provided at s. 16: "No user, personal reporter or personal reporting agency is civilly liable to the subject of a personal report or personal file, unless the user, reporter or agency, as the case may be is or ought to be reasonably aware that part or all of the information in the report or personal file is false, or misleading, or was obtained negligently."

89 Ontario, Legislative Assembly, *Official Report of Debates (Hansard)*, 29th Parl, 2nd Sess (6 December 1972) at 5199 (JA Renwick).

II. CONSUMER LAW'S CONTEMPORARY ROLE

A. Resulting Gap in Consumer Law in Ontario

Existing Enforcement Problems

A 1975 Globe and Mail article reported that when Bill 101 was passed, the Credit Bureau of Greater Toronto hired extra staff for an expected rush. However, Ontario consumers did not respond, likely because the vast majority of consumers did not hit roadblocks related to their credit.[90] The decline in interest in consumer protection law did not help.[91] Despite known flaws in the legislation, the Act was not updated until 1988 when amendments requiring agencies to inform consumers about third party requests for information were added in an attempt to stop businesses from using consumer reports to target consumer marketing.[92]

As expected by Bill 101's detractors, the Ontario courts upheld the common law qualified privilege protecting consumer reports. In *Haskett v. Trans Union of Canada Inc.,* the leading case on consumer reporting in Ontario, the Court of Appeal held that a claim for negligence is available for incorrect reporting of information.[93] In a 2009 study of the Act, Kent Glowinski criticized the low threshold agencies must meet in addressing consumer complaints.[94] For instance, *Anderson v. Excel Collection Services Ltd.* confirmed that only false information "knowingly" supplied will fall under the Act's offence provision.[95] This means that consumers who are unhappy with the practices of an agency or an entry on their report are limited to filing a complaint with the Registrar.[96]

Glowinski notes that while litigation challenging the accuracy of information on credit reports is a relatively new phenomenon, there is a significant access to justice issue limiting this evolution of consumer protection law.[97] Not all

---

[90] Elizabeth Patton explains how those who do complain about privacy, or are overtly concerned with their privacy, are often cast as "paranoid," yet this paranoia is required by privacy law jurisprudence in the assessment of whether a subjective reasonable expectation of privacy is objectively reasonable. See "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places" 50:3 UTLJ 305.

[91] See Jacob Ziegel, "Is Canadian Consumer Law Dead" (1995) 24:3 Can Bus LJ 417 (Ziegel blamed the decline in interest in consumer law on the Reagan Administration's apathy for consumer protection).

[92] Dawn King, "Ontario requires credit bureaus to tell consumers about reports," *The Globe and Mail* (27 June 1988) A13.

[93] *Haskett v. Trans Union of Canada Inc.*, 2003 CarswellOnt 692, 224 D.L.R. (4th) 419, 63 O.R. (3d) 577, [2003] O.J. No. 771 (Ont. C.A.).

[94] Kent Glowinski, "Don't Get Enough Credit? The Need for an Impartial Consumer Credit Report Appeal Tribunal in Ontario" (2009) 22 J L & Soc Pol'y 5 at 6.

[95] 2005 CarswellOnt 4829, 260 D.L.R. (4th) 367, [2005] O.J. No. 4195, 143 A.C.W.S. (3d) 391 (Ont. Div. Ct.).

[96] The Act provides a right to appeal from the Registrar. But, as Glowinski notes, since 2000, not one appeal regarding incorrect information on a credit report has been brought before the Licence Appeal Tribunal.

individual consumers have the expertise, nor can they afford litigation against a corporation like Equifax. Further, litigation over negative information on a credit report requires the entire judicial process of a civil defamation action, which backlogs Ontario's courts.[98] These limitations suggest that more direct government intervention through a statutory regime is required to protect citizens in this area.

Emerging Enforcement Problems

The nature of credit reporting has also changed. When the *Consumer Reporting Act* was enacted, there were nearly 200 credit reporting agencies in Canada; today, there are two.[99] Contemporary "credit reporting agencies" look very different because in our data-rich world, the credit bureau's access to consumer account information and past payment behaviour is no longer unique. In the age of big data, the distinction between credit and noncredit data has lost its meaning.[100] Reputations can be inferred from other variables not directly connected to credit history, such as social media activity, or even one's use of capitalization in an online application.[101] Equifax and TransUnion are now just two of many data brokers that peddle names, addresses, and behavioural insights.[102] Contrary to a purposive approach to the *Consumer Reporting Act,* Ontario has not enforced licensing requirements on new entrants to this industry.[103]

For example, the growing digital tenant and employee screening sector is currently unregulated. Two Canadian start-ups, Certn and Naborly, exemplify why this lack of enforcement may be concerning. Both Certn and Naborly offer a platform which allows landlords to create custom tenant applications that collect

---

97 Glowinski, *supra* note 94 at 10.

98 *Ibid* at 14.

99 Ziegel, "Canadian Consumer Reporting Legislation," *supra* note 43; Glowinski, *supra* note 94 at 6. There are also credit-monitoring services like Credit Karma which, in exchange for the very same information consumers try to protect, will show a credit score.

100 Lauer, *supra* note 4 at 266.

101 *Ibid* at 267.

102 The Office of the Privacy Commissioner (OPC) defines data brokers as "companies that collect personal information about consumers form a variety of public and non-public sources and resell the information to other companies." See Research Group of the Office of the Privacy Commissioner of Canada, "Data Brokers: A Look at the Canadian and American Landscape" (Ottawa: Office of the Privacy Commissioner of Canada, 2014).

103 See *Re Rizzo & Rizzo Shoes Ltd.,* [1998] 1998 CarswellOnt 1, 1998 CarswellOnt 2, [1998] 1 S.C.R. 27, 154 D.L.R. (4th) 193 (*sub nom.* Adrien v. Ontario Ministry of Labour), [1998] S.C.J. No. 2 (S.C.C.). ("Today there is only one principle or approach, namely, the words of an Act are to be read in their entire context and in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act, and the intention of Parliament.").

pertinent information from tenants.[104] The platforms create a comprehensive dossier, in some cases using "over 500 data points," on the potential tenant including social media, credit, rents histories, and even a basic Google search on the tenant, to provide a prediction to the landlord on whether or not the tenant is suitable for a lease.[105] Public knowledge of the functioning of the "artificial intelligence" algorithms used by these startups is limited to their marketing statements.[106]

Since Naborly, which is based in Ontario, does not report to a credit reporting agency, it does not need to register as a "personal information investigator" as defined in the Act.[107] However, a purposive interpretation of s. 2 of the Act would include Naborly as a "consumer reporting agency," considering the purpose of their data use is to provide data to a person who they know intends to use the information in connection with the entering into or renewal of a tenancy agreement.[108] Instead, the digital tenancy screening sector is not currently subject to provincial oversight because its terms of use contract out of the Act, and potentially the Ontario *Human Rights Code*,[109] using a privacy policy that puts the burden of its investigatory role on its customers and prospective tenants.[110]

Naborly and Certn's reach into social behavioural data is comparable to the system of social scoring contemplated by the Chinese Government, which has received widespread criticism.[111] *Wired* reports the State Council's goal is to, by

---

[104] See Naborly, online: <www.naborly.com>; Certn, online: <certn.co/tenancy/>.

[105] John Biggs, "Naborly lets landlords screen tenants automatically," *TechCrunch* (15 August 2016), online: <techcrunch.com/2016/08/15/naborly-lets-landlords-screen-tenants-automagically/>. See Naborly, "Privacy Policy" (June 29, 2018), online: <naborly.com/privacy>.

[106] For example, Naborly explains: "Our Applied Artificial Intelligence system learns from and leverages the experience gained from screening thousands of rental applicants and their tenancy outcomes. This helps Naborly's analysts and customers see patterns of risk that could only can be detected by our AI." See also Certn, "FAQ Softcheck Pre-Screening," online: <certn.co/softcheck/>.

[107] See *Consumer Reporting Act*, *supra* note 15.

[108] Section 2 of the Act defines "consumer reporting agency" as a person who, for gain or profit or on a regular co-operative non-profit basis, furnishes consumer reports. *Ibid*, s. 2.

[109] R.S.O. 1990, c. H.19.

[110] See Naborly, *supra* note 105: "We may collect information from various sources, including credit reporting agencies, collection agencies, government entities and legal suppliers. We also collect information from you directly. We collect information when you sign up for a Naborly account, when you provide information as part of our identity verification process, or when you fill out a form or enter information on the Website. We also collect information when you upload information to the Service, participate in promotions offered by Naborly or our partners, respond to our surveys, or otherwise communicate with us.".

[111] See, e.g., Rachel Botsman, "Big data meets Big Brother as China moves to rate its citizens," *Wired UK* (21 October 2017), online: <www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion>.

2020, trail all citizens with a file of public and private data, searchable by biometrics, covering all of society. The system is enabled by Alipay, a third-party mobile and online payment platform that collects financial, social media, and location data to assess a credit score and uses big data to apply a "social score."[112] Like early 20th century consumer surveillance, Alipay's social credit system and tenant screening algorithms are designed to "ensure that the bad people in society don't have a place to go, while good people can move freely and without obstruction."[113]

Predictive algorithms, like Naborly's and Certn's, mine personal information to make guesses about individuals' likely actions and risks.[114] Because humans program these predictive algorithms, their biases and values are embedded within.[115] As the OECD explains, "the misuse of these insights can affects core values and principles such as individual autonomy, equality and free speech, and may have a broader impact on society as a whole."[116] Despite claiming efficiencies for consumers in the short-term, the emphasis on sorting is detrimental to consumers. The discrimination enabled by data analytics limits an individual's ability to escape the impact of pre-existing socio-economic indicators.[117] Citizens end up with fewer choice of goods or service, higher prices, and poorer quality, thereby increasing wealth inequality.[118] The result is that "firms can not only take advantage of a general understanding of cognitive limitations, but can uncover, and even trigger, consumer frailty at an individual level."[119] Without regulation, negative inferences made by platforms like Naborly and Certn will drive landlord action because correlation is deemed sufficient.[120] However, even accurate information is capable of causing harm if

---

[112] Mara Hvistendahl, "Inside China's Vast New Experiment in Social Ranking," *Wired* (14 December 2017), online: < www.wired.com/story/age-of-social-credit/ > . Interestingly, in contrast to North America, China's massive economy developed to the present without much of a credit system.

[113] *Ibid.* Worse than in the 1930's though, the way the Chinese social credit system is designed, being blacklisted by a retailer sends you on a rapid downward spiral: "First your score drops. Then your friends hear you are on the blacklist and, fearful that their scores might be affected, quietly drop you as a contact. The algorithm notices, and your score plummets further."

[114] Keats Citron & Pasquale, *supra* note 12 at 3.

[115] *Ibid.*

[116] OECD, *Data-Driven Innovation for Growth and Well-Being: Interim Synthesis Report* (Paris: OECD, 2014).

[117] *Ibid.*

[118] Maurice Stucke & Allen Grünes, *Big Data and Competition Policy* (Oxford: Oxford University Press, 2016) at 53.

[119] Frank Pasquale, "Algorithms: How Companies' Decisions About Data and Content Impact Consumers" (Written testimony before the United States House of Representatives Committee on Energy and Commerce Subcommittee on Digital Commerce and Consumer Protection, 29 November 2017) citing Ryan Calo, "Digital Market Manipulation," (2014) 82:4 Geo Wash L Rev 995.

used in such an unreasonable manner. As Gibson and Sharp wrote in 1968, "truth is a dangerous commodity."[121]

B. Privacy Law's Private Law Limit

Limits of Consent-based Legislation

The failure to enforce provincial consumer protection law cannot be cured by existing private-sector privacy regulations. While all private companies in Canada that collect, use, or disclose personal information in the course of commercial activity, including consumer reporting agencies, are subject to the *Personal Information Protection and Electronic Documents Act* (PIPEDA),[122] the Act is insufficient to protect the right to be left alone contemplated by the consumer law movement. PIPEDA is based on the OECD Privacy Guidelines, which require that individuals must provide valid and informed consent before the collection, use, or disclosure of personal data. This model of consent, however, relies on users deciding for themselves how to weigh the costs and benefits of the collection, use, or disclosure of their information. Despite emphasizing the rights to transparency, to notice, to prevent personal data from being used for new purposes, and to correct or amend one's record, this scheme has been widely criticized because it relies on a mythical "informed and rational person" who makes appropriate decisions.[123] Further, consent today cannot reasonably be considered informed consent to a vague but accurate description of a use in the distant future, especially if that use is subject to change with context. As Zeigel knew in 1961, *consensus ad idem* is non-existent in the trade of consumer information.

Further, like in the *Consumer Reporting Act,* the notion of a tradeoff between privacy and legitimate business interests is fundamental to PIPEDA.[124] Yet, evidence suggests that rather than trading off privacy for free cheap goods and services, many "feel resigned to the inevitability of surveillance and the power of marketers to harvest their data."[125] Also, the regulatory scheme presented by PIPEDA does not include an enforcement mechanism for unreasonable reuse of personal information. Instead, it allows user-generated content to become the

---

[120] *Ibid* at 8.

[121] Gibson & Sharp, *supra* note 35.

[122] S.C. 2000, c. 5 [PIPEDA].

[123] Daniel Solove, "Introduction: Privacy Self-Management and the Consent Dilemma" (2013) 126 Harv L Rev at 1880. Frank Pasquale describes this model as a "naïvely economistic approach to privacy as a normal good or service to be bargained for, like any other," Frank Pasquale, *supra* note 119 at 19.

[124] See PIPEDA, *supra* note 122, s. 3.

[125] See University of Pittsburgh Annenberg School for Communication, "The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation," by Joseph Turow, Michael Hennessy & Nora Draper (2015).

private property of the platform which collects it, normalizing apathy amongst users.

Limits of Protecting Privacy and Reputation Together

The purpose of PIPEDA is to protect the privacy of individuals, in a manner that is tempered against the needs of organizations to collect, use, or disclose personal information for legitimate purposes, particularly focused on supporting and promoting electronic commerce.[126] Far too often, however, this purpose is conflated with the protection of reputation. Privacy, as a right of control, is very different from reputation. One fundamental difference lies in the fact that revelation of the truth in reputation cases should not be considered defamatory, while the revelation of the truth in privacy cases can often be harmful for the victim. In addition, reputation protections (primarily the tort of defamation) are seen to chill free speech, while privacy protections (either statutory or in tort) defend autonomy and are thus seen to encourage expression.[127] Reputation and privacy may be different aspects of an individual's persona, both shaping their participation in democracy, but the law has drawn a sharp distinction between the two. Privacy should not be conflated with reputation, as the harm emanating from one does not constitute the harm emanating from the other.

The S.C.C.'s recent handling of reputation in *Charter* jurisprudence perhaps extends this confusion. In *Hill v. Church of Scientology of Toronto*, the Court held that defamation constitutes an invasion of privacy, worthy of protection and careful balancing against freedom of expression.[128] This seemingly departs from the previous jurisprudence regarding the absoluteness of freedom of expression. Further, in *A.B. v. Bragg Communications*, the S.C.C. continued to blur the distinction between reputation and privacy by treating these separate aspects of an individual's persona together.[129] In this case, a teenager sought to unmask her cyberbullies in order to pursue a defamation action, while preserving her own anonymity. The Court balanced the open courts principle with the plaintiff's privacy interests, allowing the anonymous plaintiff to realize the benefits of a defamation action. Ultimately, laws protecting reputation are unhelpful for consumer protection because they rely heavily on one tool: correcting falsehoods. Therefore, defamation is limited to correcting for malice.

Further, free speech is frequently invoked to protect the business model of the attention economy. The insights mined out of user behaviour become the

---

[126] See especially David Fraser, "You'd better forget the right to be forgotten in Canada," *Canadian Privacy Law Blog* (28 April 2016), online: < blog.privacylawyer.ca/2016/04/youd-better-forget-right-to-be.html > .

[127] Antoon Da Baets, *Responsible History* (New York: Berghahn, 2008) at 131.

[128] *Hill v. Church of Scientology of Toronto*, 1995 CarswellOnt 396, 1995 CarswellOnt 534, [1995] 2 S.C.R. 1130, [1995] S.C.J. No. 64, 126 D.L.R. (4th) 129 (S.C.C.) at para 121.

[129] David Ralph, "Anonymity and Defamation" in G Martin, R Scott Bray & M Kumar, eds, *Secrecy, Law and Society* (London: Routledge, 2015) at 211; *A.B. (Litigation Guardian of) v. Bragg Communications Inc.*, [2012] 2 S.C.R. 567, 2012 SCC 46.

speech of the platform to be strongly defended against regulatory intervention. Defamation law's core balancing act between the public interest in expression and the protection of reputation affirms the power of platforms. Importantly, this "free speech opportunism" is rooted in a neoliberal tradition older than Google or Facebook's founders: the myth of consumer choice.[130] Without the option to not participate, consumer choice cannot truly exist.

Just as consumer surveillance was defended in the 19th and 20th centuries by the choice it provided to consumers and by the idea that the free flow of credit into the economy was essential to society, platform capitalism is protected by the myth of Internet exceptionalism. In the mid-1990s and early 2000s, regulators were weary of imposing burdens on Internet intermediaries because they wanted to preserve the "utopian" ideals presented by the Internet.[131] Early liability schemes accepted the importance of an "unfettered" Internet. This myth, that the Internet is unique and should be afforded its own regulatory framework outside traditional legal norms, pervades Canadian copyright, telecommunication, and even defamation law.[132] However, policies which grant sweeping immunity to Internet platforms impact the rule of law because they fail to address how technological innovation will not necessarily enhance freedoms. For example, as Dutton notes, the protection and proliferation of freedom of expression is not a technologically determined outcome or an inherent consequence of Internet use.[133] Further, contrary to popular belief, provinces are able to exert control over Internet platforms and data brokers because these intermediaries are readily localizable.[134] Intermediaries are not just global actors, but also local businesses

---

[130] See Pasquale, "Reputation," *supra* note 8 at 524 (Pasquale describes this opportunism as "Google's core defence.").

[131] See especially Pippa Norris, *Digital Divide? Civic Engagement, Information Poverty and the Internet Worldwide* (Cambridge: Cambridge University Press, 2001). The prime example of this policy position is the enactment of 47 USC § 230, an amendment to the United States *Communication Decency Act* ("CDA") which immunized online providers from liability for publishing most types of third party content.

[132] Tim Wu, "Is Internet Exceptionalism Dead?" in Berin Szoka & Adam Marcus, eds, *The Next Digital Decade—Essays on the Future of the Internet* (Washington, DC: Tech Freedom, 2010) 179 at 180. See especially *Society of Composers, Authors & Music Publishers of Canada v. Canadian Assn. of Internet Providers*, 2004 SCC 45, 2004 CarswellNat 1919, 2004 CarswellNat 1920, [2004] 2 S.C.R. 427, (*sub nom.* SOCAN v. Canadian Assn. of Internet Providers), [2004] S.C.J. No. 44 (S.C.C.). See also *Crookes v. Wikimedia Foundation Inc.*, 2011 SCC 47, 2011 CarswellBC 2627, 2011 CarswellBC 2628, (*sub nom.*Crookes v. Newton), [2011] 3 S.C.R. 269, [2011] S.C.J. No. 47 (S.C.C.), in which the S.C.C. assessed the balance between the core significance of hyperlinks to the Internet and principles of defamation, concluding "strict application of the publication rule in these circumstances would be like trying to fit a square archaic peg into the hexagonal hole of modernity."

[133] William Dutton, et al, *Freedom of Connection—Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet* (Paris: UNESCO, 2011) at 6.

[134] Janni Riordan, *The Liability of Internet Intermediaries* (Oxford: Oxford University Press, 2016) at 7.

acting through physical infrastructure.[135] Regardless, these challenges within privacy and Internet law indicate the need for help from other areas of law.

III. LESSONS FROM THE HISTORY OF CONSUMER LAW

A. Role for Consumer Law in 21st Century Canada

In 1968, Zeigel asked:

> . . . would it not be better to abandon the fiction of contract altogether and to recognize that the state may have to regulate all the significant terms of consumer credit transactions, just as it has been compelled to do in the case of several types of insurance contracts?[136]

The 2017 ruling in *Douez v. Facebook* echoes this question. In *Douez*, the court was faced with determining the correct forum for a dispute over the alleged invasion of a Canadian user's privacy by Facebook. The social media platform's contract of adhesion purported to displace the British Columbia *Privacy Act*, forcing the user to bring suit in California, a jurisdiction decidedly less sympathetic to those who exchange their personal information to access the conveniences of a free online service.[137] Writing for the majority, Justice Abella found in favour of the Canadian user, emphasizing the "quasi-constitutional" nature of privacy legislation and, most importantly, the power imbalance between the monolithic platform and the individual. Justice Abella's decision, like Ziegel before her, questions the existence of "meaningful alternatives" in a society structured around platform capitalism.[138]

Marina Pavolvic explains how this power imbalance is worsened under platform capitalism, which is dominated by a few monopolistic market players. While consumers still play the role of passive actors in the market economy, "virtually all aspects of our daily lives and social interactions are made possible by, and conditioned on, being consumers first."[139] Often, in order to access goods and services on a platform the user must first agree to a lengthy standard-from contract:

---

[135] For a more detailed account of the materiality of the Internet, see Andrew Blum, *Tubes: A Journey to the Center of the Internet* (Toronto: HarperCollins, 2012).

[136] Ziegel, "Consumer Credit Regulation," *supra* note 34 at 491.

[137] The S.C.C. continues to deny the existence of the doctrine of third party consent in Canada. See *R. v. Marakah*, 2017 SCC 59, 2017 CarswellOnt 19341, 2017 CarswellOnt 19342, [2017] 2 S.C.R. 608, [2017] S.C.J. No. 59 (S.C.C.) at para 40; *R. v. Cole*, 2012 SCC 53, 2012 CarswellOnt 12684, 2012 CarswellOnt 12685, [2012] 3 S.C.R. 34, [2012] S.C.J. No. 53 (S.C.C.) at para 74.

[138] *Douez, supra* note 1.

[139] Marina Pavolvic, "Consumer rights in a radically different marketplace," *Policy Options* (4 June 2018), online: < policyoptions.irpp.org/magazines/june-2018/consumer-rights-radically-different-marketplace/ > .

> When they read digital books, stream documentaries or submit assignments through learning management systems, students are being consumers first. When we use our phones, the Internet, messaging apps or social media to communicate with friends and family, we are all being consumers first. The list of interactions that are premised on being consumers first goes on and on.[140]

And yet, Canadian provinces have largely failed to enforce their legislative schemes regulating consumer surveillance, which themselves only address technical errors or omissions on credit reports. To date, there is still no binding legislative or administrative tool for a consumer to challenge or dispute incorrect information on a credit report.

After *Douez*, the potential for a province to regulate the interaction between platforms that collect data and consumers is clearer. As Keats Citron and Pasquale note, we have made commitments to protect consumers from serious harms that they have no means to prevent and thus "providing oversight to the scoring systems that can cause negative spirals should be a critical aim of our legal system."[141] If the fundamental problem posed by modern data brokers is that we lack viable alternatives, the law may be required to create those alternatives. However, to effectively learn from the first attempt at regulating consumer surveillance in the 1970s, the legislatures ought to recognize the specific role of data collection in platform capitalism: to support business. Correcting for this power imbalance will require returning to the three questions that plagued the legislature during debate over the *Consumer Reporting Act:* why is consumer protection necessary; who is the consumer; and why legitimize industry norms through legislation.

B. Potential Solutions

Limited Solution: No-Go Zones and Intrusion Upon Seclusion

The Office of the Privacy Commissioner suggested returning to the idea of "No-Go Zones" for data collection, use, and disclosure. This proposal seeks to separate legitimate information management practices from areas organizations should not venture into.[142] While this call from the OPC is commendable for emphasizing fair, transparent, and accountable data analysis which avoids false positive or false negative results, it is a limited solution. The history of credit reporting regulation proves that "legitimate business interests" is a low threshold, incapable of addressing the overwhelming power imbalance between platforms and users. Further, this idea is already captured in s. 9(3) of the

---

[140] *Ibid.*

[141] Keats Citron & Pasquale, *supra* note 12.

[142] See Office of the Privacy Commissioner of Canada, "Draft guidance: Inappropriate data practices — interpretation and application of subsection 5(3)" (Ottawa: OPC, 2017), online: < www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-consent-under-pipeda/gd_53_201709/ > .

Consumer Reporting Act, which lists what type of data cannot be included in a consumer report. Instead, a solution must center the citizen's ability to not participate, no matter how reasonable and bona fide the business interest.[143] Without more, this solution will repeat the mistake of simply entrenching the status quo.

Another limited solution is a turn to tort law, which was called for in the original debates over the *Consumer Protection Act*. The American tort of intrusion upon seclusion was adopted by the Ontario Court of Appeal in 2012 in *Jones v Tsige*.[144] To make out the tort, the defendant's conduct must be intentional, must have invaded, without lawful justification, the plaintiff's private affairs, and must be regarded by a reasonable person as highly offensive causing distress, humiliation, or anguish.[145] It provides a monetary remedy and is therefore a disincentive, but it does not address the norms afforded by technological change which encourage a loss of privacy because, like defamation, intrusion upon seclusion too relies on malice. While an important tool in certain circumstances, it is a line drawing exercise with little usefulness in achieving the goal of consumer protection of correcting for power imbalances.

In the court's decision in *Jones*, Justice Sharpe implied that it is morally problematic that information can now be improperly accessed with ease, but penalized only the age-old human interest in the information of others. This underscores a lack of understanding of the process of information design. The design of digital platforms, like a bank's account databases, is not arbitrary. Distinct choices are made in the design of each system, in response to contextual needs. What is unaddressed by the structure of the *Jones* test is that the injury caused by a nosey viewer is also a consequence of the cost-benefit analyses performed by a corporation while designing their business. Thus, the tort as currently formulated arguably creates a remedy without a right because it does not assess or deter systems which normalize this type of impropriety.[146] Corporations simply have to avoid malice, but the individual citizen is not granted any right to better data protection. By obscuring the role of systems design, *Jones* does not help with the problem at hand: reinforcing why consumer protection, which includes the right to be left alone or to choose which economic systems to participate in, is important to a free and democratic society.

---

[143] Relatedly, there should be protection of partial participation as a type of participation.

[144] *Jones v. Tsige,* 2012 ONCA 32, 2012 CarswellOnt 274, 108 O.R. (3d) 241, 346 D.L.R. (4th) 34, [2012] O.J. No. 148 (Ont. C.A.).

[145] *Ibid* at para 71.

[146] *Douez, supra* note 1 at para 59. ("In this context, it is especially important that such harms do not go without remedy. And since Ms. Douez's matter requires an interpretation of a statutory privacy tort, only a local court's interpretation of privacy rights under the Privacy Act will provide clarity and certainty about the scope of the rights to others in the province.")

Promising Suggestion: Enforcing "Data Cut-Off" Laws

In 1970, Professor Sharp suggested that "cut-off" dates should be applied to certain adverse facts collected by consumer reporting agencies after the lapse of given periods of time.[147] This idea, borrowed from bankruptcy law, was added to the *Consumer Reporting Act* because lawmakers recognized the contextual nature of information. However, modern Canadian proposals to enforce the deletion of information by Internet intermediaries are widely criticized and quickly dismissed.[148] At their best, these arguments recognize the fundamental importance of freedom of expression in society and the potential for abuse.[149] At their worst, a Canadian court decision requiring an American corporation to help with the administration of justice by not sharing a patent-infringing product description, using technology that the corporation uses every day to change the global distribution of information, was recast as a validation of potential human rights violations in foreign totalitarian states.[150]

These dismissals of broad, unspecific approaches to data processing should not discourage Canadian lawmakers. Enforcing the concept of data "cut-off dates" already provided for in the *Consumer Reporting Act* could also have an anti-trust element.[151] By devaluing stores of potentially irrelevant information, platforms may be less inclined to merge and hoard datasets. Accurate data on consumer preferences could then be privileged over inferences from unwieldy datasets. "Cut-off dates" are not a "right to be forgotten." As Ignacio Cofone explains, the decision in *Google v. Spain*, which ushered in global conversations about the permanency of digital memory, is not about limiting speech, but rather the liability of search engines under the rights and obligations established in the European Data Protection Directive.[152] In the decision, the European Court of Justice dictates that the processing of data that is no longer relevant violates the

---

147 Sharp, *supra* note 46.

148 See, e.g., Michael Geist, "'Right to be forgotten' ruling lacks balance: Geist" *Toronto Star* (16 May 2014), online: < www.thestar.com/business/tech_news/2014/05/16/right_to_-be_forgotten_ruling_lacks_balance_geist.html > .

149 See, e.g., Nicholas Watt & Mark Sweeney, "Sajid Javid: Terrorists and criminals are exploiting 'right to be forgotten,'" *The Guardian* (11 November 2014), online: < https://www.theguardian.com/technology/2014/nov/11/sajid-javid-terrorists-criminals-right-to-be-forgotten > .

150 See *Google v. Equustek Solutions Inc.,* 2017 SCC 34, 2017 CarswellBC 1727, 2017 CarswellBC 1728, [2017] 1 S.C.R. 824, 410 D.L.R. (4th) 625 (S.C.C.); Jason Proctor, "Google appeal of worldwide injunction headed to Supreme Court," *CBC News* (18 February 2016), online: < www.cbc.ca/news/canada/british-columbia/google-appeal-of-worldwide-injunction-headed-to-supreme-court-1.3453653 > ("the worldwide injunction could lead to lowest-common denominator law, where technology companies like Google are forced to respond to restrictive judgments from courts in countries like Saudi Arabia").

151 See Stucke & Grünes, *supra* note 118.

152 Ignacio Cofone, "Google v Spain: A right to be forgotten?" (2015) 15:1 Chicago-Kent J Int'l & Comp L 1.

terms of the directive, and extends the right to erasure and the right to objection to include search engines as a consequence of considering them. In this light, *Google v. Spain* simply supports the enforcement of data processing law. Whether data hoarding is the consumer problem we need to solve should be studied in the Canadian context.

Promising Suggestion: Enforcing a Right to Explanation

In 1966, Yale Law Profess Charles Reich testified that the obfuscation of data processing was a "denial of the constitutional right to confront, the constitutional right to face those who make statements about you, to question them, and to rebut and answer."[153] While a modern approach to data "cut-off dates" will help challenge the monopoly of data-rich platforms, a "right to explanation" influenced by the original debate over the *Consumer Reporting Act* goes one step further.

Keats Citron and Pasquale suggest that protection for citizens could result from "technological due process," where predictive algorithms would be required to live up to standards of review and revision to ensure fairness and accuracy.[154] This approach, however, is plagued by the same problem of self-regulation if "fairness" and "accuracy" are defined by the data owner, and not the data producer. An exemplary "right to explanation" can be found in Europe's new General Data Protection Regulation.[155] Certain provisions of articles 13-15 require data controllers to provide data subjects with information about the existence of automated decision making, including profiling, meaningful information about the logic involved and the significance for the subject through notification and an access to information right. Article 22 of the directive provides that data subjects "have the right not to be subject to a decision based solely on automated processing, including profiling, as well as which produces legal effects concerning him or her or similarly significantly affects him or her."

As Selbst and Powles argue, these rights support fundamental aspects of autonomy and personhood because they require explanations that are meaningful to the subject, a person presumably without technical expertise.[156] An example of this right in practice is legislation requiring a platform to explain an automated decision well enough for the data subject to determine whether they have an actionable discrimination claim.[157] This could be accomplished at

---

[153] US, *The Computer and Invasion of Privacy: Hearings Before a Subcommittee of the Committee on Government Operations*, House of Representatives, 89th Cong, 2nd sess (Washington, DC: United States Government Printing Office, 1966) at 28.

[154] Keats Citron & Pasquale, *supra* note 12 at 8.

[155] Andrew D Selbst & Julia Powles, "Meaningful Information and the Right to Explanation" (2017) 7:4 International Data Privacy Law 233.

[156] *Ibid.*

[157] *Ibid* at 8. ("This interpretation is supported by Article 5's requirement that data processing be lawful, fair, and transparent to the data subject, as well as Article 12's

the licensing phase required by the *Consumer Reporting Act*. A plain-language description of how a consumer reporting agency's data processing practices accord with the *Human Rights Code* as a precondition to obtaining a license to operate in a province would be a welcome start.

Model Solution: Vermont's Return to Meaningful Oversight

The most promising response may be the simplest: a return to an active state enforcement of basic regulatory tactics. In response to recent data breaches, the state of Vermont passed Bill H.764, *An act relating to data brokers and consumer protection*, in an attempt to impose accountability on companies that collect and sell information about Vermont residents. Under the new legislation, data brokers are defined as businesses "aggregating and selling data about consumers with whom the business does not have a direct relationship" and which "provide information that is critical to services offered in the modern economy, including: targeted marketing and sales; credit reporting; background checks; government information; risk mitigation and fraud detection; people search; decisions by banks, insurers, or others whether to provide services; ancestry research; and voter targeting and strategy by political campaigns."[158] Data brokers are required to pay a $100 annual fee to register with the state and must educate Vermont residents on the data they collect, and how to withdraw their consent to collection. Further, Vermont removed fees previously associated with freezing credit reports collected by credit reporting bureaus.[159] This legislation is promising primarily because it is not innovative. It applies tested statutory tools at the local level in an attempt to correct the imbalance of power favouring industry. It takes on the challenge of redefining the problem of consumer protection for the twenty-first century, clarifies who it seeks to protect, and explains why it is legislating in this space.[160] This project of redefining consumer rights in legislation to reflect the "new complexities" of consumer-business relationships is essential to protecting human rights.[161]

CONCLUSIONS

Consumer protection legislation across the country has not responded adequately to "the realities of today's marketplace."[162] This is not because the

---

emphasis on intelligibility and requirement that '[t]he controller shall facilitate the exercise of data subject rights.'").

158 US, H.764, An act relating to data brokers and consumer protection, 2017-18, Reg sess, Vt, 2018 (enacted).

159 AJ Dellinger, "Vermont Passes First-of-Its-Kind Law to Regulate Data Brokers," *Gizmodo* (27 May 2018), online: < gizmodo.com/vermont-passes-first-of-its-kind-law-to-regulate-data-b-1826359383 > .

160 The main impetus behind Bill H.764 is cyber security.

161 Pavolvic, *supra* note 139.

162 *Ibid.*

enactors of those statutes were incapable of contemplating platform capitalism, but rather because there is not yet public consensus on what meaningful choice over personal information means in the contemporary commercial spaces of our free and democratic society. The history of consumer surveillance in Ontario also illustrates that citizens have never been made fully aware of how the information collected about them is used. However, this does not mean citizens accept the trade-off presented to them. Where there are no meaningful alternatives to participation in platform capitalism, a legal response will not do well to only protect citizens where corporations are objectively operating in bad faith. Canada's private-sector privacy regulation has failed to meet this challenge — reducing the distance between citizen and data holder — because it is based on a model of consent which cannot easily conceptualize activities beyond the direct relationship between user and data collector.[163] As Lisa Austin argues, if we care about control over our own beliefs, prejudices, wants, we need to move past a model of privacy as access and towards a model of privacy as power.[164] When Ontario's consumer protection laws are purposively enforced in a way that recognizes the imbalance of power in modern consumer-business relationships, users may be more likely to trust firms' privacy promises, which may in turn increase the incentives for firms to compete harder on privacy.[165] This will not happen without *consensus ad idem* on the legitimate purposes of collecting and sharing consumer information. Lacking this renewed commitment to consumer protection, neoliberalism, disguised as Internet exceptionalism and enabled by the historic immunity provided to the consumer reporting industry, will continue to commodify and exploit consumer data in an unregulated environment.

---

[163] Lisa Austin, "Enough About Me: Why Privacy is About Power, Not Consent (or Harm)" in Austin Sarat, ed, *A World Without Privacy?: What Can/Should Law Do*, online: < papers.ssrn.com/sol3/papers.cfm?abstract_id = 2524512 > at 7.

[164] *Ibid.*

[165] Stucke & Grünes, *supra* note 118 at 326.