# Submission to INDU Committee Study of Bill C-27, *The Digital Charter Implementation Act, 2022*

OpenMedia is a community-based, Canadian non-profit organization that together with our community works to keep the Internet open, affordable, and surveillance-free.

May 3, 2023

## Overview of Submission:

### *A. Introduction*



### *B. Consumer Privacy Protection Act*



### *C. Personal Information and Data Tribunal Act*



### *D. Artificial Intelligence and Data Act*

## *A. Introduction*

### About OpenMedia

OpenMedia is a community-driven organization of over 350,000 members that work together to keep the Internet open, affordable, and surveillance-free. We operate as a civic engagement platform to educate, engage, and empower Internet users to advance digital rights around the world.

For many years, the OpenMedia community has been actively engaged in advocacy around privacy law reform in Canada. Most recently, we delivered more than 11,000 signatures to Prime Minister Justin Trudeau, calling for the government to introduce urgent privacy reforms for the public sector, while also clarifying that Bill C-27 fails to provide people in Canada with sufficient protections for the private sector in the modern digital economy.[1]

While we are pleased that the government has introduced privacy reforms in the private sector, we recognize that Bill C-27 could actually mean less privacy protections for people in Canada. We would be remiss if we didn't seize this opportunity of Parliamentary study to provide essential feedback that would drastically improve this important legislation.

## *B. Consumer Privacy Protection Act*

### 1. Absence of Privacy as a Human Right

The single most important change to Canadian privacy law is the acknowledgement of privacy as a fundamental human right. This is an essential measure that not only reinforces the notion of privacy as a right that enables other constitutionally protected activities – like freedom of assembly, thought, expression, and association – but also acts to rebalance the vast power asymmetries that exist within our information technology landscape. Bill C-27 fails to make this essential acknowledgement.

By failing to recognize privacy as a fundamental human right, Bill C-27's *CPPA* will force adjudicators to balance the business interests of companies against people's personal agency over their own information. This leads to a significant risk that the economic

[1] OpenMedia #DemandPrivacy delivery letter to Prime Minister Justin Trudeau (2022): https://openmedia.org/assets/_DemandPrivacy_Petition_Deliver_-_October_20%2C_2022.pdf

interests of corporations will outweigh the privacy interests of individuals, contributing to a general loss of control over one's own personal information, and fostering a sense of helplessness that erodes personal agency in Canada.

In Canada's modern digital society, the development of a sense of self, and one's ability to participate in democratic life, is often mediated by our interactions with technology. Therefore, it is absolutely essential that an individual's privacy interests relating to their own information be formally recognized in law as superseding the economic interests of companies to that same information. It is essential to recognize privacy as a fundamental human right in Canada's commercial, private sector privacy laws in order to safeguard the cultivation of a healthy society that's fully empowered to make informed decisions relating to the creation, understanding, and remaking of the self.

In order to be meaningful, this acknowledgement must take place within the text of the bill and cannot take place in the preamble. The preamble in a bill like C-27, which contains more than one Act, can be compared to a rocket that brings multiple satellites into orbit. The preamble is like the thruster; it provides the initial force that projects the satellites into space. But once the satellites have left earth's atmosphere, the thruster detaches and the satellites exist on their own, in isolation from each other and from that of the initial force. Therefore, in the context of the lifespan of the Acts contained within Bill C-27, the preamble is not a useful device to imbue long term meaning, or to direct interpretation after the fact. The Acts themselves must contain language that formally and unequivocally recognizes privacy as a fundamental human right.

More than 8,500 members of the OpenMedia community have sent members to their Members of Parliament asking them to ensure that Bill C-27's *CPPA* recognizes privacy as a fundamental human right that supersedes any commercial interests in their personal information.

## 2. Right to Request Deletion (or Right to *Ignore* Requests)

The government has framed its discussion of Bill C-27 as legislation that introduces new rights and protections for people in Canada. Under examination, however, Bill C-27's *CPPA* provides more new rights and protections for companies than it does for people in Canada. For example, the new right to request deletion empowers companies to ignore these very deletion requests.

Section 55 (1) (a) of the *CPPA* provides a potential remedy should an individual find that a company has collected their personal information in a way that contravenes the Act,

like by not seeking the consent of that person prior to the collection and use of that information. In this instance, 55 (1) would empower a person to request that the company delete their personal information. However, this potential remedy is immediately undone by the list of exceptions detailed under 55 (2). This list of exceptions includes 55 (2) (f), which allows companies to reject requests for deletion should they have an existing deletion schedule that describes when that information will be deleted.

In practical terms, it would be very difficult or impossible for an individual to discover that a company has collected their personal information if prior, informed, and meaningful consent had not been sought. Therefore, 55 (1) (a) – the provision that allows an individual to request the deletion of information that has been collected and used in a way that contravenes the *CPPA* – is already significantly undermined. Further, should the company that has collected the information in violation of the *CPPA* have a plan in place to delete the information in a set period of time, they would be empowered to reject the individual's deletion request on those grounds.

To further illustrate this point, we can look at a scenario that recently took place in Canada. A company based in the United States called Clearview AI collected the personal information of millions of Canadians in the form of biometric templates taken from images of faces scraped from the Internet, and sold access to a database of these illegally harvested biometric templates to Canadian law enforcement agencies. This collection was non-consensual, and the Office of the Privacy Commissioner of Canada determined that it was in violation of Canada's existing private sector privacy laws, the *Personal Information and Protection of Electronic Documents Act* (PIPEDA).[2] Under the *CPPA*, 55 (2) (f) would empower a company like Clearview AI to produce a data retention schedule and avoid compliance with any subsequent deletion requests. In summary, the exception provided in 55 (2) (f) is so broad that it completely nullifies any potential remedy provided by 55 (1) (a), (b), or (c).

This scenario helps to illustrate one of the many ways in which Bill C-27 tips the balance of power towards companies and away from individuals, reinforcing existing power asymmetries in our information technology landscape, and empowering bad actors like Clearview AI.

[2] Office of the Privacy Commissioner of Canada (2021): https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/

## 3. Right to Data Portability

In theory, a right to data portability can help increase the agency of individuals within the context of digital environments. In the text of Bill C-27's *CPPA*, it is difficult to determine the efficacy of this provision (Section 72) given that it's almost entirely left to the regulations, and the construction of the framework is left entirely to the discretion of the Governor in General (Section 123).

## 4. A New Consent Framework: Plain Language vs. Comprehension

Bill C-27's *CPPA* introduces a significant shift from *PIPEDA* when it comes to the obligations of companies in collecting the personal information of people in Canada. Unlike *PIPEDA*, the *CPPA* does not require that companies, to a reasonable standard, ensure that their customers understand the **nature**, **purpose**, and **consequences** of consenting to the collection, use, and disclosure of their personal information. In order to fully explore the contours of this shift, it's useful to examine the precise language that exists in *PIPEDA* as compared to the *CPPA* when it comes to the validity of digital consent agreements.

6.1 of *PIPEDA* states: "the consent of an individual is only valid if it is 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).[3] The language used in 6.1 of *PIPEDA*, which outlines the conditions that are necessary for consent to be valid in the collection of personal information, indicates that the responsibility for ensuring the understanding of "the **nature**, **purpose** and **consequences**" of permitting a commercial entity to collect, use, or disclose an individual's personal information rests, to a reasonable standard, with the company itself. The words that create the validity of this obligation within 6.1 of *PIPEDA* are: "**would understand**". Therefore, under *PIPEDA*'s existing consent framework, consent is only valid if it is reasonable to conclude that a person "would understand" the "nature, purpose and consequences" of the collection, use, and disclosure – these are the necessary preconditions to valid consent. Bill C-27's *CPPA* would reverse this element of Canada's existing consent framework by eradicating this language, and these necessary preconditions, by introducing a much less onerous plain language requirement.

[3] Section 6.1 of PIPEDA: https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/page-1.html

The *CPPA* departs from assigning this responsibility to a company and instead puts the obligation of understanding on individuals who are providing their consent. Bill C-27's *CPPA*'s Section (3) lists the newly expanded conditions for consent, while simultaneously reworking *PIPEDA*'s existing consent framework: "The individual's consent is valid only if, at or before the time that the organization seeks the individual's consent, **it provides** the individual with the following information" (emphasis added).[4] While Section (3) goes on to describe a broader array of information that a company must provide to an individual for consent to be valid, it also entirely removes the existing obligation on companies to ensure that individuals "**would understand**" (to a reasonable standard) the purpose, nature, and consequences of the collection, use, and disclosure of their personal information (the necessary preconditions for valid consent that exist in *PIPEDA*).

The word "**understand**" reappears in the new *CPPA*, but its context is very different from *PIPEDA*. Bill C-27's *CPPA* new plain language requirement on companies is contained in Section (4). However, as the obligation on companies to ensure that people in Canada "**would understand**" the implications of providing consent has been removed, the impact of this new plain language requirement is negated. Section (4) reads: "The organization must provide the information referred to in subsection (3) in plain language that an individual to whom the organization's activities are directed would reasonably be expected to understand."[5] While the word "**understand**" is present, the context is very different from *PIPEDA*'s 6.1. In the *CPPA*, the reference to understanding applies only to **the language** that the company is using in providing the additional information to meet the other conditions (i.e., do the words, in the order that they are presented, make logical sense). This is unlike *PIPEDA*'s 6.1, where the application of understanding extends beyond the language itself and into **the concepts** ("the nature, purpose and consequences") behind that language. In requiring, to a reasonable standard, that these necessary preconditions of basic understanding be met in order for consent to be valid, *PIPEDA*'s existing consent framework is a much more robust and effective tool in protecting the privacy interests of people in Canada.

On the surface, this shift appears to be an admission in the text of Canada's private sector privacy laws that individuals can no longer be reasonably expected to understand the vast implications of consenting to the collection, use, and disclosure of their personal information; that companies should not bare the burden of ensuring that their customers can understand the ways in which their personal data can be exploited for profit in a digital ecosystem known as surveillance capitalism. Therefore, the shift from

[4] Bill C-27's *CPPA*, Section 3: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading
[5] See 4, Section 4

placing this responsibility of understanding on companies to individuals seems a codified admission that the power asymmetries in our modern information technology landscape are so vast that even a reasonable attempt to foster understanding is no longer necessary. Surely, this could not be the intention of law-makers in making this subtle, but incredibly important change to Canada's existing consent framework.

In the view of OpenMedia, the narrowing of the legal obligation on companies – from ensuring, to a reasonable standard, that people in Canada "**would understand**" to a much more permissive requirement "**it provides**" in plain language – represents a major transformational shift in the practical operation of digital consent. A dramatic shift in an existing consent framework, like the one occurring between *PIPEDA* and the *CPPA*, deserves more study and consultation before being imposed on an unsuspecting Canadian public as the consequences will be significant. Rather, it would be more appropriate to retain *PIPEDA*'s existing consent framework with **the addition** of a plain language requirement.

## 5. Exceptions to Consent

Despite the drastically reduced obligations on companies due to the transformational shift relating to the validity of consent described in the above section, Bill C-27's *CPPA* goes even further to empower private organizations by proposing new ways that companies can collect, use, and disclose personal information without being required to receive valid consent at all. These are outlined in Sections 18 to 51 of the *CPPA*. In total, the *CPPA* grants companies 33 areas where they can collect, use, and / or disclose personal information without receiving valid consent. As compared to *PIPEDA*, the *CPPA* reorganizes the presentation of this information in a way that disadvantages people in Canada, and provides one exception that also acts to completely transform Canada's existing consent framework.

Compared to *PIPEDA*, this list is expanded and presented in a way that prioritizes business organizations over individuals looking to inform themselves about their privacy rights. *PIPEDA*, in setting out the circumstances in which companies are not required to achieve meaningful consent, separates the conditions into three clearly delineated sections: 7 (1) "Collection without knowledge or consent"; 7 (2) "Use without knowledge or consent"; 7 (3) "Disclosure without knowledge or consent". By presenting the information in this way, *PIPEDA* is written so that an individual can easily understand the circumstances that apply based on the above listed scenarios, and inform themselves of their rights. This is a user-centric approach. In contrast, the *CPPA* is written in a way that mixes the use, collection, and disclosure exceptions into broader

categories of business activities that are not relatable to an average person. These include categories like “legitimate interest”, “prospective business transaction”, and “socially beneficial purpose”. In effect, the reorganization of the exceptions to consent in this way prioritizes commercial interests over individual rights, which will lead to even greater confusion about when consent is a necessary precondition to the valid collection, use, and disclosure of personal information. It’s also another way in which Bill C-27 explicitly prioritizes the commercial interests that private companies have over our own personal information, while reducing our meaningful control over our data.

Bill C-27’s *CPPA* provides one incredibly broad exception to consent that will completely transform Canada’s existing digital consent framework. Section 18 (2) (a) says that consent is not necessary for any “activity that is necessary to provide a product or service that the individual has requested from the organization”. Meaning, if an individual engages a company under their own volition to procure “a product or service” – terms that are vague enough to describe nearly every business activity – the digital consent framework that we know and understand will no longer be necessary. Under these circumstances, people in Canada will no longer be permitted to click “I agree” to a terms of service agreement before using a new product or service; our agreement will be implicit in our request for the product or service, and the company’s obligation ends at providing some basic information in plain language. This will be the case anytime an individual is signing up for a new service online – especially those relating to telecommunications, banking, finance, and other federally regulated industries.

Taken in consideration with how the *CPPA* removes the existing obligation for companies to ensure to a reasonable standard that individuals “would understand” the nature and consequences of the collection, use, and disclosure of their personal information, this incredibly broad exception to consent means that people in Canada will have much more difficulty understanding the nature and consequences of the business relationships they enter into on the Internet. While OpenMedia agrees that digital consent is not a perfect solution, the *CPPA* goes too far by proposing to move past consent entirely without providing any form of reasonable alternatives or effective remedies for the harms that will inevitably be inflicted on people in Canada.

The *CPPA* contains one provision that seems intended to remedy some of the harms that will emerge from moving away from *PIPEDA*’s existing digital consent framework. Section 18 (1) (b) of the *CPPA* restricts companies from using the exceptions to consent under these circumstances: “the personal information is not collected or used for the purpose of influencing the individual’s behaviour or decisions.” This provision is intended to prevent companies from collecting or using (but not disclosing) personal

information without consent in circumstances where this information could be used to "**influence**" a person's "**behaviour** or **decisions**". In this way, Section 18 (1) (b) is the only suggestion that the drafters of the *CPPA* were, at the very least, conscious of the existence of a concept known as surveillance capitalism. (Indeed, Section 18 (1) (b) appears to be the single provision contained within Bill C-27 to ameliorate all of the harms of surveillance capitalism.)

The problem with Section 18 (1) (b) is that it acknowledges a significant issue with vast power asymmetries in Canada's information technology landscape while simultaneously failing to provide a productive solution. Ironically, the presence of Section 18 (1) (b) actually permits companies to "**influence**" the "**behaviour** or **decisions**" of people in Canada in circumstances where consent has been generated under the *CPPA*'s much less onerous obligations. It also issues an implicit challenge to people in Canada to determine on their own whether or not their personal information (that the *CPPA* empowers companies to non-consensually collect, use, and disclose) is having any effect to "**influence**" their "**behaviour** or **decisions**." Practically speaking, this is an impossibility; how can a person be reasonably empowered to determine whether or not their own personal information is being used to "**influence**" their "**behaviour** or **decisions**" if that information is being non-consensually collected in the first place, and a person has not been empowered to know **what** companies are using their personal information?

While the spirit behind the *CPPA*'s Section 18 (1) (b) is well-intentioned, it will not address any of the harms of surveillance capitalism. And, as mentioned previously, it implies that the companies should be empowered to "influence" the "behaviour or decisions" of people in Canada provided that they have consented in a way that is less onerous than our existing framework. The impact of these changes will be felt hardest by vulnerable groups like youths who are exploring and discovering a sense of self on the Internet. We are just learning about the influence that social media has on the mental health of young people in Canada. The changes to Canada's existing consent framework contained in the *CPPA* will function to legitimize, conceal, and accelerate these harms.

## 6. Socially Beneficial Purposes & De-Identified Data

The *CPPA*'s Section 39 (1) introduces another new exception to consent for "socially beneficial purposes". This new exception would permit an organization to non-consensually disclose de-identified personal information to a government

organization or contractor for any purpose deemed "socially beneficial", which the *CPPA* defines as "related to health, the provision or improvement of public amenities or infrastructure, the protection of the environment or any other prescribed purpose."

The inclusion of this exemption to consent seems a direct response to criticism of the federal government's acquisition of mobility data from Telus, which was the subject of Parliamentary inquiry by the Standing Committee on Access to Information, Privacy and Ethics (ETHI) last year.[6] That investigation found that the federal government could have acted more transparently while acquiring the location data of millions of people in Canada.

The *CPPA* in general, and Section 39 more specifically, reads as if the federal government is deflecting valid criticism to its non-transparent collection and use of the sensitive mobility data of millions of people in Canada. The response seems to say: "We didn't do anything wrong – the laws were wrong! So we're changing the laws." This becomes abundantly clear when considering the recommendations made by the ETHI committee in their report on the federal government's use of mobility data, and how they have been ignored in the text of Bill C-27's *CPPA*.

The ETHI committee report makes 22 recommendations that include new initiatives for the federal government and reforms to public and private federal privacy laws. Of the 22 recommendations made, 13 are related to reforms of Canada's federal private sector privacy laws, *PIPEDA*. Of these 13 recommendations, the *CPPA* fails in all but 4 instances.

Dr. Chris Parsons, on behalf of the Citizen Lab at the University of Toronto, makes his own set of recommendations to improve Bill C-27's *CPPA*. OpenMedia fully endorses the recommendations made in his report for the Citizen Lab.[7] Specifically, the recommendations contained in Section 5 of Dr. Parsons' report addresses eight of the failures pertaining to Canada's private sector privacy laws that are outlined in the aforementioned report from the ETHI committee. For this reason, we are putting the two reports in conversation in order to present a path towards achieving the recommendations of the ETHI report through Dr. Parsons' existing legislative amendments:

---

[6] 'Collection and use of mobility data by the government of Canada and related issues', report by the Standing Committee on Access to Information, Privacy and Ethics: https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP11736929/ethirp04/ethirp04-e.pdf

[7] 'Minding Your Business', report by Dr. Christopher Parsons, the Citizen Lab at the University of Toronto: https://citizenlab.ca/wp-content/uploads/2022/12/Report161-MindingYourBusiness120922.pdf

- The first recommendation of the ETHI report implores the federal government to ensure that people in Canada have the option of opting-out of data sharing arrangements with the federal government for socially beneficial purposes. The *CPPA* fails in this regard, but Dr. Parsons' fourth recommendation addresses this failure by providing language for legislative amendment that would require people in Canada to be informed of the opt-out process prior to the disclosure taking place;

- The second recommendation of the ETHI report implores the federal government to meaningfully consult with the Office of the Privacy Commissioner of Canada (OPC) prior and during programs that involve data sharing arrangements for socially beneficial purposes. The *CPPA* fails in this regard, but Dr. Parsons' fourth and fifth recommendations address this failure by providing language for legislative amendment that would require prior approval for data sharing arrangements for socially beneficial purposes from the OPC;

- The fifth recommendation of the ETHI report implores the federal government to ensure that people in Canada are aware of the "nature and purpose" of mobility data collection, use, and disclosure. As previously observed, the *CPPA* fails in this regard by moving away from *PIPEDA*'s existing consent framework, which creates an obligation on companies to ensure, to a reasonable standard, that their customers understand the consequences (the nature and purpose) behind consenting to the collection, use, and disclosure of their personal information. By moving away from this obligation on companies, and by introducing a new consent framework, the *CPPA* will ensure that people in Canada are less aware of the "nature and purpose" of the collection, use, and disclosure of their sensitive personal information, like mobility data. Dr. Parsons' fifth recommendation addresses this failure of the *CPPA* by providing language for legislative amendment that would require companies to complete and disclose "adverse effect assessments" that would be reviewed by the OPC in order to determine whether the potential adverse effects are proportionate to the supposed social benefits before approving a data sharing arrangement for socially beneficial purposes;

- The eighth recommendation of the ETHI report implores the federal government to ensure that Canadian privacy laws include de-identified data. The *CPPA* fails in this respect by taking a dangerously narrow view of de-identified data. Dr. Parsons' first recommendation addresses this failure of the *CPPA* by providing

language for legislative amendment that provides a more expansive definition of de-identified data. This language was present in the previous version of federal private sector privacy legislation called Bill C-11;

- The ninth recommendation of the ETHI report implores the federal government to include a standard for de-identified data. The *CPPA* fails in this regard by allowing companies to treat de-identified personal information like anonymous data in certain circumstances, but Dr. Parsons' recommendations two and three address this failure by providing language for legislative amendment that would prevent companies from treating de-identified personal information the same as anonymous data, and enables the OPC to create regulations that ensure personal information has been appropriately de-identified;

- The tenth recommendation of the ETHI report implores the federal government to prohibit companies from re-identifying data and creating a corresponding penalty for an offense. While the *CPPA* prohits de-identification in Section 75, its very definition of de-identification is problematic, but Dr. Parsons' recommendations one and two address this failure by providing language for legislative amendment that would adopt the prior definition of de-identified data from the old Bill C-11, and removing the exemptions that exist under Section 2 (3) of Bill C-27's *CPPA*;

- The twelfth recommendation of the ETHI report implores the federal government to require companies to obtain meaningful consent for the collection of mobility data. The *CPPA* fails in this regard by allowing companies new exemptions to consent that do not exist in *PIPEDA* and by permitting companies to treat de-identified personal information (including mobility data) as fully anonymized data through introducing additional exemptions under Section 2 (3) of Bill C-27's *CPPA*. Dr. Parsons' second recommendation addresses this failure by providing language for legislative amendment that would remove these exemptions;

- The fourteenth amendment of the ETHI report implores the federal government to require that service providers allow customers to opt-out of mobility data sharing arrangements. The *CPPA* fails in this regard, but Dr. Parsons' fourth recommendation addresses this failure by providing language for legislative amendment to Section 39 (1). The addition of Section 39 (1) (d) ensures that people in Canada would be informed of mobility data sharing arrangements, are aware of the stated socially beneficial purposes and any potential adverse effects, and know how to opt-out.

## 7. Sensitive Information

Best in class privacy legislation from around the world creates categories of sensitive information that are deserving of special protections. Sensitive information can include things like health and financial data, ethnic and racial origins, personal information of minors, genetic and biometric data, and more.

PIPEDA leaves the interpretation of what kinds of sensitive information are deserving of special protections to the interpretation of the Office of the Privacy Commissioner of Canada and the courts. This leads to some categories of information, like medical and income records, to be considered sensitive, whereas other categories are only considered sensitive depending on context. In the end, our judicial system is forced to strike the balance between two competing interests: an obligation to protect the privacy rights of individuals, and an obligation to facilitate the collection, use, and disclosure of personal information by the private sector. However, there should be no ambiguity about what sensitive information is deserving of special protections; Canada's privacy laws should follow best in class international standards by clearly delineating what categories of sensitive information are deserving of special protections.

For example, the European Union's *General Data Protection Regulations* establish a general prohibition on the processing of sensitive personal data, including: racial or ethnic origin; political opinion; religious or philosophical belief; trade union membership; genetic data; biometric data; health data; and sexual orientation.[8] Likewise, Australia's *Privacy Act* includes even more categories, like: biometric templates; criminal records; and membership in a political or professional association.[9]

Perhaps most relevant, in the United States, the recently proposed *American Data Privacy and Protection Act* provides the most extensive list of protections, which include: government issued identifiers (like SIN numbers, passports numbers, or driver's license numbers); any information that describes or reveals the past, present, or future physical health, mental health, disability, diagnosis, healthcare condition, or treatment of an individual; financial information; biometric information; genetic information; precise geolocation information; an individual's private communications; passwords; information identifying the sexual orientation or sexual behavior of an individual in a manner inconsistent with the individual's reasonable expectation regarding disclosure of such information; calendar information, address book information, phone or text logs, photos,

[8] *GDPR*, Article 9 – Processing of special categories of personal data: https://gdpr-info.eu/art-9-gdpr/
[9] Australian Government, *Privacy Act*: https://www.legislation.gov.au/Details/C2021C00139

audio recordings, or videos maintained for private use by an individual, regardless of whether such information is stored on the individual's device or in a separate location on an individual's device, regardless of whether such information is backed up in a separate location; non-consensual intimate images; information that reveals the video content or services requested or selected by an individual from a provider of broadcast television service, cable service, satellite service, or streaming media service; minor's information.[10]

By comparison, Bill C-27's *CPPA* creates only one category of sensitive information. As a response to criticism of the predecessor of Bill C-27, the government has made the personal information of Canadian youth sensitive information that is deserving of special protections. While this is a necessary and valuable change, the government could go much further by creating additional categories of sensitive information, which will remove the uncertainty that is sure to emerge in the private sector as companies struggle to understand what personal information can and cannot be processed and used for certain purposes. This is yet another example of where the legislation does not do enough to protect the privacy rights of people in Canada.

## 8. Controlling Data Brokers

The *CPPA* would take the same approach as *PIPEDA* to regulate data brokers – which is to take no approach at all, as they're not directly addressed or defined under Bill C-27. Instead, general rules regarding the collection, use, and disclosure of personal information would be applicable to data brokers with no new regulations or restrictions on this sector of the digital economy. Like *PIPEDA*, Bill C-27 also excludes some information like publicly available information (Section 51) and non-commercial activities (Section 6), from certain legal protections, including the activities of data brokers. Meaning, for certain types of information, and for certain kinds of activities, no protections or regulations will exist at all for data brokers.

Canada could learn from the United States when it comes to the protection of privacy from data brokers. The *American Data Privacy and Protection Act*[11] (ADPPA) was passed by the House Energy and Commerce Committee last year. Unlike *PIPEDA* and Bill C-27, it would have recognized data brokers as "third-party Collecting Entity" that does not collect personal information directly from individuals, which is a helpful

[10] U.S. Congress, *American Data Privacy and Protection Act*: https://www.congress.gov/bill/117th-congress/house-bill/8152/text
[11] See 10

definition. This proposed privacy law would also force data brokers who have a principal source of revenue in data collection to register with the Federal Trade Commission, and provide information like "[a] description of the categories of data the third-party collecting entity processes and transfers." A searchable registry of data brokers would then be made publicly available on the Internet, giving people the ability to learn more about this shadowy industry.

At the state level, there are some laws to protect the personal data of United States residents against data brokers' activities. In 2018, the State of Vermont passed an Act relating to data brokers,[12] which requires that data brokers register annually with the Secretary of State and disclose the information regarding their data collection activities, a purchaser credentialing process, the number of security breaches, and possession of sensitive information like personal information of minors. This Act also requires data brokers to have different security standards such as developing, implementing, and maintaining a comprehensive security program and designating one or more employees to maintain the program.

In 2019, a California law also took the same approach and requires data brokers to register with the Attorney General on its publicly accessible website, providing the opportunity for residents to opt-out from the data broker economy.[13] The California Consumer Privacy Act also has comprehensive rules to protect against businesses who sell personal information, like data brokers.[14]

Leaving the situation unchanged, Bill C-27 fails to address the harms that come from the non-consensual trade and profit of the sensitive personal information of people in Canada. Looking at examples from the United States, it's evident that other jurisdictions are feeling the need to tackle this issue, and are arriving upon a few good ideas that might help to improve digital privacy protections for people in Canada.

For example, to tackle concerns regarding the data brokers' behaviour, Bill C-27 would be improved if it:

1. Recognized and clearly defined data brokers;

---

[12] Vermont Legislature, *An Act Relating to Data Brokers and Consumer Protection*: https://legislature.vermont.gov/Documents/2018/Docs/ACTS/ACT171/ACT171%20As%20Enacted.pdf
[13] California Legislature, *Privacy: Data Brokers*: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB1202
[14]California Legislature, *California Consumer Privacy Act*: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

2. Required that data brokers register under an independent regulatory body, like the Office of the Privacy Commissioner of Canada;
3. Made data brokers' information publicly available and searchable;
4. Provide individuals with the ability to opt-out from data brokers and have their information deleted;
5. Required that data brokers disclose the information such as their data collection activities and possession of sensitive information.

While this won't do everything to address the problem with data brokers, it will give people in Canada some options to learn more about the secretive companies that profit from the trade of their data, and the ability to opt-out from this secretive economy.

## 9. Federal Political Parties

Canada's federal political parties must be held to the same standard as any other organization that collects and uses personal information, including private sector companies, government bodies, and non-profit organizations like us.

In 2019, the Office of the Privacy Commissioner of Canada issued guidance to Canada's federal political parties on how to comply with new privacy requirements contained in amendments to *Canada's Elections Act*.[15] At that time, OpenMedia compared the newly published privacy policies of Canada's federal political parties against these new requirements and found that **none** were meeting the basic expectations of privacy as set out by Canada's Chief Electoral Officer.[16] This failing acts to undermine the trust that people in Canada have in our democratic system and the institutions responsible for upholding it.

Recently, the government tabled its 2023 budget Bill C-47 – which contains Division 39, an amendment to the *Canada Elections Act* – and would make the current privacy protections offered to the electorate permanent.[17] That is, an approach that can only be described as "self-regulation": federal political parties are empowered to write their own privacy policies, which they are free to change at any time, and audit their own adherence to those policies, with no sanctions for non-compliance.

---

[15] Office of the Privacy Commissioner of Canada, *Guidance for federal political parties on protecting personal information*: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/gd_pp_201904/
[16] OpenMedia, *Canada's Political Parties Fail to Meet Basic Privacy Expectations*: https://openmedia.org/press/item/canadas-political-parties-fail-meet-basic-privacy-expectations
[17] Bill C-47 - An Act to implement certain provisions of the budget tabled in Parliament on March 28, 2023: https://www.parl.ca/legisinfo/en/bill/44-1/c-47

The Senate committee on legal and constitutional affairs briefly studied the changes proposed by Division 39, hearing from Canada's Chief Electoral Officer and Privacy Commissioner.[18] The opinion of both experts was that the current privacy protections afforded to the electorate are inadequate to protect our democratic process, that making these inadequate protections permanent is contrary to their recommendations, and that this kind of change should not be contained in a budget bill.

7,000 members of the OpenMedia community have signed a petition in opposition to the proposed changes of Division 39 of Bill C-47, voicing their support instead for the regulation of privacy for federal political parties to be contained in Canada's private sector privacy legislation, Bill C-27's *CPPA*.

More than 12,000 people have taken action on another OpenMedia campaign calling for the inclusion of federal political parties in Canada's privacy laws. OpenMedia supports the suggested amendment contained in Section 3 (*Address the Privacy Risks to Democracy*) of the Centre for Digital Rights report on Bill C-27: *Not Fit For Purpose – Canada Deserves Much Better*.[19]

## *C. Personal Information and Data Tribunal Act*

### 1. Undermining the Office of the Privacy Commissioner of Canada

For years, the Office of the Privacy Commissioner of Canada (OPC) has been upholding the privacy rights of people in Canada through independent investigations of complaints, publishing reports of findings, and issuing timely guidance. Despite Canada's relatively weak privacy laws, the OPC has been proactively working within our limited legal framework to defend our rights. One of the most valuable contributions of Bill C-27 is the introduction of new powers for the OPC, including introducing order-making and monetary penalties. The creation of a new tribunal structure, however, will act to undermine not just these new powers, but also the overall effectiveness of Canada's national, independent privacy regulator.

The tribunal will be composed of political appointees who will have the jurisdiction to make decisions relating to appeals of findings and the imposition of penalties from the

[18] Notice of Meeting, May 3rd, 2023: https://sencanada.ca/en/committees/LCJC/noticeofmeeting/606030/44-1
[19] Centre for Digital Rights, *Not Fit For Purpose – Canada Deserves Much Better*: https://centrefordigitalrights.org/files/document/2022-11-13/257-013312.pdf

Office of the Privacy Commissioner of Canada, an independent agent of Parliament. This will significantly undermine the autonomy of this important regulator.

In order to better understand the potential consequences of the *Personal Information and Data Tribunal Act* (*PIDTA*) OpenMedia looked to other jurisdictions around the world for examples of comparable tribunal structures. It is revealing that Canada's allies in the United Kingdom, European Union, New Zealand, and Australia have chosen not to undermine the work of their independent privacy regulators through the creation of similar tribunal structures, and instead rely upon conventional vehicles for appeal, like the one currently in existence under *PIPEDA*, the Federal Court of Canada.

The OPC has recently found strength in combining resources with its provincial counterparts through joint-investigations. There is cause for concern that the introduction of a new mechanism for appeal at the federal level might complicate the fruitfulness of these collaborations. For example, if the OPC's findings were appealed through the Tribunal in one of these joint-investigations, how might this impact the work of the OPC's provincial counterparts, who are not subject to this additional layer of bureaucracy?

## 2. Undermining the Private Right of Action

Currently, the primary recourse for people in Canada who've had their privacy violated is to band together to collectively sue companies through class action lawsuits.[20] The introduction of a private right of action in the Bill C-27's *CPPA* gives individuals the ability to pursue financial settlements with companies that have been found to have committed privacy violations – but like much else in Bill C-27, there's a catch.

Our new ability to pursue a private right of action requires that the OPC and the newly created tribunal confirm that a privacy violation has occurred. Typically, the OPC takes about a year to complete an investigation and issue a report of their findings. So that means, before any person in Canada is able to pursue the private right of action against a privacy violating company, a period of at least one year is likely to have elapsed – not to mention the time needed for the tribunal to reach their own, separate decision.

[20] Financial Post, '*Sweet deal' for Tims? Coffee-and-donut privacy breach settlement a marketing win, says expert*: https://financialpost.com/news/economy/a-sweet-deal-for-tims-coffee-and-doughnut-privacy-breach-settlement-a-marketing-win-expert

Is this really going to work for an ordinary Canadian? Taking into consideration the avenues of appeal that the company might then take after these decisions have been made, and the difficulty in determining actual harm from privacy violations, a person will likely face an extremely lengthy, difficult, and uphill road towards justice through this mechanism.

This would be improved by removing the newly created tribunal entirely through scrapping the *Personal Information and Data Tribunal Act*. A recourse for appeals of findings and penalties already exists in Canada's Federal Court.

## *D. Artificial Intelligence and Data Act*

More than 8,500 members of the OpenMedia community messaged their Members of Parliament urging them to remove the *Artificial Intelligence and Data Act* from Bill C-27. They expressed concerns that this proposed legislation is substantively different from the other components of the bill and should receive its own, separate study and consideration.

OpenMedia is in agreement with the findings of the joint report issued by the Toronto Metropolitan University, McGill University, and Princeton University when it comes to the significant shortcomings of this proposed legislation.[21] In particular, we would like to highlight two concerns.

### 1. Lack of Consultation

Regulating an emerging industry like artificial intelligence requires consultation with stakeholders. Prior to the release of the government's formerly proposed private sector privacy legislation, the old Bill C-11, the department of Innovation, Science, and Economic Development (ISED) undertook a consultation that involved roundtable discussions across Canada and internationally.[22]

While criticisms could be levied about the inclusion of civil society organizations in those consultations, and the need for updated consultation during the interceding six years between then and the tabling of Bill C-27, at least those consultations provided a basic foundation for which the government could then begin drafting legislation.

---

[21] Centre for Media, Technology, and Democracy at McGill University, *AI Oversight, Accountability, and Protecting Human Rights:* https://www.mediatechdemocracy.com/all-work/ai-oversight-accountability-and-protecting-human-rights-comments-on-canadas-proposed-act

[22] Government of Canada, *National Digital and Data Consultations:* https://ised-isde.canada.ca/site/national-digital-data-consultations/en

When it comes to the *Artificial Intelligence and Data Act* (*AIDA*) no such consultation has taken place. Indeed, there are even mixed reports on whether or not ISED even consulted their own expert advisory panel on artificial intelligence.[23]

OpenMedia agrees that there is a need to regulate emerging technologies like artificial intelligence, but the legislation that creates that regulatory framework must be grounded through engagement with relevant stakeholders. Amongst many other criticisms and shortcomings, AIDA lacks this essential foundation.

### 2. Absence of Independent Regulator

One of the strengths of Canada's privacy regulatory environment is the independent nature of the Office of the Privacy Commissioner of Canada. As an independent Member of Parliament, the Privacy Commissioner of Canada's role was designed to remove potential biases that might emerge as they examine privacy concerns around the processing of personal information by government departments and agencies, and private sector organizations. Notably, the Minister of Justice was not tasked with this responsibility for the public sector, and the Minister of ISED was not tasked with this responsibility for the private sector. Therefore, it seems problematic that the task of regulating an emerging area like artificial intelligence would fall under the portfolio of the ISED Minister (or whomever they delegate this authority to).

To remove the potential of bias, an independent regulator should be tasked with the responsibility of regulating artificial intelligence. Discussion on whether or not this should be an existing regulatory entity, or a new regulator entirely (Canada's Digital Charter mentions the creation of a new Data Commissioner)[24] should be left to the necessary consultations that take place before legislation is proposed.

## *E. Conclusion*

People in Canada deserve privacy laws that actually protect their privacy. Canada's Digital Charter, which Bill C-27 supposedly implements, was framed as introducing new

[23] Government of Canada, *Advisory Council on Artificial Intelligence*: https://ised-isde.canada.ca/site/advisory-council-artificial-intelligence/en
[24] Government of Canada, *Canada's Digital Charter*: https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter-trust-digital-world

rights and protections for individuals. Unfortunately, the reality is that Bill C-27 removes and weakens existing privacy rights for people in Canada, reduces our control over our own personal information, while simultaneously empowering private companies to do more with our sensitive personal information without our knowledge or consent. It begs the question: Is Canada's Digital Charter supposed to empower people or corporate entities? If you look towards Bill C-27 for your answer, it seems clear that the government is more interested in empowering corporate actors than people in Canada.

With significant amendments, Bill C-27's *CPPA* can be restructured and rebalanced to ensure that the privacy interests of people in Canada supersede those of corporate interests. The *PIDTA* is unnecessary and should be removed alongside the *AIDA*, which requires a foundation built on inclusive stakeholder consultation.