Submissions on Bill C-27
The Digital Charter Implementation Act
Submitted by Jane Bailey,[1] Jacquelyn Burkell,[2] and Brenda McPhail[3]

OVERVIEW

These submissions respond to Parliament's referral of Bill C-27, *The Digital Charter Implementation Act* to the Standing Committee on Industry and Technology in April 2023. Our submissions are based on decades of academic and policy work relating to privacy and equality in digitally networked environments, including local, national, and international policy interventions and research.

We share concerns about numerous aspects of Bill C-27 that have been identified in other submissions, including those of the Canadian Civil Liberties Association, the Women's Legal Education and Action Fund (LEAF), PIAC, Open Media, The Office of the Privacy Commissioner of Canada (OPC), and UNICEF Canada. We add to these submissions by focusing on the connection between privacy and equality, identifying the implications of personal data collection, use, and disclosure for individual and collective rights, discussing the limitations of individual informed consent in light of those considerations, and proposing related changes to Bill C-27.

We submit that:

(1) **Individual *and* collective rights are in jeopardy, and both privacy *and* equality are at stake** – the collection, use, and disclosure of data about individuals undermine individual and collective privacy, and also lie at the heart of concerning discriminatory outcomes for individuals and for groups that are associated with our current algorithmically sorted society.

(2) **Individual informed consent is necessary but not sufficient for the protection of privacy and equality rights** A robust individual informed consent model (IICM) is important as a response to some of the privacy challenges posed to individuals, but the IICM is not sufficient to address collective privacy and equality concerns. Other measures must be taken to address these issues.

(3) **Bill C-27 must be amended to strengthen its consent-related provisions** Bill C-27 centres individual consent as the lynchpin for protecting privacy, while simultaneously weakening the IICM by nominally positioning privacy as a human right in the preamble, but substantively treating it as commercial matter to be balanced against corporate interests. The Bill must be amended to remove provisions that undermine individual informed consent.

(4) **Bill C-27 must be amended to address situations where the IICM is insufficient because more than individual rights are at stake** The IICM is insufficient to address the collective privacy and equality concerns raised by the collection, use, and disclosure of personal data. Regulating AI is one approach to addressing these concerns. However, as detailed in LEAF's submissions (which we endorse), the limited and vague regulatory system relating to AI that is currently proposed will not be enough to address the related privacy and equality rights at stake.

---

[1] Full Professor, University of Ottawa Faculty of Law (Common Law Section), Working Group Leader and Co-Investigator on The Autonomy Through Cyberjustice Technologies Project (uMontréal), Co-Leader of The eQuality Project (uOttawa).
[2] Associate Vice-President Research & Full Professor Faculty of Information and Media Studies (Western University), Working Group Leader and Co-Investigator on The Autonomy Through Cyberjustice Technologies Project (uMontréal), Co-Investigator on The eQuality Project (uOttawa).
[3] PhD, Acting Executive Director, Masters in Public Policy in Digital Society McMaster University, Director of the Canadian Civil Liberties Association's Privacy, Surveillance, and Technology Project (on leave).

In light of these submissions, we call on the government to commit to public consultation and ongoing review:

(a) *convene and/or fund deep public consultation, awareness-raising and facilitated dialogue* to engage the public in discussion about the widespread democratic, systemic, and human rights implications of technological advancements like AI and the limitations of primary reliance on transactional individual decision-making models for protecting those rights;
(b) *thoroughly assess and address the impacts of the specific deficits identified in this submission and others, and amend Bill C-27 accordingly*; and
(c) *review within 5 years of their coming into force all legislative changes pursuant to Bill C-27 in light of the public consultations and assessment noted above, and publicly report upon that review***.**

1. Individual *and* collective rights are in jeopardy: both privacy *and* equality are at stake.

Privacy has long been recognized as a fundamental underpinning of any democratic society committed to individual dignity, autonomy, and self-determination. It has also been described as a producer of common, public, and collective goods by, among other things, contributing to diversity, tolerance, and pluralism, and supporting democratic processes by enabling individuals to live up to their social responsibilities and more meaningfully participate in public processes (e.g., voting).[4]

Privacy is also a "gateway right" that enables or reinforces other rights, including equality.[5] Indeed, where the collection, use, and disclosure of personal data is concerned, privacy is inexorably connected to equality -- and that connection has critical implications for privacy-focused legislative initiatives such as those included in Bill C-27. When adequate privacy protections are in place with respect to the collection, use and disclosure of personal data, equality rights that are threatened by excessive, unfair, or discriminatory uses of that data stand also to benefit from those protections. By contrast, where privacy protections fail to appropriately limit the collection, use, and disclosure of personal data, those data have the potential to be used in ways that undermine equality rights. The case of a First Nations man in a BC Canadian Tire store flagged as a shoplifter based on inaccurate facial recognition results is a case in point.[6] The racial profiling experienced by this individual was possible only because the retailer was using facial recognition technology, and their use of the technology was, according to the BC Information and Privacy Commissioner, in violation of BC privacy laws.[7] But for the privacy-violating collection and processing of personal data, the equality harm could not have occurred.

Further, privacy risks are inequitably distributed, and members of marginalized communities are in many cases more likely to be subject to the collection, use, and disclosure of personal data that can lead to additional equality harms. Thus, for example, the police practice of 'carding' based on racial profiling disproportionately exposes black, Indigenous, and other racialized individuals to collection of personal data which then becomes part of police databases. The result is equality harms for the targeted individuals and for the communities of which they are part. Individuals are subject to heightened police scrutiny, criminal litigation, and incarceration, and the consequences for communities include negative

---

[4] Priscilla M. Regan, Legislating Privacy: Technology, Social Values and Public Policy (Chapel Hill: University of North Carolina Press, 1995) at 220-226.
[5] Canadian Civil Liberties Association, online: https://ccla.org/our-work/privacy/.
[6] Austin Grabish, "First Nations man wants apology after being flagged as a shoplifter, asked to leave Canadian Tire store" CBC News (19 October 2022), online: https://www.cbc.ca/news/canada/manitoba/first-nation-apology-store-accused-1.6620457.
[7] *Canadian Tire Associate Dealers' use of facial recognition technology*, Investigation Report 23-02, Office of the Information and Privacy Commissioner of British Columbia, online: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.oipc.bc.ca/investigation-reports/3785.

impacts on dignity, financial well-being, and health, as well as renewed cycles of poverty.[8] Although this and many other relevant examples pertain to public sector activities, they are nonetheless important in the context of discussions of private sector regulation such as that proposed in Bill C-27 given that public sector bodies are increasingly accessing private sector data[9] and leveraging AI tools created by the private sector and trained on private and/or open data in public sector applications.[10]

The surveillance capitalist structure of our digitally networked environment escalates the urgency of recognizing the privacy-equality connection and responding with meaningful legislative interventions that protect the rights, both individual and collective, that are at stake. The massive data grab that characterizes the digital environment in which we are all increasingly immersed converts data -- highly intimate as well as those that are apparently innocuous -- about virtually all our social, economic, political, cultural, and (increasingly) legal interactions into profiles. These profiles are used to make decisions about us as individuals – and those same profiles deeply and silently embed harmful stereotypes into every aspect of our lives, including our perceptions of ourselves and others.[11] The deployment of AI models trained on troves of personal data escalates the risk of equality-undermining outcomes such as selective targeting of teen girls with content harmful to body image and mental health,[12] perpetuation of discriminatory stereotypes in search engine results,[13] and algorithmic 'supercharging' of the spread of content harmful to equality-deserving groups.[14] Such outcomes result from a self-reinforcing process whereby technology companies seek to maximize profit by collecting and using personal information in part to maximize user engagement, in turn generating further data that can then be used for additional targeting.[15]

The algorithmic processes that produce these results are far from transparent and are often beyond human comprehension even if they were to be revealed. Moreover, these processes produce outcomes that are usually not even recognized until well after the damage has been done. Even more troubling,

---

[8] Kate Robertson, Cynthia Khoo, and Yolanda Song, "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada" (September 2020), Citizen Lab and International Human Rights Program, University of Toronto at 15-18.
[9] Ira Rubinstein, Gregory T. Nojeim and Ronald D. Lee, "Systematic Government Access to Private-Sector Data: A Comparative Analysis" in Fred H. Cate and James X. Dempsey (eds) *Bulk Collection: Systematic Government Access to Private Sector Data* (Oxford Academic Press: New York, 2017) 5-46.
[10] For example: Office of the Privacy Commissioner of Canada, "RCMP's use of Clearview AI's facial recognition technology violated *Privacy Act*, investigation concludes" News Release (10 June 2021), online: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/nr-c_210610/.
[11] Oscar H. Gandy Jr., The Panoptic Sort: A Political Economy of Personal Information (Boulder, CO: Westview Press, 1993); Shoshana Zuboff, The Age of Surveillance Capitalism (London, England: Profile Books, 2019).
[12] Will Oremus, "Facebook keeps researching its own harms – and burying the findings" The Washington Post (16 September 2021), online: https://www.washingtonpost.com/technology/2021/09/16/facebook-files-internal-research-harms/.
[13] Sweeney's study showed that Google Adsense was 25% more likely to deliver an ad suggestive of a criminal record on a search of a black-identifying name than a white-identifying name: Latanya Sweeney, "Discrimination in Online Ad Delivery" (28 Jan 2013), online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2208240. Noble's analysis revealed that the top responses to a Google search on the term "black girls" were far more likely to be sexually explicit terms and links to porn sites than searches on the term "white girls": Safiya Umoja Noble, Algorithms of Oppression (NYU Press, 2018), see: https://nyupress.org/9781479837243/algorithms-of-oppression/.
[14] Amnesty International, "Myanmar: Facebook's Systems Promoted Violence Against Rohingya; Meta Owes Reparations" (29 September 2022), online: https://www.amnesty.org/en/latest/news/2022/09/myanmar-facebooks-systems-promoted-violence-against-rohingya-meta-owes-reparations-new-report/.
[15] Karen Hao, "The Facebook whistleblower says its algorithms are dangerous. Here's why." MIT Technology Review (5 October 2021), online: https://www.technologyreview.com/2021/10/05/1036519/facebook-whistleblower-frances-haugen-algorithms/.

their justifiability is sometimes made to seem beyond question because of the veneer of mathematical and scientific certainty in which they are coated.[16]

Legislative reform is clearly needed to address the privacy and equality concerns at stake. Bill C-27 offers some prospects for improvement over the current situation in certain areas. However, it falls short of meaningfully addressing the grave potential human rights consequences at issue by relying primarily on the IICM, while at the same time limiting its efficacy. This undermines C-27's ability to meaningfully address issues at the juncture of privacy and equality, such as group and community privacy and social sorting facilitated by big data and AI.

Because both individual and collective rights are at stake, implicating both privacy and equality, we submit that two things are needed: (i) strengthen the consent related provisions in Bill C-27 (for those situations in which the IICM is appropriate); and (ii) amend Bill C-27 to meaningfully address situations where significant overlaps between privacy and equality limit the IICM's protective capacity.

2. **Robust individual informed consent is necessary but not sufficient**

Obtaining an individual's consent to collect, use and disclose their data is a critical way to show respect for that individual's agency, dignity, self-autonomy and right to make decisions affecting their own life.[17] This measure remains important. However, we must also recognize limitations in the capacity of the IICM to meaningfully protect privacy, and equality in a digitally networked and algorithmically sorted environment where individuals have little choice but to click "I agree" in order to access services that affect every part of their lives from education to employment to social services and basic communication.

Considerable scholarship and analysis has questioned the legitimacy and efficacy of the IICM in numerous contexts, including consumer transactions,[18] sexual assault,[19] and privacy.[20] Two of the primary concerns articulated in those critiques are particularly relevant in the context of Bill C-27: (1) the timing and complexity of data use can make it difficult to ensure that individuals fully understand the nature, extent and consequences of their consent; and (2) one consenting individual's decision can have serious effects on the rights of other individuals, and on the rights of groups of individuals whose consent has neither been requested nor obtained.

The challenges to the efficacy of the IICM fall into five non-mutually exclusive areas to which we have attached the following plain language labels:

[16] Jane Bailey, Jacquelyn Burkell, and Valerie Steeves. (2020) "AI technologies-like police facial recognition – discriminate against people of colour" The Conversation. Retrieved 18 September 2020 from https://theconversation.com/ai-technologies-like-police-facial-recognition-discriminate-against-people-of-colour-143227.
[17] Joana Varon & Paz Peña, "Consent to our Data Bodies: Lessons from Feminist Theories to Enforce Data Protection" (2019) online: Association for Progressive Communications <https://codingrights.org/docs/ConsentToOurDataBodies.pdf>.
[18] Marina Pavlovic, "Consumer rights in a radically different marketplace" (4 June 2018), online: Policy Options <https://policyoptions.irpp.org/magazines/june-2018/consumer-rights-radically-different-marketplace>.
[19] Susan J. Brison, "Beyond Consent" in Lori Watson, Clare Chambers & Brian D Earp, eds, The Routledge Handbook of Philosophy of Sex and Sexuality, 1st ed (New York: Routledge, 2022).
[20] Daniel J. Solove, "Introduction: Privacy Self-Management and the Consent Dilemma" (2013) 126 Harv L Rev 1880.

(1) *Now for later* – asking individuals in advance for consent to collect and use their data later is problematic because future uses of one's data can be very difficult to predict at the time consent is requested, especially in an environment of fast-moving socio-technological change;[21]

(2) *This implicating that* – individuals may be asked to consent to collection and use of certain data, without being told or at least without appreciating that other information about them may be revealed by disclosure of the original data. Data aggregation and analytic practices bring together individually-consented-to pieces of data in ways that can be used to accurately predict information about that individual that they did not consent to releasing, such as age, sexual orientation, and political affiliation.[22] The predictive categories generated can then be used as a basis for, among other things, discrimination against that individual;[23]

(3) *Affecting other individuals* – consensually collected data from one individual can also reveal data about other individuals from whom consent was not sought. For example, a person posting a photo online may consent to collection and use of that photo and any personal data relating to it, including information revealed about other individual(s) depicted in the photo. Further, technological advancements such as facial recognition technology[24] and forensic genealogy[25] can deepen the potential or actual violation of the privacy of non-consenting individuals by revealing increasingly personal information about them, including their identity;

(4) *Affecting an identifiable group* – data collected with an individual's consent (e.g., genetic information) can be grouped together with data consensually collected from multiple other individuals to generate inferences about a group of people all of whom share a particular characteristic historically used as a basis for categorization and discrimination (e.g. race, gender, etc.).[26] Such categorization can contribute to stereotypes about and discrimination against that group and its individual members, with collective equality-violating effects of concern to society at large;[27] and

(5) *Affecting a new algorithmically created group* – data consensually collected from multiple individuals can be used to generate inferences about a group of people all of whom share a particular profile, and it may be that each piece of data used comes with no prior known history of being used as a

---

[21] Tuukka Lehtiniemi & Yki Kortesniemi, "Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach" (2017) 4:2 Big Data & Society 1 at 3; Daniel J Solove, "Introduction: Privacy Self-Management and the Consent Dilemma" (2013) 126:7 Harv L Rev 1880; Custers, Bart, "Click here to consent forever: Expiry dates for informed consent" (2016) 3:1 Big Data & Society 1.

[22] Rob Kitchin, The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences (California: Sage Publications Ltd, 2014) at 40; Michal Kosinski, David Stillwell & Thore Graepel, "Private traits and attributes are predictable from digital records of human behavior" (2013) 110:15 Proceedings National Academy Sciences 5802; John Gordon, "When Should Data-Processing Agents Be Allowed to Collect Our Personal Information? The Case against Reliance on Individuals' Consent in the Age of Big Data" (2020) 2:1 Studies in Philosophy, Politics and Economics 55.

[23] Kosinski, Stillwell & Graepel, supra note 22.

[24] Aletta Norval & Elpida Prasopoulou, "Public faces? A critical exploration of the diffusion of face recognition technologies in online social networks" (2017) 19:4 New Media & Society 637.

[25] Thomas J White & Steven B Lee, "Forensic Genetics, Ethics, Privacy, and Public Policy" in Henry Erlich (ed) Silent Witness: Forensic DNA Evidence in Criminal Investigations and Humanitarian Disasters (Oxford: Oxford University Press, 2020).

[26] Taylor, Linnet, Luciano Floridi & Bart van der Sloot, Group Privacy: New Challenges of Data Technologies, (Switzerland: Springer International Publishing, 2017); Michele Loi & Markus Christen, "Two Concepts of Group Privacy" (2020) 33 Philosophy & Technology 207 at 210.

[27] Loi & Christen, *supra* note 26.

basis for categorization or discrimination.[28] Those data, however, in combination using a particular AI model, could become the basis for new and concerning forms of stereotyping and discrimination[29] such as bestowing unfair advantages or disadvantages on the group and/or its members, once again raising important privacy and equality concerns for society at large.

The first two of these concerns could potentially be addressed through a strong individual informed consent model. The remaining three, however, raise privacy and equality rights that cannot be addressed through individual informed consent, and these require different protective approaches and mechanisms.

3. Amend Bill C-27 to strengthen its consent-related provisions

Parts 1 and 2 of Bill C-27 (the *Consumer Privacy Protection Act* (CPPA) and the *Personal Information and Data Protection Tribunal Act*, respectively) deal primarily with framework matters (1) *now for later* and (2) *this implicating that* by, among other things:

- setting out parameters for obtaining individual consent (ss. 12-17);
- listing exceptions to the consent requirement (ss. 18-51);
- creating an individual right to request disposal (s. 55);
- entitling individuals to receive notice of security breaches (s. 57);
- creating a right to access and request amendments to PI held by an organization (s. 63);
- creating an individual right to an explanation of automated decision-making systems' predictions, recommendations, or decisions with significant impact on the individual (s. 63(3));
- setting out requirements relating to de-identification of information relating to an individual and limiting use of de-identified information to re-identify an individual (s. 75);
- setting out a privacy-complaints process (s. 82); and
- creating an individual private right of action (s. 107).

Overall, even though aspects of Parts 1 and 2 are premised on sound ideas for protecting individual privacy (e.g., by allowing individuals recourse in relation to violative practices), they fall short in numerous ways that undo much of the privacy-protective work done by other provisions. The following 7 categories of concern, many of which are also mentioned above, are framed here in the context of an argument for the necessary amendments which follow.

1. Privacy as a Human Right[30]

Recognizing privacy as a human right in Canadian law generally, and in Bill C-27 in particular, is not just important in principle, but also has practical implications for providing adequate protections for personal information in the big data world where, as we've argued above, informed consent is increasingly challenged. The European General Data Protection Regulation (GDPR) has been able to judiciously introduce alternative grounds for processing personal information, in lieu of consent, because that law explicitly balances business interests against a recognized right to privacy. A right necessarily weighs more heavily in the balance than an "interest" or "expectation" as it is not something an

[28] Brent Mittelstadt, "From Individual to Group Privacy in Big Data Analytics" (2017) 30 Philosophy and Technology 475 at 488; Sandra Wachter & Brent Mittelstadt, "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI" (2019) 2019:2 Colum Bus L Rev 1.
[29] Oscar H. Gandy Jr., "Exploring Identity and Identification in Cyberspace" (7 June 2000), online: Annenberg School for Communication, University of Pennsylvania <http://www.asc.upenn.edu/usr/ogandy/Identity.pdf>.
[30] Some of these points were developed in unpublished material produced by McPhail in her former role of Privacy Director at CCLA.

individual may legitimately be asked to trade away, whether for convenience or profit. A right sets the correct threshold conditions for reasonable protection in the face of increasing motivations for data collection and monetization across a wide range of sectors. Recognizing a right to privacy is also a recognition that many of our other rights, including rights of free expression and equality, hinge in many cases on an ability to maintain a degree of privacy while engaging in the transactions of everyday life.

Like the GDPR, Bill C-27 also seeks to introduce exceptions to the requirement for meaningful consent, but the Bill fails to appropriately prioritize human rights because, as per the title of the *CPPA*, its purpose is "to support and promote electronic commerce by protecting personal information" rather than "to ensure that the fundamental human right to privacy is respected by protecting personal information that is collected, used or disclosed in the course of commercial activities." Revising the preamble and enactment of provisions to more firmly position privacy as a fundamental human right and a priority rather than one of many interests to be balanced would begin to address this gap.

2. **De-identified and anonymized information**

De-identified information is information derived from and about individuals, and it is increasingly used in ways that have consequential impacts on individuals and groups whether or not any one data point can be linked directly to an individual. As such, it is important that such information has appropriate legal protections. Bill C-27 offers a significant improvement over *PIPEDA* in appropriately bringing de-identified information explicitly into the scope of the law. However, the definition of de-identified information in C-27 has been watered down from the former Bill C-11 in such a way as to require only the removal of direct identifiers without addressing indirect identifiers, rendering questionable the ostensible protective value of the processes that conform to that definition. The definition now more closely aligns to the concept of "pseudonymization" as it is defined in the GDPR. Further, there are a series of exceptions to the principle that de-identified information is personal information and covered in the *CPPA*, itemized in s. 2(3), which further erode protections for individuals.

A new category of Information, anonymized information, is introduced in Bill C-27 and then promptly removed from the scope of the Act. It must be recognized that true anonymization is notoriously difficult, and there is even debate as to whether it is even possible in all cases. Taking anonymized data out of the scope of the law (in contrast to the approach in Quebec's new privacy law) means that there is no regulatory oversight to determine the effectiveness of anonymization, re-introducing the problem we had under PIPEDA. In Bill C-27, anonymization is also, in *CPPA* s. 2(1), allowed to stand as equivalent to disposal, which renders illusory the right of individuals' rights to ask for deletion of their information. That equivalency should be removed. It must also be recognized that even fully effective anonymization of personal data in no way addresses the collective privacy and equality rights concerns that are raised in this submission, as these arise in many cases from algorithmic processing of personal (even if anonymized) information to create profiles that when used to categorize or target groups or individuals create new privacy and equality threats. For these reasons, all personal data and data derived from personal data, whether identifiable, de-identified, or anonymized, should be within the scope of the law and subject to oversight by the OPC.

3. **Appropriate Purpose**

CPPA s. 12(2) itemizes the factors to consider when deciding whether a collection, use or disclosure of information is accomplished in a manner and for a purpose which a reasonable person would consider appropriate in the circumstances. The final factor in the list is (e) whether the individual's loss of privacy is proportionate to the benefits in light of the measures, technical or otherwise, implemented by the

organization to mitigate the impacts of the loss of privacy on the individual. This may be a useful factor to help assess whether, for example, a disclosure of de-identified data (de-identification being a technical measure to mitigate privacy loss) is or is not appropriate -- but in the drafting language, it is not clear whether the proportionality equation measures benefits to individuals or to the organization making the decisions impacting the individual, and the latter interpretation inappropriately allows the organization to decide if the benefits to them outweigh the loss of privacy of an individual.

New or changing use for collected information is also at issue. *CPPA* s. 12(4) allows organizations to decide to use or disclose information collected for one purpose for another purpose simply by recording the new purpose, presumably in their privacy policy. This is significantly weaker than under *PIPEDA* in Schedule 1, s. 4.2.4, which requires specific consent for a new use of collected information unless that purpose is required by law.

While this is a feature business actors certainly desire in the age of big data, where new uses for old information often emerge, it also renders relatively meaningless the requirements for purpose specification to consumers—they will be told, if they check out the privacy policy, what uses of their information can be expected at the time they share it, but have no guarantee that promise will hold in the future. How many people go back to see if policies change a year or two after doing business with a company? Despite the limited protection provided by *CPPA* s. 13, which allows collection of only the information necessary for the originally recorded purposes, allowing new purposes unconstrained by any limitation as to the nature of such purposes opens the door to a bait and switch approach to data collection. At minimum, constraints are necessary, such as a requirement that any new purpose for using personal information unknown and unspecified at the time of the original consent should be consistent with the original purpose for which they shared their information, and that organizations must proactively flag changes to their policies where new purposes for previously collected information have been recorded.

4. **Explicit Consent**

In recognition of the range of issues with consent as the sole grounds for information processing as discussed at length above, a compromise, attempted in the GDPR and partially and poorly mimicked in Bill C-27, is to carve out exemptions from consent for certain kinds of legitimate business and public interest purposes. Some holes created in the consent regime in former Bill C-11 have been removed, but significant issues remain with the revised consent regime and the exceptions in Bill C-27.

Under *PIPEDA* s. 6(1) for consent to be valid, it must be "reasonable to expect that an individual to whom the organization's activities are directed *would understand* the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting" (emphasis added). Bill C-27 removes this language of "understanding", and instead identifies the information that must be provided and, in *CPPA* s. 15(4), affirms the need for plain language privacy policies. The new framing subtly lowers the bar for "meaningful" consent by focusing on the information provided rather than on the necessity to strive for understanding. This opens the door for companies to argue that so long as the requisite information is provided in short words, they have met the threshold for valid consent.

5. **Implied Consent**

The GDPR, to balance the presence of exceptions which increase the scope of consent-free collection, requires explicit consent for those collections where consent is the basis upon which information is collected, used, or disclosed. *CPPA* s. 15(5), in contrast, provides for implied consent to be assumed

under circumstances where it is "appropriate" after "taking into the account the reasonable expectations of the individual and the sensitivity of the personal information that is to be collected, used or disclosed." This is consistent with *PIPEDA*, but there is a significant difference between that law and the new Bill, because C-27 also introduces GDPR-like exceptions for some business and public interest purposes. Allowing implicit consent alongside the business and public interest exceptions in C-27 creates a certain degree of confusion and some very muddy ground for consumers and businesses alike—particularly since *CPPA* s. 15(6) clarifies that implicit consent is not a legitimate form of consent for the exempt business activities itemized in s. 18(2) or (3), despite those activities requiring neither knowledge nor consent from consumers to allow information to be collected. If that sounds confusing, it is simply a reflection of the confusion introduced in the text of the Bill. If consent is to be only one of several grounds for information collection in the new law, then it should always and only be explicit.

6. **Exceptions to Consent**

As noted above, C-27 introduces two categories of exceptions to the consent requirements for information collection, use and disclosure: business activities and public interest activities.

a) Business Activities

CPPA s. 18(3) adds a legitimate business interest exception that specifies:

> An organization may collect or use an individual's personal information without their knowledge or consent if the collection or use is made for the purpose of an activity in which the organization has a legitimate interest that outweighs any potential adverse effect on the individual resulting from that collection or use and
>
> a. a reasonable person would expect the collection or use for such an activity; and
> b. the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions.

This is a dangerously permissive exception that allows the organization making the decision to determine whether their interest outweighs adverse effects on the individual. The individual in question may never have enough information about that collection (remember, collection can happen without "without knowledge or consent" in many circumstances) to understand what's going on or whether those decisions are being made fairly. In our complaint-based system, where the regulator relies strongly on individual complaints to identify unfair practices, this provision leaves individuals unaware and undermines the regulator. It is unclear whether the requirements for privacy management programs will be sufficiently detailed, or that the OPC will be sufficiently resourced, to ensure that such decision processes, made on an ongoing basis, would be caught in a review of those programs.

The exception in *CPPA* s. 18(3) extends beyond reasonably removing the consent requirement for an expected collection necessary for providing a product or service a customer wants and has asked for, to collections and uses of information for organizational purposes that are not required to be of any benefit to the consumer whatsoever, without their knowledge. This is a step too far, privileging businesses at the expense of their customers' privacy for any reason related to a legitimate interest, as assessed by the business itself, without any certainty that assessment of legitimacy will ever be subject to regulatory or public scrutiny and without a commitment to a fundamental right to privacy.

b) Socially beneficial purposes

Bill C-27 responds to the real need for some private sector data to be made accessible to governments and used for the public interest. However, it does so in a way that is not fit for purpose if one of the goals is to ensure public trust in the sharing and use of information between the private sector and government. What is in the public interest may be a matter of debate subject to the vagaries of politics and potentially turbulent national/global contexts, as we have seen all too often during the pandemic.

There is no principled reason why de-identified information should be categorized as personal information in other circumstances but not when government wants it, even if for a good reason. De-identified information is derived from personal information, and by definition carries a risk of re-identification, and therefore must remain in the scope of the Act as personal information. It should not simply carry the accountability and transparency requirements attached to de-identified data generally in the Act, but actually warrants *enhanced* requirements to promote public trust.

Additional safeguards are necessary to mitigate these risks to public trust and personal privacy for the use of de-identified data. These include engagement by the regulator, and additional constraints and required analyses and disclosures, identified in the recommendations below, in order to appropriately facilitate the sharing of information for socially beneficial purposes in a manner that Canadians can trust and support.

7. Automated decision making

Bill C-11 introduced the right to be informed regarding the nature of automated decision systems to make a prediction, recommendation, or decision about an individual and Bill C-27 also includes this provision, slightly modified. In *CPPA* s. 63(3) the right is limited to systems that could have a significant impact on an individual, although it fails to define what a "significant" impact might be. It also fails to provide any recourse, beyond an explanation, for the use of automated decision systems. This falls well short of the standard set by Art 22 of the GDPR, which provides that a "data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[31] An option to request reconsideration of a recommendation or decision made by an automated system by a human decision-maker would go some way toward addressing this shortcoming in Bill C-27.

3. Amend Bill C-27 to address those situations where the IICM falls short because more than individual rights are at stake.

Aspects of Parts 1 and 2 of Bill C-27 could also be seen as beginning the work of addressing collective privacy and equality concerns. For example, new restrictions relating to the collection, use and disclosure of children's data, if revised as per UNICEF Canada's submissions, could enhance privacy protection for members of this group. *CPPA* requirements related to automated decision-making that impose openness and transparency requirements where systems are used for purposes of recommendations, decisions and predictions that can significantly affect individuals (s. 62) and creation of individual rights to request disposal (s. 55) and to obtain an explanation relating to automated

[31] EU General Data Protection Regulation (GDPR): Regulation (EU) 2066/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation. Article 22. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679).

decision-making systems (s. 63(3)) impose some limits on algorithmic decision-making - the process raising the greatest concerns for group or community privacy.

These provisions do not, however, expressly address relational/group or community privacy concerns, nor do they address the equality concerns that arise from the processing of personal information. There Bill does not consider the privacy interests of individuals implicated in the personal information released by related others (framework matter 3 above). There is no express recognition of group-based privacy rights, except to some extent in relation to children, and then only based on their membership in a group that is independently recognized as vulnerable (on the basis of age). This kind of protection must also be extended to members of other equality-deserving groups. It must do so not just in relation to individual members of those groups, but also to groups and collectives themselves, as they face privacy and equality risks arising from the processing of personal information. These protections should extend not only to existing groups (framework matter 4 above) but also to ephemeral groups formed on the basis of algorithmic processing (framework matter 5 above). Addressing these gaps is of particular importance since Part 1 of Bill C-27 (*CPPA*) will govern data flows for algorithmic processing ostensibly to be governed by provisions of Part 3 (the *Artificial Intelligence and Data Act* (*AIDA)*), so that shortfalls in *CPPA* protection facilitate potentially problematic data flows for training and using algorithmic systems.

Part 3 of Bill C-27 (*AIDA*), unlike the first two Parts of Bill C-27, received virtually no public or expert consultation prior to being included in the C-27 omnibus bill. That lack of feedback has resulted in an Act that is fundamentally under-developed and prioritizes commercial over public interests. There is wide consensus amongst a range of submissions before Committee that Canada deserves AI regulation that is the subject of appropriately broad and deep consultation and that *AIDA* as currently drafted fails to meet that requirement.

Having registered that concern, which is fundamental, we acknowledge that legislation of this sort in some ways aligns with the work of addressing challenges laid out above in our framework. Specifically, framework matters (3) *affecting other individuals*, (4) *affecting an identifiable group*, and (5) *affecting a new algorithmically created group* could be ameliorated by taking primary responsibility out of individual hands and instead imposing regulatory limits on the use of AI systems to, among other things, address the discriminatory effects produced by those systems by:

- establishing pan-Canadian requirements relating to the design, development and use AI systems; and
- prohibiting certain conduct relating to AI systems that may result in "serious harm to individuals or harm to their interest" (*AIDA* s. 4(b)).

Regulation of this sort is an important step forward in addressing the privacy and equality impacts of our algorithmically sorted society because it begins the process of articulating publicly formulated controls on what can be done with data, rather than leaving those outcomes to corporations based on individual consent (or exceptions to consent). That said, the potential effectiveness of the proposed legislation is very difficult to assess in any meaningful way given that so much is left to be developed in regulations, including the very important question as to which systems would constitute "high impact systems" to which the law would actually apply (*AIDA* s. 5(1)). Leaving such important measures to be determined in regulatory processes that are not necessarily subject to public consultation, scrutiny and input is highly problematic given the significant collective and societal implications raised by AI systems, and the risk that those processes will be captured by powerful vested corporate interests. This is especially true given that systems that may not be obviously identified as being "high impact" can carry with them significant

equality risks.[32] To ensure effective regulation, either the definition of a high impact system will have to be exceptionally inclusive, or *AIDA* will require a more graduated and nuanced conception of risk than the single category of "high impact" can provide.

Other aspects of the *AIDA* as proposed also raise cause for concern (many of which are outlined in LEAF's submissions), including:

- its inapplicability to public and government AI systems and uses of AI (*AIDA* s. 3(1)), which themselves can have significant impact on the lives of equality-seeking groups and their members;
- the allocation of decision-making powers with respect to AI systems to a designated Minister (*AIDA* s. 5(1)), rather than to an independent, arms-length public tribunal with full investigatory and enforcement powers;
- its current focus on harms to individual members of certain marginalized groups without explicit protection for those groups as a whole; and
- its limited application to bias stemming from discrimination based on currently recognized prohibited grounds (*AIDA* s. 5(1)), thereby leaving out the prospect for addressing new categories of discrimination that may be algorithmically generated or existing categories such as poverty that are not explicitly protected under the *Canadian Human Rights Act*.

4. Conclusion and recommendations

In light of the foregoing, we offer the following general and specific recommendations:

General recommendations – the government should:

1. convene and/or fund deep public consultation, awareness-raising and facilitated dialogue to engage the public in discussion about the widespread democratic, systemic, and human rights implications of technological advancements like AI and the limitations of primary reliance on transactional individual decision-making models for protecting those rights;
2. thoroughly assess and address the impacts of the specific deficits identified in this submission and others and amend Bill C-27 accordingly;
3. review within 5 years of their coming into force all legislative changes pursuant to Bill C-27 in light of the public consultations and assessment noted above, and publicly report upon that review**.**

Specific recommendations – the government should:

1) Firmly identify privacy as a fundamental human right rather than an interest by revising the *CPPA* preamble and enactment sections to consistently and clearly reflect this position.
2) Ensure continued and appropriate protection of de-identified and 'anonymized' information:

[32] For example, the Toronto Police Service Board's AI policy classifies moderate risk technologies as those where the "human in the loop" might have difficult identifying bias or other decision failures of the AI, or where training data is based on existing service data: Toronto Police Services Board, "Use of Artificial Intelligence Technology" (28 February 2022) (P2022-0228-6.3), online: https://tpsb.ca/policies-by-laws/board-policies/195-use-of-artificial-intelligence-technology. Despite the equality risks of such systems, they would not seem to clearly fall into the factors of "high impact systems" discussed in the government consultation paper for AIDA: Government of Canada, "The Artificial Intelligence and Data Act (AIDA) – Companion document" (13 March 2023), online: https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document#s6.

a) All personal data and data derived from personal data, whether identifiable, de-identified, or anonymized, should be within the scope of the law;
b) Restore the definition of "de-identify" as it was in former Bill C-11, so that it includes both direct and indirect identifiers (*CPPA* s. 2(1));
c) Ensure that all de-identified data, including such data shared for purposes designated in the Act including for a socially beneficial purpose is explicitly considered to be personal information and within scope of the Act (*CPPA* ss. 2(3));
d) Bring anonymized data into the scope of the law (e.g. delete *CPPA* s. 6(5)) to enable the OPC to: (i) audit and approve measures taken to ensure the data is fully anonymized as per the definition in the Act or to investigate complaints by members of the public; and (ii) play a clear role in defining or determining what practices or standards are sufficient to meet the thresholds of de-identification and anonymization for the purposes of the law, which will require updating over time as technology evolves.

3) Strengthen individual informed consent requirements by removing or amending the provisions undermining individual informed consent:
   a) Limit the statistics, study, and research exceptions to "scholarly" endeavours (*CPPA* s. 35)*;*
   b) Constrain the use or disclosure of information collected for one purpose for new purposes simply by recording the new purpose to prevent a "bait and switch" approach to notification (*CPPA* s. 12(4)). At a minimum, this should include:
      i) a requirement that any new purpose for using personal information unknown and unspecified at the time of the original consent should be consistent with the original purpose for which the information was shared, and
      ii) that organizations must be proactive in flagging changes to their policies in ways visible to customers where new purposes for previously collected information have been recorded.
   c) Amend the language of *CPPA* s. 15(4) to return the principle of *understanding* to consent requirements and to require the information be in accessible formats so that people who do not read print can access it.
   d) Narrow or remove the option for implied consent in *CPPA* s. 15(5); if consent is to be only one of several grounds for information collection in the new law, then in those circumstances it is required, it should be explicit.
   e) Remove the legitimate interest exception in *CPPA* ss. 18(3-5). The business activities exception sufficiently alleviates the consent requirement for common business activities requiring information that is commonly understood to be necessary for the purposes of delivering services or products. The ss. 18(3-5) exception privileges businesses at the expense of their customers' privacy by allowing collection for any reason related to a legitimate interest, as assessed by the business itself, with no certainty that assessment of legitimacy will ever be subject to regulatory or public scrutiny.
   f) Ensure appropriate limits on any collection, use, or disclosure of personal de-identified information under the "socially beneficial" exemption (*CPPA* s. 39). What is "socially beneficial" may be a matter of debate subject to the vagaries of politics and potentially turbulent national/global contexts, so this exception must be used in a way that is open, transparent, and publicly accountable and the law must enforce those guardrails. To that end, amendments are needed to:
      i) Require that requested disclosures of data under *CPPA* s. 39 be assessed by the OPC and publicly disclosed in a prominent, accessible manner. Information to be published should include: (1) the socially beneficial purpose met by disclosure; (2) the OPC's assessment results, including any recommendations made to mitigate privacy risks or adverse impacts resulting from disclosure; and (3) the parties who will have access to the information and the duration of its anticipated use.

ii) Empower the OPC to deny disclosures or require action to ensure de-identification reaches an appropriate standard, with attention to the sensitivity of the data, prior to any disclosure.
iii) Provide individuals with the option to "opt-out" of disclosures for socially beneficial purposes. This opt-out must be prominent and accessible at the time of information collection, and subsequently.
iv) Empower the OPC to audit all disclosures made under s. 39 and to investigate complaints regarding such disclosures by members of the public.

4) Enhance the recognition and protection of group/collective/community privacy and equality rights by:
   a) implementing the amendments to the provisions relating to children in Part 1 recommended by UNICEF Canada in its submissions;
   b) supporting appropriate limits on automated decision systems that include recourse and not just explanation, including the option to request reconsideration of a recommendation or decision by a human decision-maker (*CPPA* s. 63(3));
   c) delaying passage of *AIDA* pending full public consultation and amendments aimed at reducing the number of important matters left to be dealt with via regulation;
   d) creating an arms-length, independent public tribunal with full investigatory and enforcement powers to carry out the functions determined to be necessary through public consultation;
   e) implementing the amendments to *AIDA* recommended in LEAF's submission, including:
      i) extending its application to public and government institutions (delete *AIDA* s. 3);
      ii) expanding the definitions of "harm" and "biased output" (*AIDA* s. 5) and "persons responsible" (*AIDA* s. 5);
      iii) expanding its application beyond "high-impact" systems (*AIDA* s. 7-9, 11, 12, 36(b));
      iv) requiring performance of privacy and equity audits (*AIDA* s. 8, 11, 36); and
      v) insuring substantive equality and public consultation inform development of regulations.

All of which is respectfully submitted,

Jane Bailey
Full Professor
University of Ottawa Faculty of Law
(Common Law Section)

Dr. Jacquelyn Burkell
Full Professor
Faculty of Information & Media Studies
Associate Vice-President, Research
Western University

Dr. Brenda McPhail
Acting Executive Director, Master of Public Policy in Digital Society Program
Faculty of Social Sciences
McMaster University