

# Democratic Rights in a Technocratic Age

## WHEN CONSTITUTIONS (IN LAW) ARE NOT ENOUGH

*Jane Bailey\**

*Today we can examine the interconnected systems of manufacturing, communications, transportation and the like that have arisen during the past two centuries and appreciate how they form a de facto constitution of sorts, the constitution of a sociotechnical order.*

— Langdon Winner<sup>1</sup>

*You have zero privacy anyway. Get over it.*

— Scott McNealy, then CEO of Sun Microsystems<sup>2</sup>

## A. INTRODUCTION

In 2017 we mark the occasion of the thirty-fifth anniversary of the repatriation of Canada's Constitution<sup>3</sup> and the entrenchment of the *Canadian*

---

\* Full Professor, University of Ottawa Faculty of Law (Common Law Section), jbailey@uottawa.ca. Thanks to Safa Abdel Rahman for her excellent research support and to the Social Sciences and Humanities Research Council for funding The eQuality Project ([www.equalityproject.ca](http://www.equalityproject.ca)), a seven-year partnership initiative, of which the research in this paper forms a part.

1 Langdon Winner, *The Whale and the Reactor: A Search for Limits in an Age of High Technology* (Chicago: The University of Chicago Press 1988) at 47.

2 Polly Sprenger, "Sun on Privacy: 'Get Over It'" *Wired* (26 January 1999), online: [www.wired.com/1999/01/sun-on-privacy-get-over-it/](http://www.wired.com/1999/01/sun-on-privacy-get-over-it/).

3 *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.

*Charter of Rights and Freedoms* (the *Charter*).<sup>4</sup> As early as 1972, the predecessor to Canada's Constitution, the *British North America Act*,<sup>5</sup> had been described as inadequate in that it did "not serve Canadians fully as either a mirror of ourselves or as an aspirational ideal."<sup>6</sup> Similarly, the *Charter's* predecessor, the unentrenched *Canadian Bill of Rights*,<sup>7</sup> also came up short in terms of democratic ideals. The 1972 Special Joint Committee on the Constitution saw

a Bill of Rights which is entrenched in the Constitution serving as a guarantee to individuals that democracy does not mean ruthless uniformity, as a symbol to minorities that their reasonable autonomy will be respected, and as a sign to the whole people of a wholesome rationality in a world often given to a ceaseless struggle for power.<sup>8</sup>

In 1982, after years of debate, dialogue, and negotiation, Canada's Constitution was finally repatriated, although the province of Quebec (which has its own statutory *Charter of Human Rights and Freedoms*<sup>9</sup>), declined to sign on.<sup>10</sup> Incorporated in Canada's Constitution is a body of rights and freedoms entrenching guarantees relating to expression, mobility, life, liberty, and security of the person, search and seizure, equality and many others. At the repatriation ceremony, then-Prime Minister Pierre Trudeau described the process as a "coming of age" story:

For more than half a century, Canadians have resembled young adults who leave home to build a life of their own, but are not quite confident enough to take along all their belongings . . . .

After fifty years of discussion we have finally decided to retrieve what is properly ours . . . . It is my deepest hope that Canada will match its new legal maturity with that degree of political maturity that will allow us to make a total commitment to the Canadian ideal.

---

4 *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.

5 *The Constitution Act, 1867* (UK), 30 & 31 Vict, c 3, reprinted in RSC 1985, Appendix II, No 5.

6 Senate & House of Commons, Special Joint Committee of the Senate and House of Commons on the Constitution of Canada, *Final Report*, Joint Chairs: Senator Gildas L Molgat & Mark MacGuigan (Ottawa: Information Canada, 1972) at 6.

7 *Canadian Bill of Rights*, SC 1960, c 44.

8 *Final Report*, above note 6 at 19.

9 *Quebec Charter of Human Rights and Freedoms*, CQLR c C-12.

10 Recent news coverage, however, suggests that the Constitution could be reopened in order to address Quebec's concerns: Amy Minsky, "After 35 Years, Why Does Quebec Want in the Constitution?" *Global News* (2 June 2017), online: <https://global-news.ca/news/3496355/quebec-canada-constitution-amend-reopen/>.

...

I speak of a country where every person is free to fulfill himself or herself to the utmost, unhindered by the arbitrary actions of governments.

...

We now have a Charter which defines the kind of country in which we wish to live, and guarantees basic rights and freedoms which each of us shall enjoy as a citizen of Canada.

It reinforces protection offered to French-speaking Canadians outside Quebec, and to English-speaking Canadians in Quebec. It recognizes our multicultural charter. It upholds the equality of women, and the rights of disabled persons.<sup>11</sup>

The *Charter* doesn't just set out rights that are internationally recognized as building blocks of democracy and respect for humanity. It also provides a judicial oversight mechanism as a check and balance to delimit the exercise of *government* authority vis-à-vis the individual.<sup>12</sup> It has long been recognized, however, that restrictions on individual rights and freedoms emanate not just from government, but from other individuals<sup>13</sup> and groups, particularly those that enjoy concentrated forms of power, such as multinational corporations.<sup>14</sup> In this sense, it is by no means startling to point out, as Langdon Winner does in the epigraph to this chapter, that the decisions that technology companies make can and do affect the rights of individuals and the communities to which they belong. What I suggest here, however, is that whatever that point may be lacking in novelty, it makes up for in urgency, particularly in light of unilateral declarations that privacy is dead or outdated by representatives

- 
- 11 Pierre Elliot Trudeau, "Remarks by the Prime Minister at the Proclamation Ceremony on April 17, 1982" (1982), online: Office of the Prime Minister [www.collectionscanada.ca/primeministers/h4-4024-e.html](http://www.collectionscanada.ca/primeministers/h4-4024-e.html).
- 12 Indeed, concerns about unnecessary government intrusion on individuals' lives formed part of the debate around the repatriation process: see, for example the remarks of Hon Arthur Jacob Epp during parliamentary debate: Parliament, Special Joint Committee of the Senate and of the House of Commons on the Constitution of Canada 1980–1981, *Minutes of Proceedings and Evidence*, 32nd Parl, 1st Sess, Issue 46 (27 January 1981) at 66 (Hon Arthur Jacob Epp).
- 13 John Stuart Mill, for example, highlighted the "tyranny of opinion" as a de-liberating force: *On Liberty* (London: Longman, Roberts & Green, 1869), online: [www.bartleby.com/130/3.html](http://www.bartleby.com/130/3.html).
- 14 See, for example: Florian Wettstein, *Multinational Corporations and Global Justice: Human Rights Obligations of a Quasi-Governmental Institution* (Palo Alto, CA: Stanford University Press, 2009).

of former and existing technology titans, like that of Scott McNealy in the epigraph.<sup>15</sup>

It is tempting to think of the situation we face as one involving two tracks for world making. In one, elected officials enact *laws* that are constrained by entrenched constitutional rights that delimit government authority vis-à-vis the individual, where the bounds are overseen by courts with obligations of public accountability. In the other, private corporations and actors regulate behaviour through *code*, with little oversight and few formal obligations of public accountability. The reality, however, is much more complex, because these are intersecting, rather than parallel, tracks. Government officials and law enforcement agents, for example, are often the beneficiaries and users of the data gathered and the sorting processes created by private enterprise, generating controversy around the bounds of “lawful access.”<sup>16</sup> Further, law and public policy become inextricably interwoven with technocraft<sup>17</sup> when service providers privately entrench, in standard form contracts, exclusive rights for themselves to regulate what users do and what can be done with users’ content and data. In so doing, they arguably purport to take on the role of “quasi-governmental bodies”<sup>18</sup> without the trappings of public accountability that normally apply to performance of government functions.

This chapter aims to highlight the impact of technocraft on fundamental matters of Canadian constitutional law and public policy. Part B sketches out some of the metrics of the increasingly digitally networked world that Canadians inhabit, in order to contextualize the significance of the practices of corporate technology players on our daily lives. Part C considers two examples relating to technological systems that affect fundamental democratic rights to privacy, equality, and free expression. The conclusion offers suggestions as to what more can and should be done to shore up the democratic rights entrenched in Canada’s repatriated Constitution thirty-five years ago.

---

15 For a similar view expressed by Facebook CEO Mark Zuckerberg regarding privacy no longer being a social norm, see: “Mark Zuckerberg at TechCrunch ‘10 on Privacy and Social Norms,” online: YouTube [www.youtube.com/watch?v=18uTrGmDCkg](http://www.youtube.com/watch?v=18uTrGmDCkg).

16 Jane Bailey & Sara Shayan, “Systematic Government Access to Private-Sector Data in Canada” in Jim Dempsey & Fred Cate, eds, *Bulk Collection: Systematic Government Access to Private-Sector Data* (New York: Oxford University Press, 2017) 147.

17 My use of the terms “technocraft” and “statecraft” throughout this chapter draws on the work of Winner, above note 1.

18 Thorsten Busch & Tamara Shepherd, “Doing Well by Doing Good? Normative Tensions Underlying Twitter’s Corporate Social Responsibility Ethos” (2014) 20:3 *Convergence* 293 at 293.

## B. THE DEPTH OF OUR CONNECTIVITY

Thirty-five years ago, when certain rights and freedoms were constitutionally embedded into Canadian law following laborious, highly public, and often divisive acts of political statecraft, the permeation of digitized communications systems into every aspect of our lives and their potential impact was just beginning to creep into public consciousness. In 1982, the first truly mobile cell phone had just been invented,<sup>19</sup> the list of all of the email addresses on the forerunner of the Internet was contained in one two-inch thick book,<sup>20</sup> Disney opened its Experimental Prototype Community of Tomorrow (EPCOT) Centre that was to “take its cue from the new ideas and new technologies that are now emerging from the creative centers of American industry,”<sup>21</sup> and *Time* magazine named “the personal computer” the “Man of the Year” – “the first non-human to receive the award since its inception in 1927.”<sup>22</sup> According to *Time*,

There are some occasions, though, when the most significant force in a year’s news is not a single individual but a process, and a widespread recognition by a whole society that this process is changing the course of all other processes. That is why, after weighing the ebb and flow of events around the world, TIME has decided that 1982 is the year of the computer.<sup>23</sup>

In 1980, 724,000 personal computers had been sold, a number that doubled in 1981 and in 1982.<sup>24</sup> Thirty-five years later, these numbers are quaint by comparison. In the first half of 2017, over 100,000,000 personal computers shipped worldwide,<sup>25</sup> a figure representing only a fraction of

- 
- 19 Abhishek Singh, “The Journey of Mobile Phones and its Price Since 1982 [Infographic]” *Dazeinfo Media* (29 December 2011), online: <https://dazeinfo.com/2011/12/29/the-journey-of-mobile-phones-and-its-price-since-1982-infographic/>.
- 20 Kate Torgovnick May, “What the Internet Looked Like in 1982: A Closer Look at Danny Hillis’ Vintage Directory of Users” (18 March 2013), *TedBlog* (blog), online: <http://blog.ted.com/what-the-internet-looked-like-in-1982-a-closer-look-at-danny-hillis-vintage-directory-of-users/>.
- 21 “Epcot Grand Opening,” *This Day in Disney History.com*, online: [www.thisdayindisneyhistory.com/EpcotGrandOpening.html](http://www.thisdayindisneyhistory.com/EpcotGrandOpening.html).
- 22 Marcel Brown, “Personal Computer ‘Man of the Year’” (26 December 1982), *This Day in Tech History* (blog), online: <http://thisdayintechhistory.com/12/26/personal-computer-man-of-the-year/>.
- 23 *Ibid.*
- 24 *Ibid.*
- 25 “Quarterly Personal Computer (PC) Vendor Shipments Worldwide, from 2009 to 2017, by Vendor (in million units)” (2017), *Statista*, online: [www.statista.com/statistics/263393/global-pc-shipments-since-1st-quarter-2009-by-vendor/](http://www.statista.com/statistics/263393/global-pc-shipments-since-1st-quarter-2009-by-vendor/).

the nearly seven billion phones, tablets, and PCs in use in the world by the end of 2016.<sup>26</sup> These figures are, in and of themselves, antiquated ways of measuring technological penetration as users move away from these “traditional devices” towards head mounted displays, virtual personal assistants, and wearables,<sup>27</sup> and as other everyday objects are embedded with computing capacity.<sup>28</sup>

Half way through a weekday in September 2017, an online odometer of sorts showed over 3.7 billion Internet users worldwide, 1.25 billion websites, and in that half day alone: over 146 billion emails sent, over 3.3 billion Google searches, over 3.1 million blog posts, 418 million tweets sent, 3.8 billion videos viewed, 43 million photos uploaded, 69 million Tumblr posts made, and almost 2 billion active Facebook users.<sup>29</sup> These connections, involving people and their *things* (their phones, their tablets, their appliances, their cars), are growing exponentially year over year. For example, in 2015, there were an estimated 15.4 million devices connected to the Internet, a number that is conservatively estimated to grow to 75.4 billion by 2025, while the number of wearable devices is estimated to grow by 31 percent from 28.3 million units sold in 2016 to 82.5 million in 2020.<sup>30</sup> All of these connections create digital trails of ever-increasing detail and scope about our lives,<sup>31</sup> while also exacerbating our attachment to and dependency on technology just to participate in day-to-day life, sometimes with and sometimes without our consent or knowledge.<sup>32</sup>

So, as we memorialize the thirty-fifth anniversary of Canada’s political act of *statecraft*, it is essential to recognize how our ways of life are continuously being altered by both visible and invisible acts of *technocraft*. Perhaps more importantly, we should think carefully about *technocraft*’s effect on the rights and freedoms consciously enshrined as a result of Canada’s acts of *statecraft*. We exist in a time where net-

---

26 “Gartner Forecasts Flat Worldwide Device Shipments Until 2018” *Gartner* (4 January 2017), online: [www.gartner.com/newsroom/id/3560517](http://www.gartner.com/newsroom/id/3560517). This figure itself is estimated to grow by over 2.3 million units per year from 2017–2019.

27 *Ibid.*

28 Afif Osseiran et al, “The Internet of Things” (2017) 1:2 *IEEE Communications Standards Magazine* 84.

29 “Internet Live Stats,” online: [www.internetlivestats.com](http://www.internetlivestats.com).

30 Kelvin Claveria, “13 Stunning Stats on the Internet of Things” (28 April 2017) *Vision Critical* (blog), online: [www.visioncritical.com/internet-of-things-stats/](http://www.visioncritical.com/internet-of-things-stats/).

31 Bruce Schneier, *Data and Goliath* (New York: WW Norton, 2015) at 1–5.

32 Even those who are not connected may find detailed aspects of their lives online by virtue of the connections and postings of others with whom we associate or are associated.

worked digital connectivity of us *and* our things is both pervasive and deeply socially embedded in our everyday lives.<sup>33</sup> Data about us and our transactions, some of which is highly personal, flow through the Internet and are stored in quantities difficult for humans to comprehend.<sup>34</sup> While directly organizing this data into an understandable form is beyond the capacity of the human mind, given the volume, velocity, and variability of “big data,” developing technological methods and techniques “to enable the capture, storage, distribution, management, and analysis of the information” is a significant current project of technocraft.<sup>35</sup> Without doubt, big data analytics have created opportunities for addressing pressing social justice issues in situations where there was simply too much data to be processed in light of existing limitations on human capacity and resources.<sup>36</sup> Further, trading our data can be an economical and convenient way of getting access to information and services where facts about our location or reading preferences are relevant to a specific transaction.<sup>37</sup>

That said, too often the service providers with and through whom we transact, although self-marketed as providers and protectors of basic rights and freedoms, fail to enact those commitments in their dealings

---

33 In 2016, Canadians, on average, spent 4 hours and 21 minutes per day using digital media (including personal computers and phones): “Time Spent with Media in Canada Continues to Grow” *Media-Corps* (2 June 2016), online: <http://media-corps.com/time-spent-with-media-in-canada/>.

34 The four largest online storage and service companies, Google, Amazon, Microsoft, and Facebook, were estimated in 2013 to hold at least 1,200 petabytes of data: Gareth Mitchell, “How Much Data Is on the Internet?” *Science Focus* (23 January 2013), online: [www.sciencefocus.com/qa/how-many-terabytes-data-are-internet](http://www.sciencefocus.com/qa/how-many-terabytes-data-are-internet). A petabyte of data would fill 746 million 3.5 inch high density floppy discs, which would weight 113,422 tonnes (just under the size of two Type 45 destroyers, such as the HMS Duncan): Brian McKenna, “What Does a Petabyte Look Like?” *Computer Weekly* (March 2013), online: [www.computerweekly.com/feature/What-does-a-petabyte-look-like](http://www.computerweekly.com/feature/What-does-a-petabyte-look-like). Cisco estimates that by 2019 Internet traffic will reach 2 zettabytes per year, with 1 zettabyte representing the equivalent of “36,000 years of high-definition video” or the “equivalent of streaming Netflix’s entire catalog 3,177 times”: Stephanie Pappas, “How Big is the Internet, Really?” *Live Science* (18 March 2016), online: [www.livescience.com/54094-how-big-is-the-internet.html](http://www.livescience.com/54094-how-big-is-the-internet.html).

35 Amir Gandomi & Murtaza Haider, “Beyond the Hype: Big Data Concepts, Methods, and Analytics” (2015) 35:2 *International Journal of Information Management* 137, online: [www.sciencedirect.com/science/article/pii/S0268401214001066](http://www.sciencedirect.com/science/article/pii/S0268401214001066).

36 For some examples, see: Caroline Perry, “The Promise of ‘Big Data’” *Harvard Gazette* (31 January 2014), online: <https://news.harvard.edu/gazette/story/2014/01/the-promise-of-big-data/>.

37 Schneier, above note 31 at 49–51.

with us.<sup>38</sup> Complicated user agreements tend to reserve considerable discretion to service providers to make decisions around privacy and equality issues, such as how our data will be used to profile us, and who will use those profiles and for what purpose, as well as free expression issues, such as when a use of their service will be considered an abuse that merits removal of users or content. In addition, these processes of technocraft are typically invisible to the user, as they work to create an environment that reflects the machine-generated profile of that user (or a group to which they are assumed to belong). The non-transparency of these processes is often connected to the fact that service providers want to protect the intellectual property in the mathematical models they have designed. In other cases, even if providers wanted their processes to be transparent, their complexity may simply not be understandable to most people (or sometimes even to the providers themselves).<sup>39</sup> Indeed, the march toward automated decision making through human or machine-designed processes that are documenting and analyzing the minutiae of our lives, for the profit of private enterprise with increasingly concentrated market power,<sup>40</sup> seems destined to ensure that, unless we intervene, the invisibility, non-transparency, and, indeed, incomprehensibility of these systems are only likely to grow.<sup>41</sup>

## C. DEMOCRATIC RIGHTS MEET TECHNOCRATIC PROCESSES

### 1) Algorithmic Sorting: Equality at Stake

In his 1982 repatriation speech, Pierre Trudeau expounded on the virtues of equality and equal opportunity as part of the “Canadian ideal,” noting:

---

<sup>38</sup> Busch & Shepherd, above note 18.

<sup>39</sup> In some cases, humans may not be able to explain the process by which a decision was reached, particularly where the parameters of decision making are the product of machine learning, rather than programmed logic and commands: Will Knight, “The Dark Secret at the Heart of AI” *MIT Technology Review* (11 April 2017), online: [www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/](http://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/).

<sup>40</sup> This concentration of power has led to an anti-trust probe in the US. In that regard, Barry Lynn, Executive Director of the Open Markets Institute, stated in 2016 that Amazon, Google, and Facebook “‘have more power than any previous monopolies we’ve dealt with in the past century’”: Rob Lever, “Debate Swirls as Power of US Tech Giants Grows” *PhysOrg* (24 September 2017), online: <https://phys.org/news/2017-09-debate-swirls-power-tech-giants.html>.

<sup>41</sup> Knight, above note 39.



We know that justice and generosity can flourish only in an atmosphere of trust.

For if individuals and minorities do not feel protected against the possibility of tyranny of the majority, if French-speaking Canadians or native peoples or new Canadians do not feel they will be treated with justice, it is useless to ask them to open their hearts and minds to their fellow Canadians.

. . . [The Charter] recognizes our multicultural character. It upholds the equality of women, and the rights of disabled persons.<sup>42</sup>

Since that time, a not-insignificant body of jurisprudence has developed that considers the meaning of equality, and the limits on government discrimination based on listed and analogous grounds.<sup>43</sup> Similarly, a body of jurisprudence addressing equality has grown over time from human rights tribunals across the country hearing cases involving claims under quasi-constitutional,<sup>44</sup> publicly debated, and promulgated legislation relating to discrimination by private actors providing goods, services, housing, and employment. While the outcomes of these cases are sometimes for better and sometimes for worse in terms of achieving substantive equality,<sup>45</sup> they are regularly deliberated upon in a public forum in which reasons for decision are required. The public processes associated with constitutional entrenchment and articulation of decisions relating to equality and discrimination stand in sharp contrast with technocratic outcomes generated by the algorithmic sort.

An algorithm can be thought of as “a step-by-step procedure for solving a problem or accomplishing some end, especially by a computer.”<sup>46</sup> Considered broadly, then, humans have a long history of using algorithms to do everything from making dinner to predicting outcomes in baseball games.<sup>47</sup> However, in an era of “big data,” involving “nearly ubiquitous collection of consumer data from a variety of sources, the

---

42 Trudeau, above note 11.

43 For an overview of Supreme Court of Canada equality jurisprudence, see Patricia Hughes, “Supreme Court of Canada Equality Jurisprudence and ‘Everyday Life’” (2012) 58 *Supreme Court Law Review* (2d) 245 (Osgoode’s Annual Constitutional Cases Conference), online: <http://digitalcommons.osgoode.yorku.ca/sclr/vol58/iss1/9>.

44 For a review relating to quasi-constitutional legislation, see Vanessa MacDonnell, “A Theory of Quasi-Constitutional Legislation” (2016) 53: 2 *Osgoode Hall Law Journal* 508, online: <http://digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?article=2995&context=ohlj>.

45 Hughes, above note 43.

46 Merriam-Webster Dictionary, online: [www.merriam-webster.com/dictionary/algorithm](http://www.merriam-webster.com/dictionary/algorithm).

47 Cathy O’Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (New York: Crown, 2016) at 15–19.

plummeting cost of data storage, and powerful new capabilities to analyze data to draw connections and make inferences and predictions,<sup>48</sup> algorithms can analyze and use data “in ways that were not previously possible.”<sup>49</sup>

Algorithms create opportunities to monitor and analyze large datasets to generate new insights relating to a wide variety of human endeavours, ranging from safe operation and repair of jets, to prediction of the onset of illness at unprecedentedly early stages, and the identification and destruction of improvised explosive devices in war zones.<sup>50</sup> That said, they are also used to make decisions about individuals’ access to credit, employment, goods and service, education, and even justice.<sup>51</sup> The resulting sort can have serious consequences for fundamental democratic rights such as privacy and equality because, as Gideon Mann and Cathy O’Neil put it, algorithms are “typically trained to learn from past successes, which may embed existing bias.”<sup>52</sup> Further, in many cases, including those involving decisions made by artificially intelligent systems, (i.e., where the system learns from experience rather than from pre-programmed logic), the reasons for algorithmically derived decisions often can neither be understood, nor explained in terms understandable to humans.<sup>53</sup> In many other instances, such as when Google determines our search results based on profiling prior uses, we don’t even seek explanations because we’re simply unaware that such decisions are being made. For most of us, they’ve become part of the background noise of our lives.

Twenty-four years ago (when the *Charter* was only eleven and the World Wide Web was only four), Oscar Gandy, rather presciently, raised

---

48 US, Federal Trade Commission, *Big Data: A Tool for Inclusion or Exclusion?: Understanding the Issues* (Washington, DC: Federal Trade Commission: 2016) at 1, online: [www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf](http://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf).

49 *Ibid.*

50 Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values* (Washington: The White House, 2014) at 6, online: [https://obamawhitehouse.archives.gov/sites/default/files/docs/big\\_data\\_privacy\\_report\\_5.1.14\\_final\\_print.pdf](https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf).

51 O’Neil, above note 47.

52 Gideon Mann & Cathy O’Neil, “Hiring Algorithms Are Not Neutral” *Harvard Business Review* (9 December 2016), online: <https://hbr.org/2016/12/hiring-algorithms-are-not-neutral>.

53 Sandra Wachter, Brent Mittelstadt, & Luciano Floridi, “Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation” (2017) 7:2 *International Data Privacy Law* 76.

concerns about the impacts of algorithmic decision making, describing the “panoptic sort”

[a]s the name I have assigned to the complex technology that involves the collection, processing and sharing of information about individuals and groups that is generated through their daily lives . . . and is used to coordinate and control their access to the goods and services that define life in the modern capitalist economy.<sup>54</sup>

Gandy warned of the panoptic sort’s potential for discrimination, characterizing it as

a sort of cybernetic triage through which individuals and groups of people are being sorted according to their presumed economic and political value. The poor, especially poor people of color, are increasingly being treated as broken material or damaged goods to be discarded or sold at bargain prices to scavengers in the market place.<sup>55</sup>

In addition to the sort resulting in discriminatory judgments about marginalized populations, Gandy predicted an insidious, negative impact on targeted individuals’ understanding of themselves, noting:

Individual identities are formed in interaction with others. The characteristics of those interactions help to determine the salience, as well as the level of comfort with which different aspects of one’s self co-exist. Self-esteem . . . is determined in part by the ways in which [one’s] relevant reference groups are evaluated by others.<sup>56</sup>

Today, we live in a world increasingly controlled and organized by the silent operation of algorithms. And although it is difficult to get inside the “black box”<sup>57</sup> to understand exactly how algorithmic profiling and sorting are operating, we occasionally get glimpses of their discriminatory impacts.

In some cases, algorithms produce discriminatory outcomes because they reflect discriminatory “recipe knowledge”<sup>58</sup> that is embedded in

---

54 Oscar Gandy, *The Panoptic Sort: A Political Economy of Personal Information* (Boulder, CO: Westview Press, 1993) at 15.

55 *Ibid* at 1–2.

56 *Ibid* at 4.

57 Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge, MA: Harvard University Press, 2015).

58 In a brilliant contribution to a set of contemporary judgments in the “Case of the Speluncean Explorers” (first conceived of by Lon Fuller, “Case of the Speluncean Explorers” (1949) 62:4 *Harvard Law Review* 616), John Calmore pointed out that racism can play a central, but unspoken, role in the knowledge that “supplies

them. For example, employers increasingly require candidates to apply for jobs online rather than in person, either on their organization's website or through third-party sites that seek to match available candidates with available positions.<sup>59</sup> Online strategies can expand the scope of recruitment and the use of algorithms can reduce human resource time spent on sorting through applications.<sup>60</sup> In 2016, it was estimated that in the United States 72 percent of resumes filed for positions online were never seen by employers because they "get rejected by applicant tracking systems before a live person even has a chance to review them."<sup>61</sup> However, as Gideon Mann and Cathy O'Neil have pointed out, the algorithms used to sort may themselves reflect and reinforce existing prejudices by, for example, predicting that an applicant is more likely to be successful if they share characteristics with someone who has succeeded in that workplace before.<sup>62</sup> As a result, in workplaces that already lack diversity, this kind of sort simply serves to perpetuate inequality by continuing to exclude those who do not reflect the pre-existing and inequitable status quo. For those with sufficient time and resources, it is possible to "game" online application systems to increase the chances of your resume being seen. Unfortunately, those without such resources "may never know that they are sending their resumes into a black hole."<sup>63</sup>

Similarly, algorithms used by police and courts also reflect and reinforce existing prejudices, all while seeming to produce "positive results." For example, where police use algorithmic models to predict high crime areas as a tool for deciding where to concentrate police patrols, poor and homeless populations that tend to be less mobile and to be more frequently targeted by nuisance charges are likely to be more

---

the institutionally appropriate rules of conduct" and its "motivating dynamics": Naomi Cahn et al, "The Case of the Speluncean Explorers: Contemporary Proceedings" (1993) 61 *George Washington Law Review* 1754 at 1779, citing Peter Berger & Thomas Luckmann, *The Social Construction of Reality* (London: Penguin Books, 1966) at 65.

59 For an early analysis of this trend, see Peter Hausdorf & Dale Duncan, "Firm Size and Internet Recruiting in Canada: A Preliminary Investigation" (2004) 42:3 *Journal of Small Business Management* 325.

60 For example, an online application process used by Unilever in 2017 generated 275,400 applications, half of which were weeded out by an algorithm: Kelsey Gee, "In Unilever's Radical Hiring Experiment, Resumes Are Out, Algorithms Are In" *Fox Business* (26 June 2017), online: [www.foxbusiness.com/features/2017/06/26/in-unilevers-radical-hiring-experiment-resumes-are-out-algorithms-are-in.html](http://www.foxbusiness.com/features/2017/06/26/in-unilevers-radical-hiring-experiment-resumes-are-out-algorithms-are-in.html).

61 "72% of Resumes are Never Seen by Employers" *Accesswire* (16 February 2016), online: [www.accesswire.com/436847/72-of-Resumes-are-Never-Seen-by-Employers](http://www.accesswire.com/436847/72-of-Resumes-are-Never-Seen-by-Employers).

62 Mann and O'Neil, above note 52.

63 O'Neil, above note 47 at 114.

highly surveilled and more at risk of criminalization.<sup>64</sup> Uneven patterns of policing spurred by algorithmic models can also expose marginalized populations to higher prison sentences where predictive sentencing models are used. Models that predict recidivism, for example, by assessing data, such as the first time a convicted person was ever involved with the police and whether their friends and relatives have criminal records, will tend to evaluate members of marginalized populations as greater risks, in large part as a function of the fact that discriminatory prejudices make members of those populations more likely to come into contact with the police<sup>65</sup> in the first place. In these cases, algorithmic models add a veneer of mathematical credibility that obfuscates discriminatory processes and outcomes.

The algorithmic sort sometimes also discriminates on the basis of prohibited grounds, such as gender and race, in the context of access to online information, advertising and pricing. Usually, however, the public is unaware of these discriminatory impacts unless and until they are revealed through research studies. For example, research by Latanya Sweeney demonstrated that Google and Reuters search tools were more likely to show advertisements for criminal record checks in relation to searches involving African-American-sounding names than white-sounding names.<sup>66</sup> Similarly, Cathy O’Neil demonstrated the disproportionate targeting of socio-economically disadvantaged persons with advertisements for private colleges associated with predatorily priced student loans.<sup>67</sup> ProPublica Research has documented numerous examples of discriminatory outcomes related to algorithmic sorting used for online target marketing. These include persons of Asian origin being twice as likely to pay a higher price for SAT prep tests because they are profiled as being Asian or live in certain zip codes,<sup>68</sup> and a Facebook ad

64 *Ibid* at 88–89.

65 For example, a recent study of policing practices in Ottawa showed that Middle Eastern and Black groups, irrespective of age and sex, were subject to disproportionately high incidences of traffic stops (at 2–3 times the rate of their representation in the total driving population): Lorne Foster, Les Jacobs, & Bobby Siu, “Race Data and Traffic Stops in Ottawa, 2013–2015: A Report on Ottawa and the Police Districts” (2016) *York University Research Team* 1 at 3 online: [www.ottawapolice.ca/en/about-us/resources/TSRDGP\\_York\\_Research\\_Report.pdf](http://www.ottawapolice.ca/en/about-us/resources/TSRDGP_York_Research_Report.pdf).

66 Latanya Sweeney, “Discrimination in Online Ad Delivery” (2013) 56:5 *Communications of the ACM* 44, online: [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2208240](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2208240).

67 O’Neil, above note 47 at 68–73.

68 Jeff Larson, Surya Mattu, & Julia Angwin, “Unintended Consequences of Geographic Targeting” *ProPublica* (2017), online: <https://static.propublica.org/projects/princeton-review/princeton-review-methodology.pdf>.

buying platform that enabled advertisers to target market to “Jew Haters” and to block a housing ad from being shown to African-Americans, Hispanics, and Asian-Americans.<sup>69</sup>

Whether or not intentional, these discriminatory outcomes of algorithmic sorting serve to undermine the vision of equality espoused thirty-five years ago when our *Charter* was entrenched. Perhaps more troublingly, in many instances humanly understandable explanations for machine-based decisions resulting from churning through unprecedented troughs of data often cannot be provided. Since these discriminatory outcomes can emanate from algorithms used both by government and corporations, accountability mechanisms for both public and private sector players will be essential to ensuring that the commitment to equality expressed in our Constitution continues to have meaning and effect. If not, we might expect to wake up one morning to technocratic admonitions to get over the fact that “equality is dead too.”

## 2) Terms of Service and Privacy Policies: Privacy, Free Expression, and Equality at Stake

In 1982, while freedom of expression was explicitly entrenched in section 2(b) of the *Charter*, privacy was not. Instead, privacy was implicitly protected through rights against unreasonable search and seizure in section 8 and protections for life, liberty, and security of the person in section 7. Some parliamentarians expressed concern about this choice, pressing for explicit inclusion of protections against “unreasonable interference with privacy, family, home and correspondence,”<sup>70</sup> and articulating viewpoints from Canadians that “government has become too large and that they want government off their backs.”<sup>71</sup> The Liberal Government’s position at the time was that sections 7 and 8, combined with the then-soon-to-be-enacted *Privacy Act* provided sufficient protection for Canadians’ privacy,<sup>72</sup> notwithstanding the opposition’s critique that constitutional entrenchment of privacy rights was essential to ensuring that they can never be eroded or taken away by an ordinary statute of the federal or provincial government.<sup>73</sup>

69 Julia Angwin, Madeleine Varner, & Ariana Tobin, “Machine Bias: Facebook Enabled Advertisers to Reach ‘Jew Haters’” *ProPublica* (14 September 2017), online: [www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters](http://www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters).

70 Joint Committee 1980–1981, above note 12 at 65 (Hon David Crombie).

71 *Ibid* at 66 (Hon Arthur Jacob Epp).

72 *Ibid* at 67 (Rt Hon Jean Chrétien).

73 *House of Commons Debates*, 32nd Parl, 1st Sess, No 6 (29 January 1981) at 6695 (Svend Robinson), online: [http://parl.canadiana.ca/view/oop.debates\\_](http://parl.canadiana.ca/view/oop.debates_)

Since that time, a substantial body of jurisprudence demonstrates both that freedom of expression is linked to the right to access information,<sup>74</sup> and that privacy, although not explicitly referred to in the *Charter*, is nonetheless protected by it (at least in relation to intrusion by government and its agents).<sup>75</sup> This includes constitutional protection of “informational privacy,” which the Supreme Court of Canada in *Dyment* described as “extremely important” in a “modern society” in order to protect personal autonomy and integrity.<sup>76</sup> Further, federal, provincial, and territorial privacy legislation offer privacy protections in relation to both public and private sector dealings with personal information about individuals.<sup>77</sup> While the federal privacy commissioner’s lack of enforcement power has consistently been questioned, jurisprudence interpreting and applying privacy legislation treats it as quasi-constitutional because privacy rights “play an essential role in a free and democratic society and embody key Canadian values.”<sup>78</sup> As with equality, decisions relating to free expression and privacy as articulated in the *Charter* and related legislation are typically deliberated upon and explained in public forums. Lengthy contested litigation, sometimes ending in the Supreme Court of Canada, has resulted in determinations about the breadth of free expression and privacy protection, as well as the parameters of each as they interact with each other.<sup>79</sup> These publicly contested battles to articulate and shape the parameters of constitutional protections for privacy and free expression stand in sharp contrast with private deliberations over expression and user data purportedly reserved to Internet service providers through standard form terms of service and privacy policies.

If in 1982 the government was seen to be the key threat to Canadians’ free expression and privacy, in 2017 that picture has become much more complicated. As digital connectivity becomes increasingly key to and

---

HOC3201\_06/819?r=0&s=1.

74 See, for example: *Ford v Quebec (Attorney General)*, [1988] 2 SCR 712 at 767.

75 *Hunter v Southam Inc.*, [1984] 2 SCR 145 at 159.

76 *R v Dyment*, [1988] 2 SCR 417 at para 22.

77 For an overview of privacy legislation in Canada, see: Office of the Privacy Commissioner of Canada, *Overview of Privacy Legislation in Canada* (Ottawa: Office of the Privacy Commissioner, 2014), online: [www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02\\_05\\_d\\_15/](http://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/).

78 See, for example: *Douez v Facebook, Inc.*, 2017 SCC 33 at para 58 [Douez].

79 With respect to conflicts between privacy and free expression, see for example: *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers Union, Local 401*, 2013 SCC 62. For an overview of some of the section 8 caselaw, see: Jane Bailey, “Framed by Section 8: Constitutional Protection of Privacy in Canada” (2008) 50:3 *Canadian Journal of Criminology and Criminal Justice* 279.

integrated within all aspects of Canadians' lives, the privately owned and operated platforms through which we connect have become essential services for functioning in modern society, with young Canadians in particular living seamlessly integrated "online/offline" lives.<sup>80</sup>

Further, the "data in exchange for services" model that underlies the Internet as we currently know it means information shed during every online transaction has become a form of currency with which we knowingly and sometimes unknowingly "buy" access to other information and services. In this economy of information, private sector surveillance is a business model and the documents associated with gaining access to online services and platforms are drafted to reflect those priorities, not only so that service providers can tailor *their* services to users, but so that they can sell users' data to other public<sup>81</sup> and private sector players who also seek to create aggregated profiles for marketing and other purposes.<sup>82</sup> Faced with having to accept these one-sided terms of service or go without access to platforms that are increasingly essential to daily life, many Canadians, especially young people, feel they have little choice but to click "I agree."<sup>83</sup>

As a result, unlike the public processes through which alleged limitations on constitutional and quasi-constitutional rights to free expression, equality, and privacy are exposed, the processes by which platforms make decisions affecting these rights are in most cases non-transparent and not subject to a requirement to give reasons. Privacy policies or privacy terms incorporated into terms of service to which users must explicitly agree (or are taken to agree by using the service itself) frequently use vague or ambiguous language about what data is being collected about users, whether and how it will be used, and by

---

80 For further discussion, see Valerie Steeves, "Young Canadians in a Wired World, Phase III: Life Online" (2014) at 2–4, online: MediaSmarts [http://mediasmarts.ca/sites/mediasmarts/files/pdfs/publication-report/full/YCWWIII\\_Life\\_Online\\_Full-Report.pdf](http://mediasmarts.ca/sites/mediasmarts/files/pdfs/publication-report/full/YCWWIII_Life_Online_Full-Report.pdf).

81 Governments, too, are consumers of this data, sometimes purchasing data from brokers, while at other times monitoring online fora owned and operated by private sector players for state surveillance purposes: Ulrik Ekman et al, *Ubiquitous Computing, Complexity and Culture* (New York: Routledge, 2015) at 119.

82 Schneier, above note 31 at 49–52.

83 Matthew Johnson et al, "To Share or Not to Share: How Teens Make Privacy Decisions about Photos on Social Media" (2017) at 36–37, online: MediaSmarts <http://mediasmarts.ca/sites/mediasmarts/files/publication-report/full/to-share-or-not-share.pdf>.



whom.<sup>84</sup> This undermines the efficacy of regulatory models that permit the collection, use, and disclosure of data *with consent* of the user because a lack of clear information makes it impossible for the user to consent in an informed way.<sup>85</sup> Moreover, as technology changes, the uses to which data can and will be put will continue to expand, and increasingly involve systems of machine-based learning, the underlying “reasoning” of which will be beyond human understanding.<sup>86</sup> In the interim, the little that users are able to discern about what is being done with their data often arises from breaking news leading to public scandals such as:

- the 2013 Yahoo data security leak estimated to have compromised the privacy of three billion email users;<sup>87</sup>
- the leaked documents that suggested Facebook had “offered advertisers the opportunity to target 6.4 million younger users . . . during moments of psychological vulnerability”;<sup>88</sup> and
- the revelation that Google’s search algorithm links the names of parties and witnesses to litigation prohibited from publication by court-ordered bans on online coverage.<sup>89</sup>

Terms of service also directly impact equality and free expression, two constitutional rights that have been subject to considerable jurisprudence, including in relation to working out the relationship between the two in contexts such as obscenity, child pornography, and hate speech.<sup>90</sup>

---

84 Joel Reidenberg et al, “Ambiguity in Privacy Policies and the Impact of Regulation” (2016) 45:52 *Journal of Legal Studies* S163, online: <http://ssrn.com/abstract=2715164>.

85 Eloise Gratton, “Beyond Consent-based Privacy Protection” Submission to the Office of the Privacy Commissioner of Canada (11 July 2016) at 3, online: [www.eloisegratton.com/files/sites/4/2016/07/Gratton\\_Beyond-Consent-based-Privacy-Protection\\_July2016.pdf](http://www.eloisegratton.com/files/sites/4/2016/07/Gratton_Beyond-Consent-based-Privacy-Protection_July2016.pdf).

86 Knight, above note 39.

87 Techworld Staff, “26 of the Most Infamous Data Breaches” *Techworld* (4 October 2017), online: [www.techworld.com/security/uks-most-infamous-data-breaches-3604586/](http://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/).

88 Nitasha Tiku, “Get Ready for the Next Big Privacy Backlash Against Facebook” *Wired* (21 May 2017), online: [www.wired.com/2017/05/welcome-next-phase-facebook-backlash/](http://www.wired.com/2017/05/welcome-next-phase-facebook-backlash/).

89 Andrew Duffy, “Google Is Linking Secret, Court-protected Names – Including Victim IDs – to Online Coverage” *Ottawa Citizen* (21 September 2017), online: <http://ottawacitizen.com/news/local-news/google-is-linking-secret-court-protected-names-including-victim-ids-to-online-coverage>.

90 For a discussion of some of the key cases relating to these issues, see: Jane Bailey, “Missing Privacy through Individuation: The Treatment of Privacy in the Canadian Case Law on Hate, Obscenity and Child Pornography” (2008) 31:1 *Dalhousie Law Journal* 55.

Many social media platforms, for example, outline community standards and/or rights and obligations of users with respect to online posting and activities, as well as providing mechanisms by which users can report alleged infringements of those standards.<sup>91</sup> A number also market themselves as defenders of democratic values, such as free expression and privacy.<sup>92</sup> While some offer more specific upfront information about what will be considered to fall outside of those standards,<sup>93</sup> the language in these documents still tends to reserve to the company full discretion for determination of the complaint and any consequences that will apply, without any concomitant obligation to explain the decision (or even to notify the reporting party that a decision has been made).<sup>94</sup> As a result, citizens are left with no explanation of the reasoning behind decisions that can fundamentally affect free expression and equality, such as whether or not to remove material alleged to be hateful or harassing. Further, some evidence suggests that users are becoming so frustrated with and concerned about the lack of transparency and apparent inconsistencies in responses that they don't even bother to engage with these services.<sup>95</sup> Failure to address hateful and threatening content has serious implications for equality, since women, girls, and members of the LG-BTQ and other marginalized communities are more at risk of this kind of targeting.<sup>96</sup>

---

91 For a helpful summary relating to Facebook, Instagram, Snapchat, and Twitter, see: Ottawa Coalition to End Violence Against Women and Purple Sisters, "Social Media Guides" (2016), online: [www.techwithoutviolence.ca/social-media-guides](http://www.techwithoutviolence.ca/social-media-guides) [OCTEVAW].

92 These include Twitter (see: Busch & Shepherd, above note 18 at 301), and Shopify (see: Darrell Etherington, "Shopify CEO Attempts to Defend Continued Hosting of Breitbart's Online Store" *Tech Crunch* (9 February 2017)), online: <https://techcrunch.com/2017/02/09/shopify-ceo-attempts-to-defend-continued-hosting-of-breitbart-online-store/>.

93 Facebook's Community Standards, for example, provide fairly specific descriptions about adult nudity and sexual activity, hate speech, and violence and graphic content considered to fall outside of their standards: "Community Standards" *Facebook* (2017), online: [www.facebook.com/communitystandards](http://www.facebook.com/communitystandards).

94 *Ibid*; OCTEVAW, above note 91.

95 Jane Bailey & Valerie Steeves, "Defamation Law in the Age of the Internet: Young People's Perspectives" (2017) at 53–54, online: Law Commission of Ontario [www.lco-cdo.org/wp-content/uploads/2017/07/DIA-Commissioned-Paper-eQuality.pdf](http://www.lco-cdo.org/wp-content/uploads/2017/07/DIA-Commissioned-Paper-eQuality.pdf); Suzanne Dunn, Julie Lalonde, & Jane Bailey, "Terms of Silence: Addressing Weaknesses in Corporate and Law Enforcement Responses to Cyberviolence against Girls" (2017) 10:2 *Girlhood Studies* 80 at 87–88.

96 *Ibid* at 85.

While it might be tempting to dismiss the sheltering of these kinds of decisions about fundamental rights and freedoms behind vague contractual language as simply an example of a property owner's right to make decisions about how their property is used, I would suggest that what is at stake in this context requires a markedly different approach, for at least two reasons. First, in some cases, these documents appear to supplant existing legal regulation,<sup>97</sup> so much so that even legal authorities may defer to them,<sup>98</sup> and young people may have the impression that service providers "are the law on their own platform."<sup>99</sup> Second, we are not dealing here with just any corporate player. As discussed above, an increasingly smaller number of large corporate players enjoy considerable power in relation to our exponentially growing economic, social, and cultural dependency on digitally networked technologies.<sup>100</sup> In these circumstances, they might more accurately be thought of as providers of essential public services that concomitantly ought to attract higher order public obligations and responsibilities, including those relating to accountability and transparency, particularly in relation to constitutionally enshrined rights and freedoms.<sup>101</sup>

## D. CONCLUSION: WHAT CAN BE DONE?

Even if we are disturbed by the prospect of non-transparent private decision making coming to reshape the parameters of fundamental constitutional rights and values, the complexity and enormity of the situation might lead us to conclude there is nothing we can do — it's out of our hands, beyond our ken. Notwithstanding a powerful corporate lobby that might like us to believe that, I want to suggest otherwise, starting with a principle and working toward some concrete proposals.

---

97 Busch & Shepherd, above note 18 at 306. For example, while terms of service reserve for service providers mass licences to copy, disseminate, use, reproduce, and remix user-generated content, users themselves can be subject to removal of their remixed content and even to legal liability for it: *Ibid* at 307–8.

98 For an instance in which police, in responding to a complaint of online fraud, appear to have deferred to the terms of service of Twitter, see: Dunn, Lalonde, & Bailey, above note 95 at 89–90.

99 Bailey & Steeves, above note 95 at 53.

100 Lever, above note 40.

101 For further discussion relating to service providers and human rights, see: Rikke Jorgensen & Anja Pedersen, "Online Service Providers as Human Right Arbiters" in Mariarosaria Taddeo & Luciano Floridi, eds, *The Responsibilities of Online Service Providers*, Law Governance and Technology Series Vol 31 (Cham, Switzerland: Springer, 2017), abstract online: [https://link.springer.com/chapter/10.1007/978-3-319-47852-4\\_10](https://link.springer.com/chapter/10.1007/978-3-319-47852-4_10).

In 2000, in the face of the socio-technical constitution spawned through emerging digitally networked communications, Lawrence Lessig advised that the market should be tested against the same constitutional values as government because:

Unless we do, or unless we learn how, the relevance of our constitutional tradition will fade. The importance of our commitment to fundamental values, through a self-consciously enacted constitution, will fade. We will miss the threat that this age presents to the liberties and values that we have inherited. The law of cyberspace will be how cyberspace codes it, but we will have lost our role in setting that law.<sup>102</sup>

Lessig's observations remain apt, almost two decades later, as we witness the profound, often invisible impact that corporations involved with digitally networked services and goods are having on our day-to-day existences, and our fundamental commitments to democratic rights and values, such as privacy, equality, free expression, transparency, and accountability. And yet, the process for ensuring market compliance with these rights and values is perhaps more daunting than ever, particularly as we descend into the territory of artificially intelligent decision making. While Winner would clearly have favoured public input and dialogue about the political implications of these technologies *before* they began to overlay a new socio-technical constitution on our way of life,<sup>103</sup> meaningful opportunities for dialogue and action are still available, if we have the courage to engage them. While there are many possibilities,<sup>104</sup> I have chosen to highlight below five principle and policy proposals that I believe could make a difference in efforts for those who may be interested in shoring up the commitments entrenched in the *Charter* thirty-five years ago.

First, recognize that while the *Charter* emanates from the very appropriate concern that rights against *government* interference are essential to democracy, substantive realization of those rights also requires the imposition of limits on certain kinds of *private* action, particularly in relation to private actors who enjoy concentrated forms of structural privilege and power. And collusion between government and private actors must also be taken seriously.

Second, ensure well-funded support for public engagement and education on these issues by:

---

102 Lawrence Lessig, "Code is Law: On Liberty in Cyberspace" *Harvard Magazine* (1 January 2000), online: <http://harvardmagazine.com/2000/01/code-is-law.html>.

103 Winner, above note 1 at 28–29 and 47.

104 For a much more comprehensive list, see: Schneier, above note 31 at 155–238.

1. engaging the public, including young people, directly in policy-making processes related to these matters;
2. supporting research and action by community organizations representing diverse constituencies with a stake in these issues;<sup>105</sup>
3. creating processes for dialogue relating to technological developments *before*, rather than only *after*, they happen, which will require establishing ongoing multi-stakeholder collaborative forums in which all participants are assured sufficient resources to participate on an equal footing with government and private sector actors; and
4. creating educational campaigns, both in schools and in public forums, focused on digital literacy, *not* from the perspective of how to protect ourselves from private and public sector practices inconsistent with our fundamental constitutional rights, but rather from the perspective of ensuring that everyone knows their rights, understands how corporate and government practices may be undermining them, and is given access to the tools to demand better.

Third, reform federal privacy legislation to:

1. ensure that the Office of the Privacy Commissioner of Canada (OPC) has meaningful investigatory *and* enforcement powers. This would enhance the OPC's ability to deal with governmental and private sector organizations in both reactive and proactive ways to, among other things, respond to privacy-violating practices, but also to insist on disclosure of information that allows for a better understanding of the processes through which these practices are carried out and decisions are made;<sup>106</sup>
2. move beyond consent-based approaches to privacy and engage regulatory models that impose actual limits on certain kinds of practices, particularly in relation to collection and use of data from young people for marketing purposes;<sup>107</sup> and

---

105 See, for example: OCTEVAW, above note 91; YWCA Canada, "Rights Guide for Girls, Young Women and Gender Nonconforming Youth" (2016), online: <http://ywcarrightsguide.ca>; Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC), "Privacy" (2017), online: <https://cippic.ca/en/privacy>.

106 The *General Data Protection Regulation* that will come into effect in 2018 provides some useful mechanisms in this regard, including art 22, which requires that an explanation be made available in relation to machine-based decisions in certain kinds of cases: EC, *General Data Protection Regulation* [coming into force 25 May 2018], art 22, online: <https://gdpr-info.eu/art-22-gdpr/> [GDPR].

107 In the US, the *Children's Online Privacy Protection Act* and the rule promulgated pursuant to it require commercial websites and online services (including mobile apps) to obtain parental consent before collecting personal information from children

3. impose reporting requirements on service providers, to the extent that they are vested with any further decision-making powers resulting from creation of additional user rights, such as a right to request the de-linking of information about them from search engine results where access to that information is no longer in the public interest,<sup>108</sup> a right that may be particularly important for young people, given growing evidence about the potential impact of data about them on their health and well-being both now and in the future.<sup>109</sup>

Fourth, remember that although litigation is a reactive, rather than proactive strategy that is expensive and often slow to produce results, it still has a role to play, as do the courts in imbuing constitutional values not only into cases involving government, but in private litigation as well. Recently, for example, the Supreme Court of Canada in *Douez v Facebook Inc* rejected a bid by Facebook to oust the jurisdiction of the British Columbia courts to determine a class action proceeding alleging that Facebook had violated the privacy rights of its users in British Columbia.<sup>110</sup> The Court found that, among other things, “[t]he grossly uneven bargaining power between the parties and the importance of adjudicating quasi-constitutional privacy rights in the province” were compelling reasons for not enforcing the forum selection clause in Facebook’s

---

under the age of thirteen: Federal Trade Commission, “Complying with COPPA: Frequently Asked Questions” (March 2017), online: [www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions](http://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions). In addition, California prohibits advertisers from marketing certain products and services to minors: Wesley Campbell, “But It’s Written In Pen: The Constitutionality of California’s Internet Eraser Law” (2015) 48 *Columbia Journal of Law and Social Problems* 584.

- 108 Article 12 of the EC’s 1995 *Data Protection Directive* allows data subjects to request “rectification, erasure or blocking of data” because it is incomplete or inaccurate: European Commission, “Factsheet on the ‘Right to be Forgotten’ Ruling” (2014), online: [http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet\\_data\\_protection\\_en.pdf](http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf). Article 17 of the *GDPR*, above note 106 [coming into force in 2018] will expand that right to include situations where the data is no longer relevant to the original purposes for processing, but will require service providers to also consider the public interest in availability of the data in reaching a determination: European Commission, “GDPR Key Changes” (2017), online: [www.eugdpr.org/key-changes.html](http://www.eugdpr.org/key-changes.html). California’s “Internet eraser law” allows minors to request website operators to erase content they have posted on the website: Campbell, above note 107.
- 109 For further discussion, see: Bailey & Steeves, above note 95 at 32–45; Jane Bailey, “A Perfect Storm: How the Online Environment, Social Norms and Law Constrain Girls’ Online Lives” in Jane Bailey & Valerie Steeves, eds, *eGirls, eCitizens* (Ottawa: University of Ottawa Press, 2015).

110 *Douez*, above note 78.

standard form terms of service, which would otherwise have required the matter to be litigated in California.<sup>111</sup>

Fifth, imbue greater public accountability into decisions relating to online content removal by:

1. requiring service providers to issue public reports that provide clearer information about the standards used, the number of complaints received, the number of complaints resulting in administrative action, and the kinds of actions taken, without disclosing information that would compromise the privacy of specific parties involved in complaints; and/or
2. creating, expanding, and/or reinstating<sup>112</sup> *public* administrative mechanisms to resolve complaints relating to online content in a fast, cost-effective, and publicly accountable way. Existing models include regulatory bodies in Manitoba and Nova Scotia set up to assist targets of non-consensual distribution of intimate images in getting their images removed or deleted.<sup>113</sup>

The repatriation of Canada's Constitution involved the blood, sweat, and tears of many people, polities, and organizations, not all of whom were pleased with or respected the outcome. However imperfect the result, the process was a public one and its outcome one of many milestones in a continuing drive to realize democracy and justice. Surely Canadians didn't spend fifty years retrieving control over our democratic vision from one unelected monarch only to let it slide into the hands of another.

---

<sup>111</sup> *Ibid* at para 4.

<sup>112</sup> For example, the *Canadian Human Rights Act* could be amended to reinstate section 13, which previously provided a human rights-based mechanism for resolution of complaints relating to online hate propagation: Jane Bailey, "Canadian Legal Approaches to 'Cyberbullying' and Cyberviolence: An Overview," Ottawa Faculty of Law Working Paper No 2016-37 (2016) at 9, online: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2841413](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2841413).

<sup>113</sup> *Ibid* at 40.