

STANDARDS RESEARCH

Exercising Privacy: Policy Options for Privacy and Wellness Wearables

February 2022

Author

Alannah Dharamshi, Springboard Policy

Adrienne Lipsey, Springboard Policy

Project Advisory Panel

Brenda McPhail, Canadian Civil Liberties Association

Christopher Parsons, Citizen Lab

Debra Mackinnon, University of Windsor

Joe Masoodi, Ryerson Leadership Lab

Laura Fadrique, Communitech

Matthew Johnson, MediaSmarts

Teresa Scassa, University of Ottawa

Valerie Steeves, University of Ottawa

Vass Bednar, McMaster University

Victoria Hailey, Victoria Hailey Group Corporation

Hélène Vaillancourt, CSA Group

Tania Donovska, CSA Group (Project Manager)

Financial Support

This CSA Group research report was prepared with generous financial support from the Office of the Privacy Commissioner of Canada's Contributions Program.

Acknowledgements

The authors would like to thank Samantha Coronel for her excellent research assistance. The authors are also grateful to the research interviewees for sharing their expertise and the members of the project Advisory Panel for their input and strategic advice.

Disclaimer

This work has been produced by Springboard Policy and is owned by Canadian Standards Association. It is designed to provide general information in regards to the subject matter covered. The views expressed in this publication are those of the authors and interviewees. Springboard Policy and Canadian Standards Association are not responsible for any loss or damage which might occur as a result of your reliance or use of the content in this publication.

Table of Contents

Executive Summary 5

Introduction 7

About the Report 7

1 The Need to Focus on Wellness Wearables 8

1.1 Wellness Wearables Generate Distinct Information 8

1.1.1 Volume of Information 8

1.1.2 Type of Information 8

1.2 How Different Actors Use Wellness Wearables 9

1.2.1 Consumers 9

1.2.2 Public Health Bodies, Researchers, and Organizations 9

1.2.3 Data Markets 9

2 The Public Policy and Legislative Landscape 9

2.1 Medical Device and Consumer Product Regulations 10

2.2 Health Privacy Legislation 10

2.3 Consumer Privacy Legislation 11

2.4 American Public Policy and Law 11

3 The Privacy Challenges of Wellness Wearables 13

3.1 Information Risks 13

3.1.1 Continuous and Sensitive Information Collection 13

3.1.2 Data Inferences and Re-identification 13

3.1.3 Weak Cybersecurity Practices 14

3.2 Consent Risks 14

3.2.1 Limited Awareness and Understanding 14

3.2.2 Poor Policies and Consent Practices 14

3.2.3 Data Sharing and Secondary Uses 15

3.3 Risks to Other Rights 15

3.3.1 Facilitation of Bias and Discrimination 15

3.3.2 Compromising Security and Safety 15

3.3.3 Restriction of Autonomy and Contextual Decision-making 16

4 Difficult Use Cases for Wellness Wearables 17
4.1 Wellness Wearables in the Workplace 17
4.1.1 Applications of Wellness Wearables in the Workplace 17
4.1.2 Privacy Risks of Wellness Wearables in the Workplace 18
4.2 Wellness Wearables in Insurance 19
4.2.1 Applications of Wellness Wearables in Insurance 19
4.2.2 Privacy Risks of Wellness Wearables in Insurance 20
5 Recommendations to Promote Privacy 22
5.1 Modernizing Privacy Protections 22
5.1.1 Create Protections for Consumer Health-Related Information 22
5.1.2 Enhance and Extend Privacy Protections to All Employees 23
5.1.3 Limit the Use of Wellness Wearable Data in Insurance 24
5.2 Helping Businesses Bolster Privacy 26
5.2.1 Create Standards and Guidance for Best Practices 26
5.2.2 Change How Businesses Relate to Regulators 27
5.2.3 Develop a Pipeline of Privacy Professionals 28
5.3 Promoting Informed User Choices 28
5.3.1 Require Enhanced Notice and Consent Mechanisms 28
5.3.2 Encourage Certification and Labelling 29
5.3.3 Promote Digital Literacy 29
Conclusion 30
References 31

Executive Summary

Wellness wearables are playing a growing role in the lives of Canadians. Manufacturers of these devices and their associated apps are promising a future world of enhanced well-being by enabling users to keep track of and take action on their health and wellness goals.

However, wellness wearables are distinct from other emerging technologies in that they directly connect to the body, generating a high volume of health-related information. They are also of increasing interest to stakeholders beyond consumers and are being applied in contexts where there are power asymmetries and potential misuses. Employers have been incorporating wellness wearables at work, making monitoring more intrusive and continuous. Insurers have also been keen to leverage the real-time data that these devices can generate about policyholders.

Despite these unique aspects of wellness wearables, there has been limited policy development in this area. Instead, these types of devices occupy a regulatory grey area. As neither medical devices nor low-stakes consumer products, wellness wearables are generally excluded from medical regulations and health privacy laws, and they are not sufficiently provided for under consumer privacy laws. Policymakers urgently need to collaborate with industry and civil society to address this gap and implement effective interventions for privacy. If left unaddressed, this will have profound implications as next generation wellness wearables establish even deeper connections to the body, with greater implications for privacy.

This report seeks to contribute to policy development by increasing understanding of privacy challenges and considerations for wellness wearables. It does so by focusing in on **three main areas of risk:** information risks, consent risks, and rights risks. These issues are then explored further through **two use cases** where the application of wellness wearables is growing and poses potential harms: workplace and insurance contexts.

Table E1: Summary of the privacy challenges of wellness wearables

Information risks	Consent risks	Rights risks
Continuous and sensitive information collection	Limited awareness and understanding	Facilitation of bias and discrimination
Data inferences and re-identification	Poor policies and consent practices	Compromising security and safety
Weak cybersecurity practices	Data sharing and secondary uses	Restriction of autonomy and contextual decision-making

The report also identifies several **recommended action areas** where government has the opportunity to implement interventions that address the privacy challenges of wellness wearables. As presented in Table 1, some recommendations target modernizing privacy protections for these devices and their applications in workplaces and insurance. Others focus on helping businesses adopt best privacy practices and on enabling consumers to make privacy choices. While these recommendations cannot eliminate all potential harms wellness wearables pose, they represent important steps to exercising privacy in this arena.

Table E2: Summary of recommended action areas to promote privacy

Modernizing privacy protections	Helping businesses bolster privacy	Promoting informed user choices
Create protections for consumer health-related information	Create standards and guidance for best practices	Require enhanced notice and consent mechanisms
Enhance and extend privacy protections to all employees	Change how businesses relate to regulators	Encourage certification and labelling
Limit the use of wellness wearable data in insurance	Develop a pipeline of privacy professionals	Promote digital literacy



"While most Canadian jurisdictions have privacy legislation that specifically protects health information, wellness wearables generally fall outside the scope of these laws."

Introduction

From wristbands that track steps, to shirts that measure heart rates, to headbands that assess emotional states, Canadians are turning to wellness wearables to quantify, analyze, and act on their health and well-being. One in five Canadians aged 35 to 49 owns a wearable device [1]. And the global fitness tracker market size is expected to grow; it was valued at around USD $18 billion in 2016 and is projected to reach USD $62 billion by 2023 [2]. The COVID-19 pandemic has only accelerated this trend, with consumers turning to wellness wearables and associated apps as gyms and other in-person fitness activities closed across the country [3].

Wellness wearable manufacturers claim their devices will empower users to take a proactive and personalized approach to health by increasing awareness and motivating behaviour change. It's not just everyday consumers who have been keen to realize this promise. Policymakers, employers, and insurers alike are using wellness wearables to promote public health, conduct research, decrease costs, and improve efficiency.

Wellness wearables, however, pose substantial privacy issues. These devices continuously, and often discreetly, track and analyze one of the most intimate sources of information – our bodies. This data is often more similar to personal health information than users realize and provides commercial entities with insight into aspects of our lives that have traditionally been restricted from view. In the age of wellness wearables, our health status and behaviours can be surveilled and leveraged to create profiles that turn a profit and impact our future opportunities.

What's more, Canada's privacy protections offer users weak safeguards from these risks. While most Canadian jurisdictions have privacy legislation that specifically protects health information, wellness wearables generally fall outside the scope of these laws. They occupy a regulatory grey area as the line between medical devices and consumer products becomes increasingly blurred.

About the Report

This report addresses the policy gap by analyzing the privacy implications of wellness wearables and providing recommendations to promote privacy in this space. It explores two use cases where the privacy risks of wellness wearables are prevalent because of emerging popularity and power dynamics: workplaces and insurance. The report addresses privacy related to wellness wearables, rather than for stand-alone wellness apps without associated hardware, because of the distinct risks arising from pervasive and direct body surveillance. It is directed at policymakers concerned with the privacy challenges and opportunities posed by these devices.

The report draws on a variety of research methods including a review of the academic and grey literature, environmental scans of industry practices and government approaches, three advisory panel workshops, and six research interviews. The advisory

panel workshops took place in Summer – Fall 2021 with members from leading universities and organizations. The interviews took place in Summer 2021 with key informants including researchers, a large workplace union, and business leaders in the wellness wearable space. The interviews were conducted using a semi-structured format and on an on-background basis to allow informants to speak freely and openly.

1 The Need to Focus on Wellness Wearables

Wellness wearables are a growing category of consumer devices worn on the body – from wristbands like Fitbit [4], to clothing like Hexoskin [5], to headbands like Muse [6]. These devices are part of the broader Internet of Things (IoT) and are marketed as helping wearers track their fitness and other metrics of well-being. They are equipped with sensors that capture data about users in real-time as they move through their daily lives [7]. This data is generally sent to an associated app [8], typically stored remotely in online databases, and brought back to the app for presentation. The devices and apps often apply algorithms that translate the data into insights that are meant to spur users to achieve their wellness goals [9].

While diverse in form, wellness wearables share characteristics that warrant particular attention from a privacy perspective. First, these devices collect, analyze, and share high volumes of sensitive information about the body. Second, wellness wearables and the information they generate are of growing interest to diverse actors for a wide range of purposes and applications.

1.1 Wellness Wearables Generate Distinct Information

Unlike other technologies, wellness wearables are uniquely connected to the body. As such, these devices are distinct in terms of the volume and type of information they can generate.

1.1.1 Volume of Information

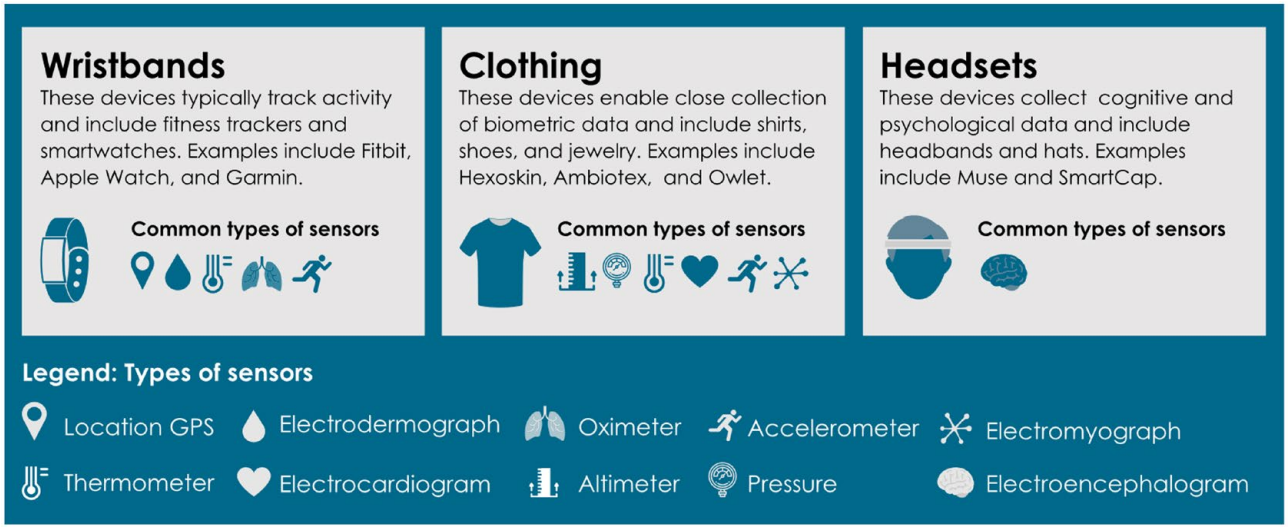
Wellness wearables require massive quantities of information to function; data collection is central to their value [9]. They are specifically designed to be worn constantly by users, allowing them to gather even more data than some other IoT technologies and enabling round the clock generation of user data [10]. This pervasive and passive monitoring, along with active information disclosure in apps by users, generates an extremely high volume of information [11].

1.1.2 Type of Information

This data is particularly sensitive. Wellness wearables extend the abilities of stand-alone wellness apps by collecting information directly from the human body [12]. These devices sense biometric, physiological, and behavioural information about individuals that is similar, or sometimes identical, to data from medical devices [13], [14]. As shown in Figure 1, wellness wearables use various sensors to generate this health-related information. For example, accelerometers are used to track physical activity and thermometers are used to track fertility cycles [15]. Some wearables are even being used for "affective computing," collecting cognitive data to analyze and sense emotional states, including indirectly through inferences [16], [17].

This type of health-related information has generally been considered highly sensitive, given the potential for discrimination, embarrassment, and other economic, social, or psychological harms if disclosed [18]. Research shows that people perceive technologies in contact with our bodies as "creepy," a perception that is doubly the case for wearables and other technologies using psychological sensing [19]. Data about bodies is felt by many to be in a special class of sensitivity. Take, for instance, information about sexual activity. The wearable Fitbit previously allowed users to track this kind of health-related information. In its early days, the company made user profiles public by default, meaning that users' profiles and recorded sexual activity could be found in Google Search results [20]. While the company has since changed this practice, the case demonstrates the privacy risks associated with health-related information. Access to this type of data has typically been restricted to health care contexts, but wellness wearables are now bringing this information into the commercial space.

Figure 1: Examples of wellness wearables, adapted from Piwek et al. (2016)



1.2 How Different Actors Use Wellness Wearables

Wellness wearables and the information these devices generate are of interest to many different stakeholders for different purposes.

1.2.1 Consumers

Wellness wearables are largely marketed for individual consumer use. By motivating behaviour change, these devices claim to help individuals proactively enhance their well-being [8]. However, evidence on their efficacy is mixed. There have been few studies on the long-term impacts of using wellness wearables [15]. Results are also mixed for device accuracy; a 2020 study of consumer activity trackers found that while most devices measured steps accurately, there was variable accuracy for heart rate tracking and inaccuracy for calories burned [21].

1.2.2 Public Health Bodies, Researchers, and Organizations

In public health, wearables have been considered to help decrease costs and admissions into the healthcare system [22]. For example, wearables have been used by authorities during COVID-19 for activities such as quarantine monitoring and biometric surveillance [13]. In academia, wellness wearables are providing medical and health researchers with large quantities of health-related data not readily available in laboratory settings [23]. For example, researchers have used Fitbit data to track recovery from COVID-19 and long-term effects [24].

1.2.3 Data Markets

In today's data economy, the uniquely high volume of sensitive health-related information about the body that is generated by wellness wearables is valuable and can be monetized [25], [26]. Manufactures of these devices stand to benefit from leveraging users' data as an asset, by selling it directly or selling de-personalized aggregated insights to data brokers and other third parties.

2 The Public Policy and Legislative Landscape

Wellness wearables occupy a regulatory grey area in Canada, with privacy protection gaps. Neither true medical devices, nor low-stakes consumer products, wellness wearables are not captured by Canada's medical regulations and health privacy legislation, nor are many of their risks specifically addressed under consumer privacy law. Further, because data can move from Canadian consumers' devices to companies and servers in the United States (US), American public

policy and legislation is also relevant. However, in the US, as in Canada, wellness wearables exist within a regulatory gap: they are not captured by medical device regulation, nor subject to specialized consumer protection.

2.1 Medical Device and Consumer Product Regulations

Canada has a robust regulatory regime overseeing medical devices. However, to be captured by Health Canada's regulations under the *Food and Drugs Act,* a device must be intended to help diagnose or treat a specific medical condition [27]. The thrust of this regime is to ensure device safety, efficacy, and quality so that it doesn't undermine a person's treatment or diagnosis [28]. Although regulation doesn't include detailed privacy rules, it does set clear cybersecurity standards that devices must meet [29]. Many of these types of medical devices also require a Canadian Medical Device License issued by Health Canada to be sold in the country [30]. More recently, Health Canada has created a new Digital Health Review Division to increase its pre-market review capacity for emerging digital health technologies, including those using platforms, smart phones, and wearable devices [31].

However, wellness wearables are not considered medical devices under federal regulation because their manufacturers do not make claims about their ability to treat or diagnose specific conditions [25]. Yet some devices — for example, those that measure heart rate or blood pressure — provide similar information to medical devices. Instead of being classified as medical devices, wellness wearables are subject to the *Canada Consumer Product Safety Act* [32], also administered by Health Canada, which applies more generally to all kinds of consumer products – from paint to toys. This legislation focuses more on the physical safety of products and has no specific regulations for cybersecurity, wearable devices, or IoT more broadly.

2.2 Health Privacy Legislation

Almost every province and territory has developed privacy legislation specifically concerned with protecting personal health information [33]. For example, Ontario has the P*ersonal Health Information Protection Act* (PHIPA) [34] and Alberta has the *Health Information Act* [35].

However, these provincial laws generally do not apply to personal use of wellness wearables. Health privacy legislation prescribes and limits how particular people and institutions can collect, keep, and handle health information. It is concerned with regulating specific actors within the healthcare system (e.g., medical practitioners) who are custodians of the data. Under this current-state, data from wellness wearables is only protected as personal health information when in the hands of a custodian. When the exact same information is outside the medical system — for example, on a personal device or app — provincial health privacy law does not apply.

Research interviewees highlighted that many health privacy laws were designed in an era when only a handful of formal health authorities were collecting personal health information. Yet medical and medical-adjacent information is now routinely created and handled by private actors. Policymakers have started to account for this in health privacy legislation. For instance, Ontario's PHIPA has been amended to include a new class of actors: consumer electronic service providers. These entities are defined as providing electronic services to individuals that allow them to "access, use, disclose, modify, maintain or otherwise manage their records of personal health information" or "such other purposes as may be prescribed" [36].

While this amendment, not yet in force, was created within the context of giving Ontarians a right to access their personal health information records in an electronic format, via patient portals and health apps [37], its broad language may increase the scope to include any entity involved in a platform that allows for management of this type of information [38]. For instance, in an explanation of consumer electronic service providers, the Information and Privacy Commissioner of Ontario notes how "an individual might use a smartphone app to store information about their blood sugar levels" [39]. Because this new provision is not yet in force, regulations have not yet been developed to define scope nor requirements for this new class of providers. Until these are in place, it remains to be seen what the implications of this amendment are for consumer wellness wearables and their associated apps.

2.3 Consumer Privacy Legislation

While generally excluded from health privacy laws, wellness wearables do fall under federal and provincial consumer privacy legislation. Canada's federal consumer privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA) [40], governs how wearable companies can collect, use, and disclose personal information. Some provinces including Alberta [41], British Columbia [42], and Quebec [43], also have private sector privacy laws that have been deemed substantially similar to PIPEDA. Within these jurisdictions, the provincial laws typically govern the private sector instead [44], including companies that develop and use wellness wearables. Of these statutes, Quebec's has been recently reformed to align more with the leading international data protection law, the European Union's (EUs) General Data Protection Regulation (GDPR) [45]. While these provincial privacy laws do apply in the wellness wearables context, the scope of this report will predominately focus on the federal legislation.

One of the basic mechanisms of PIPEDA is consent, giving individuals the right to accept or decline the collection, use, and disclosure of their data. However, meaningful consent can be hard to achieve under new business models and technologies like wearables [46]. PIPEDA offers some provision for enhanced protections related to "sensitive information"; organizations must protect personal information in a way proportional to the sensitivity of that information and seek express consent when the information is likely to be considered sensitive. However, the term "sensitive information" is not defined in legislation. While the Office of the Privacy Commissioner of Canada (OPC) has released guidance suggesting that health and biometric data are likely to be considered sensitive, it emphasizes that there is no "bright line" to delineate what is or is not sensitive [47]. It is not yet clear whether "health data" means data related to treatment and diagnosis, data collected by custodians, or the data from devices like wellness wearables.

The federal government has taken steps to design a replacement to PIPEDA that would react to the context of emerging technologies, including IoT devices like wellness wearables. Prior to the 2021 federal election, Bill C-11, the *Digital Charter Implementation Act, 2020,* was before Parliament [48]. Bill C-11 aimed to replace PIPEDA with the proposed *Consumer Privacy Protection Act* (CPPA) and the *Personal Information and Data Protection Tribunal Act.* However, critics of Bill C-11, including the OPC, have argued that despite some strengths, in some ways it represented a step back for privacy protection [49]. Particularly relevant for wellness wearables, interviewees for this report and other scholars have highlighted that it still did not define sensitive information, meaningfully enhance transparency requirements around how data is used, or adequately address automated decision-making [50]. Moreover, Bill C-11 would have introduced a long list of exceptions to knowledge and consent requirements, including for business activities such as activity deemed necessary for the safety of a product [48]. What's more, without knowledge of these exempted activities, it would be difficult to hold organizations accountable [51].

As new consumer privacy legislation may be considered in the future, there are further opportunities to modernize and enhance consumer privacy protections in Canada for the digital age. Later in this report, some recommendations are made on how next generation privacy legislation might be designed to consider the risks of wellness wearables.

2.4 American Public Policy and Law

While Canadian law and policy govern how companies interact with Canadian consumers, in practice the data from wellness wearables is often controlled by American companies and stored in the US [52]. Most popular wellness wearables in Canada, like Fitbit and Garmin, are produced by US-based companies. At the same time, many Canadian companies in the wearables industry are start-ups very likely to be acquired by American or international firms. [17]. When this happens, Canadian user data can be shared with new ownership without notification or new consent from users [17]. While PIPEDA will apply to US-based companies where there is a real and substantial connection to Canadian consumers [53], investigating international complaints and enforcing orders can be difficult and complex. In this context, it is also important to consider the American public policy landscape.



"Policymakers and legislators should note that Canada's privacy regime is not neutral, and instead must always rest on one or another normative model."

In the US, there is also a privacy protection gap for wellness wearables and associated apps. Like its Canadian counterpart, the US Food and Drug Association does not treat wellness wearables as medical devices [54]. Likewise, American federal health privacy law only applies to certain types of entities, like medical facilities or insurance companies, rather than private firms that develop wellness wearables outside the traditional health system [22]. While the Federal Trade Commission has expressed concern about wearables and privacy, it has not provided regulatory guidance for data generated from these devices [55], [56]. The result is that American companies are generally fairly free to use sensitive data generated by wearables worn by Canadians. However, California has recently developed a modern consumer privacy law, the *California Consumer Privacy Act* [57], which has complicated the American privacy landscape and imposed stronger obligations on companies operating in that state, which includes many technology companies.

Models of Privacy

This report is about privacy and wellness wearables. Privacy, however, is not a neutral concept, and there are at least two leading approaches to considering what it means.

The individual approach focuses on a person's rights to share or not share information about themselves. In this model, there is a line between the private and public spheres. In the public sphere people have little privacy. In the private sphere they have a great deal, and crucially, should be in control of who knows what about them. Consent is a key part of this approach: in this model people allow intrusions into their private sphere by trading their information in exchange for benefits. For the most part, Canadian law and policy rest on an individual approach to privacy, placing a high degree of importance on individual consent to share information or not.

The other general model is **the social approach.** Instead of privacy being exercised by individuals making their own choices about what to share about themselves, in this model privacy is made — or violated — through social expectations. For example, a couple on a bench, in public, do not expect a stranger to sit next to them and listen to what they're saying. The privacy they expect is not based on a distinction between the private and the public sphere, or their right to consent or not consent to someone sitting on the bench. It comes from the context of who is in their relationship and who is not. This privacy is also not individual: the couple have created privacy between them. This perspective is gaining importance and popularity [58].

This report does not advocate for one approach over the other. But policymakers and legislators should note that Canada's privacy regime is not neutral, and instead must always rest on one or another normative model. In most cases, the status quo of this regime rests on the individual approach. This report considers the ways in which this does or does not reflect Canadian consumer's interests in respect of wellness wearables.

3 The Privacy Challenges of Wellness Wearables

Until Canadian privacy law is reformed, the challenges to privacy posed by wellness wearables continues to grow, with consequences for users. The special characteristics of wellness wearables — the fact that they collect information about people's bodies, and such a large quantity of it — create three types of challenges for users as shown in Table 1: information risks, consent risks, and rights risks.

3.1 Information Risks

The main value proposition of wellness wearables is that they enable individuals to collect, analyze, and share information about themselves easily and continuously. The more individuals measure and learn about themselves using wellness wearables, the more they provide information about their bodies to manufacturers, and sometimes third parties.

3.1.1 Continuous and Sensitive Information Collection

As described above, wellness wearables are always on, enabling the constant collection of vast quantities of information about individuals. Constantly worn, constantly tracking, ubiquitous surveillance is a core feature of the devices' functionality but is often invisible and unclear to everyday users [9]. These devices can sense and process information discreetly and in ways that are often hard for users to recognize and understand [14]. What's more, wellness wearables are different from other IoT devices in that they collect health-related information directly from and concerning the body. Many wellness wearables also collect constant location information. Yet, this is not new — plenty of smartphone apps collect location data — this information poses special risks in that it can be tied to other data to reveal whom individuals meet and further information about their health status and activities [55], [59].

3.1.2 Data Inferences and Re-identification

Wellness wearables can create a detailed portrait of users beyond the information collected by the device. Analysis of wellness wearable data using artificial intelligence, especially when combined with information from other sensors, devices, and sources, can generate detailed inferences about users from seemingly innocuous information [60], [61]. For instance, even without GPS, location and movement patterns can be extracted from other sensors like accelerometers and gyroscopes [17]. These patterns can be used to draw conclusions about users' emotional states like stress or anger [17].

The types of data collected add to the risk that anonymized information can be re-identified. For instance, sensory data like prolonged speaking and elevated stress can be used to infer public speaking [60]. This insight can then be combined with public information like records of university lectures to re-identify an individual wellness wearable user. Common techniques used to counter such re-identification are hard to apply to the sensor data from wearables because of the distinct combinations of health attributes they measure [60], [61]. This is a privacy concern because users typically have a low understanding of the ways in which their raw data can be combined with other information, and the innovative ways in which that combination can change over time.

Table 1: Summary of the privacy challenges of wellness wearables

Information risks	Consent risks	Rights risks
Continuous and sensitive information collection	Limited awareness and understanding	Facilitation of bias and discrimination
Data inferences and re-identification	Poor policies and consent practices	Compromising security and safety
Weak cybersecurity practices	Data sharing and secondary uses	Restriction of autonomy and contextual decision-making

3.1.3 Weak Cybersecurity Practices

Wellness wearables and their associated apps are often insecure. These types of technologies may expose user data in several ways — from poor security practices of the device itself, the cloud where data is stored, and the connections between different IoT products [62]. For instance, a 2016 study on popular fitness trackers found that many of the most popular devices do not employ basic data transmission security practices and have other vulnerabilities that expose user data to surveillance or tampering by unauthorized third parties [59]. Similarly, a study on consumer smartwatches for children has shown that these devices have serious security flaws and can be easily hacked [63]. Researchers have found that some wearable devices like smartwatches can be exploited to crack Personal Identification Numbers (PINs) and passwords with 80% accuracy on the first try [64], [65]. Unlike the operating systems of computers and smartphones, wellness wearables are typically not designed to be constantly updated to fix security problems as they emerge once devices are released in the consumer market [61], [66]. Because they collect vast amounts of data from users, fitness tracker companies are attractive targets for government agencies and criminal organizations [67].

3.2 Consent Risks

Notice and consent are key cornerstones of most privacy protection approaches in North America, and they form the bedrock of PIPEDA. The premise is that if consumers are provided with adequate information, they can make their own choices about their privacy and personal information [68]. Wellness wearables pose several challenges to the current consent paradigm — ranging from a lack of user awareness to constraints on choice, to unclear secondary uses of data. It may be that privacy legislation following this consent model is insufficient for wellness wearables, and perhaps today's technology at large.

3.2.1 Limited Awareness and Understanding

Informed consent assumes users fully understand how their data will be used, shared, stored, and any associated risks. Research shows, however, that people who use wearables tend to have only partial understanding about privacy, its implications, and risks [69]. Wearables are intentionally designed to be unobtrusive and easily blend into the background, making users less attuned to the data being collected [70]. Unlike other IoT devices, many wellness wearables, such as shirts or jewelry, are screenless or lack an interface on the device, meaning some users are unclear about the extent of invisible data generated and some feel as though they do not need to be as concerned about their privacy [14], [71].

This potential for harm is compounded by the particular ways in which information about the body can be combined with other information to draw inferences. Not only do people have a low understanding of what data is being collected, they also do not understand how it can be used. Research suggests people are uncomfortable when they learn that that data from their fitness trackers, combined with other contextual information like the proximity of other people's phones, can yield insights about things like who they are talking to and their emotional state [60]. These types of inferences are often central, rather than incidental, to the business models that undergird wellness wearables.

3.2.2 Poor Policies and Consent Practices

Because wellness wearables must be small enough to be worn comfortably, they often lack practical ways to display privacy notices on the device itself [72]. This means users have to find them in other places like the manufacturer's website and as a result are even less likely to read them [72], [73]. The physical characteristics of wellness wearables exacerbate a problem common to IoT devices and wellness apps. A 2014 review of IoT devices found that none included privacy-related information or direction to a privacy policy located on either the box, packaging, or user guides [61]. Similarly, a 2013 study of health and fitness apps found that only 43% of free apps and 25% of paid apps analyzed provided a direct link to a privacy policy on the developer's website, while the rest required users to locate this information themselves [74].

It is well documented that privacy policies in general do a poor job of setting the groundwork for consent. A 2019 review of 150 privacy policies found that most were "an incomprehensible disaster" [75]. For wellness

wearables, the OPC has found that "the privacy communications for many health and wellness devices [...] don't adequately explain personal information collection, use and disclosure practices" [76].

What's more, most privacy policies are written in all-or-nothing terms, where users are not given any granular options on how to modify their consent at a later point in time, meaning users must agree to all terms or else not use the device. Not using devices becomes harder as they become more prevalent, and, sometimes, engrained in relationships with employers and other institutions [22], an issue discussed in more detail below. It may also be hard to stop using wearable devices that have become a tool supporting healthy habits and represent months or years of time invested in tracking.

3.2.3 Data Sharing and Secondary Uses

Both the raw and analyzed data from wellness wearables and associated apps may be shared with or sold to third parties, whose identity is often not disclosed to users [77]. The market for this information is vast, as data is an increasingly valued commodity or asset [78]. Unlike most physical commodities, it is abundance rather then scarcity that gives data greater value. Even a "surplus" of data has enduring utility, as it forms the basis of inferences. Data from wellness wearables is particularly prized because the information they collect has not previously been commercialized or available to actors outside the health care system [25]. Parties interested in this information include data brokers, advertisers, insurers, pharmaceutical companies, employers, financial institutions, universities, and government [55]. Developers of wellness wearables and these third parties may use the data collected from devices in ways that are beyond the original stated purpose, creating new privacy threats users could not have considered when providing their consent [13], [79].

3.3 Risks to Other Rights

According to the UN Special Rapporteur on the Right to Privacy, the right to privacy enables "the free development and expression of an individual's personality, identity and beliefs, and their ability to participate in political, economic, social and cultural life" [80]. While privacy concerns associated with wearables are tied to many human and civil rights, this report focuses on areas of anti-discrimination rights, rights to physical safety, and autonomy and decision-making restrictions.

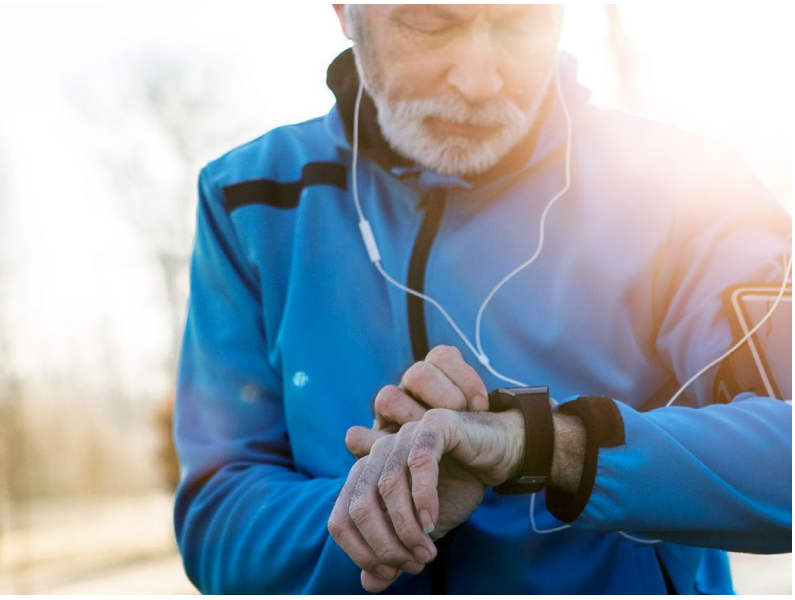
3.3.1 Facilitation of Bias and Discrimination

As devices that collect a deep wealth of data and feed it into algorithms, wellness wearables are subject to the many pressing concerns around bias in artificial intelligence, including biased data and outcomes, and "black box" processes [81], [82]. Wellness wearables, however, pose unique problems for bias and discrimination. One aspect is bias in the way sensors work, and how people's habits and indicators are interpreted. For example, Fitbits can register wheelchair users' movements, but warn that measurements may be inaccurate, and call these movements "steps" [83]. Other researchers have found that consumer wearable devices may also not be as accurate for people with darker skin tones [84]. This is a privacy issue partly because it means that, under the consent paradigm of privacy, some people are getting less benefits than they expect, while giving away the same information as others. The consent paradigm also requires knowing how one's information will be used, which is difficult when technologies interpret it inaccurately.

Privacy rights also protect people from discrimination based on their data. Wellness wearables generate huge amounts of information, which can easily be used for profiling and overt discrimination or discriminatory impacts. Because the data they collect relates to people's physical capacities and habits, wellness wearables could be used to discriminate against people based on health status, medical condition, and disability or perceived disability [22]. This is most clear in contexts like employment or insurance, described in more detail below.

3.3.2 Compromising Security and Safety

Wellness wearables can easily be misused to perpetrate intimate partner and gender-based violence, and enhanced privacy protections can act as a bulwark against this. Information about location,



"Because the data they collect relates to people's physical capacities and habits, wellness wearables could be used to discriminate against people based on health status, medical condition, and disability or perceived disability."

physical activity, vital signs, or habits can be misused to threaten or harm users [85]. One key hallmark of intimate partner violence is tracking or managing the abused partner's location, something wellness wearables can enable via associated GPS tracking technology. This can be misused by abusive partners to stalk, control, and monitor survivors' movements. It can also create opportunities to assault people when they are likely to be alone. For example, Strava, a fitness app that can be connected to fitness trackers, previously made location heatmaps of users public by default [52]. This is a troubling fact when taken with reports that 60% of women have been harassed on runs and 26% have been followed [86].

That same GPS data can also create threats to national security. For example, when Strava data was public by default, it was used to reveal the locations of secret military bases where staff were exercising [52]. Experts interviewed for this report raised concerns about detailed, and potentially embarrassing, location data leaving high ranking government officials open to blackmail from foreign operatives. Data from fitness trackers can also be used to draw inferences about sexual activity and infidelity, [87] which can also be used to exploit high ranking officials. While wellness wearables are far from the only devices to track GPS location, they are unique in that they are often meant to be worn at all times, including during sleep, which means the magnitude of data collected is an order higher than in other cases.

3.3.3 Restriction of Autonomy and Contextual Decision-making

As described above, there are different ways of understanding privacy. Wearables pose challenges for each model. On the one hand, in the individual approach, privacy can be about defining private spheres of life, to communicate and move through spaces freely, and to make autonomous choices without interference [88], [89]. The use of wellness wearables and other IoT products puts these other aspects of privacy at risk by breaking down the boundary between public and private spaces [90]. Because these devices are always on, they weaken people's ability to maintain boundaries and ultimately choose when and where to be left alone [73].

According to the social approach, the right to privacy is not just about controlling personal information. It is also about the ability to make decisions about which way information should flow and what is appropriate to share in different situations [91]. But given that agreements between wearables manufacturers and users depend on blanket-consents, users are unable to guide the flow of their information to vary by context.

This could have chilling effects on behaviour and open opportunities for consumer manipulation. For example, research interviewees raised concerns about the potential for law enforcement to use information from wellness wearables to locate and track individuals as they move through their private lives. Others have raised concerns about the potential of wellness

wearables and the sensitive real-time data they collect to be used for hyper-personalized advertising, including advertising for products through push notifications on devices like armbands worn directly on the body [22]. This has potential implications for the ability of consumers to freely make choices.

4 Difficult Use Cases for Wellness Wearables

Wellness wearables can pose privacy challenges wherever they're used. However, in particular contexts, these potential privacy intrusions can be exacerbated by existing power asymmetries, further entrenching these dynamics. For instance, wellness wearables are increasingly being used in workplaces and by insurance companies, situations where a) employees and consumers respectively have constraints on their bargaining power, and b) where the collection, use, and sharing of their sensitive information can lead to privacy harms. Policymakers should consider the special problems of wellness wearables in these use cases.

4.1 Wellness Wearables in the Workplace

Workplace surveillance is nothing new – from time clocks to performance assessments, employers have long been keeping track of their workers. However, the use of technologies like wellness wearables is taking employee monitoring to unprecedented levels, enabling more continuous and intrusive kinds of tracking and analysis. Leading manufacturers are now actively targeting enterprises to bring wearables into the workplace in their efforts to expand beyond consumer markets [17]. Employer appetite for these types of technologies has only increased during COVID-19, with implications for privacy and other labour rights [92], [93].

4.1.1 Applications of Wellness Wearables in the Workplace

While wearables are being used in employment contexts for many different purposes, including as a means of enforcing the mechanics of physical distancing and assessing employee productivity, this report specifically focuses on wellness in the workplace. It assesses the privacy implications of two applications: corporate wellness programs and workplace health and safety programs.

Corporate Wellness Programs

Wellness wearables are increasingly a part of the corporate wellness landscape. Canadian organizations like BP Canada have already integrated these types of devices into their corporate wellness initiatives [94]. At the same time, companies dedicated to providing offerings for these types of workplace programs are emerging. For example, Canadian company Sprout Wellness Solutions offers Sprout At Work, a corporate health and wellness platform that includes health risk assessments using physical activity and wellness wearable data [95], [96].

While program approaches vary by workplace, a common model is having employees opt-in to a gamified, competitive program where groups work together and against other parts of the organization to "win" by some metric — most steps, most active minutes, etc. The objective could be fundraising for a cause or general workplace health promotion [97]. Some plans use data from wearables to incentivize change, rewarding employees with gift cards and discounts [70].

The potential benefits of wellness wearables include improved employee well-being and morale. Employers are meant to benefit in part because a healthy and active worker is assumed to be more productive and less likely to use sick leave [97]. Fitness trackers might also be adopted in group insurance plans, with a view to potentially reducing employer health benefit costs by improving well-being [98]. However, it is not clear whether these purported benefits actually flow from the use of wearables in corporate wellness plans. Research indicates that employees who opt-in to using corporate wellness plans in general tend to already be healthier, with lower medical expenditures, than those that do not opt-in [99]. At the same time, there is evidence that pervasive employee monitoring can negatively impact morale, including higher employee stress levels and diminished trust towards management [100].

Workplace Health and Safety

Wearables are also used for health and safety in sectors where fatigue, proximity to dangerous equipment, or being unaccounted for on the jobsite can be work hazards. These types of devices include mining helmets that monitor ambient conditions and workers' vitals [101], along with smart watches that track location and shut down machines when employees are in danger [102]. Wellness wearables have even been implemented to identify and track health conditions. For example, WHOOP Strap, a fitness tracker, was used to monitor over 5,000 construction workers at Expo 2020 Dubai. It tracked cardiovascular health and sleep, including identifying workers who need to take precautions at work due to underlying conditions like heart-rate variability [103]. Similarly, corporations are looking to LifeSignals' disposable skin patch, which has an integrated biosensor, to monitor employees for early signs of COVID-19 [103].

However, many of these wearable devices serve dual purposes. Not only are they used to help protect workers' health and safety, but also to provide data to make them more productive. For example, the smart watch that shuts down dangerous machines can also be used to count how many steps workers need to do particular tasks [71]. These wearables allow employers to articulate, in minute detail, not only what workers must do, but also exactly how they should do it.

4.1.2 Privacy Risks of Wellness Wearables in the Workplace

These applications of wellness wearables in the workplace challenge workers' privacy. Employee privacy in Canada is already complex. It is governed by a patchwork of laws that offer more or less protection depending on the jurisdiction and workplace sector. For instance, PIPEDA applies to the federally regulated private sector workplaces [44], while substantially similar data protection legislation in Alberta [41], British Columbia [42], and Quebec [43], apply to respective provincial private sector jobs. At the same time, federal and provincial public sector privacy laws apply to government employees in their respective jurisdictions [104]. Unionized employees may receive distinct privacy protections as well, under collective agreements [105].

However, across these instruments, employers are generally provided with significant scope to monitor their employees, as long as it can be linked to legitimate business purposes [104]. Current legislation lacks specific provisions for electronic employee surveillance [106], and a framework to address emerging technologies like wearables that do not just track employees, but also use artificial intelligence (AI) and analytics to assess them [107]. Within this context, wellness wearables generate unique privacy risks to worker information, consent, and associated rights.

Information Risks

Wellness wearables bring health-related data directly generated from workers' bodies into the hands of employers [108]. Employers must follow strict rules when accessing this information from health information custodians [109], but these conditions do not apply to consumer and enterprise wearables at work. Even more, when employees are encouraged to track their steps and meet step goals, it's predictable that they will wear devices at home and on the weekends, blurring distinctions between work and personal spaces [70]. This raises questions about how equipped employers are to keep-private and handle huge quantities of sensitive information about employees, collected both during and outside-of-work.

Consent Risks

The collection, use, and sharing of personal information is generally subject to knowledge and consent requirements, with express consent for sensitive information [110]. However, there are different pressures in the workplace than in private life that impact consent. There is unequal power between employers and employees [106], meaning workers might not be making full and free choices regarding the use of wellness wearable devices at work. Employees may feel they have to consider not just their own desire to track fitness, for example, but also their desire to avoid any potential consequences of refusal [107]. What's more, privacy statutes in Canada contain several exceptions to consent that might apply to wearables in

the workplace. For example, under many private sector privacy laws, consent is not required when the purpose is necessary to establish, manage, or terminate an employment relationship [106], [107].

There are limits on the extent to which employers can collect, use, and disclose the information collected by emerging technologies like wellness wearables [111]. Even with consent, employers can only collect information for purposes that a reasonable person would consider appropriate under the circumstances [104], [112], and more recent analysis has focused on whether the surveillance act itself is reasonable [113]. So, for instance, while the workplace environment and consent to company policies may diminish an employee's reasonable expectation of privacy, it does not extinguish it. While this caveat is important, it is ambiguous, and it is not yet clear whether and under what circumstances it is reasonable for employers to gather information generated by wellness wearables in the workplace [17].

Rights Risks

In Canada, it is illegal to discriminate against employees based on several prohibited grounds, including disability [114]. This means that employers cannot legally leverage this data from wellness wearables for decisions like hiring, raises, etc. However, despite restrictions, wearable information could still potentially be used not just for wellness purposes but to discriminate and treat employees unfairly [100]. For instance, it is possible that wellness wearable information about healthy or unhealthy behaviour could lead to being promoted or demoted or fired [115]. Data could also be used to discriminate based on predictions or inferences about certain conditions, behaviour, or outcomes, like a worker's potential pregnancy or their predicted risk of injury [71]. Protecting people's privacy and setting limits on employers' access to and use of information can prevent discrimination.

Apart from discrimination, the use of wellness wearables at work generally gives employers access to information about employee's whereabouts. This could further weaken workers' negotiating powers [100].

For instance, wearables with GPS at work could have implications for collective bargaining, as employers could see which employees regularly attend union meetings [71], or who regularly meets in a workplace that is trying to unionize.

4.2 Wellness Wearables in Insurance

The insurance industry has historically collected information when on-boarding clients to make underwriting assessments. However, IoT technologies like wellness wearables are increasingly being integrated into service offerings, enabling more continuous and real-time data collection about policyholders — from home insurance that uses smart-home devices to car insurance that uses sensors to monitor driving behaviour [116], [117]. This trend has been rapidly expanding into health and life insurance.

4.2.1 Applications of Wellness Wearables in Insurance

Traditional health and life insurance has typically been based on one-time data snapshots from self-administered questionnaires, clinical exams, and medical information releases [118]. Once a premium is set, there is typically little a policyholder or the insurer can do to change it. However, emerging interactive health and life insurance products that integrate wellness wearable devices and associated apps are changing this dynamic. This report assesses the privacy implications of the use of wellness wearables in these new types of insurance products.

Wellness Wearables in Interactive Health and Life Insurance

Interactive health and life insurance targets both individuals and group benefit plans. These programs include wellness wearable devices and apps that enable the continuous collection of health-related information about users [55]. The data is then analyzed and informs ongoing assessments of policyholder well-being. This wellness monitoring is used to help incentivize healthier behaviours amongst customers, thereby reducing risk and potential costs to the insurer, through rewards like gift cards and discounts on premiums [55], [119].



"Wellness wearables enable insurers to access greater volumes of granular personal and health-related information about policyholders and beneficiaries than ever before."

These types of interactive insurance policies have been most common in other jurisdictions like the US [100]. They also have greater implications in other countries have no publicly-funded health system. However, there is still a substantial market for private health and life insurance in Canada and the industry has been moving into the interactive space. For example, since 2016 consumers at Manulife Financial can sign up for the organization's *Vitality Program,* which enables members to track their health improvement efforts by inputting information into the program's app or by synching it with a wellness wearable device [120]. Members earn points for these activities, and then use them for rewards [121] including an up to 10% discount on the annual cost of a policyholder's insurance and gift cards, or special pricing for products [122], [123].

Using wellness wearables in insurance plans is often marketed as a "win-win," with benefits for policyholders and insurers. Under this model, users have the opportunity to improve their health and well-being while earning rewards and discounts. Insurers then benefit by gaining a portfolio of clients who may be healthy and long-lived, therein decreasing costs of service provision [124]. Of course, these anticipated benefits may not be realized due to a number of issues, including the potential for inaccuracy of device readings, inequity in program design, and focus on only quantifiable aspects of health [125], [126].

We also heard from research interviewees that insurance companies can have additional motivations for these programs. For instance, they also benefit by building strong, ongoing relationships with clients through app-based wellness programs. There is also speculation on the future potential of continuous underwriting, wherein real-time data from wellness wearables could be used to drive dynamic adjustments to premiums based on policyholders' health and behavioural changes throughout the life of the policy [127], [128]. This is not currently a reality in Canada when it comes to wellness wearables, and industry experts we talked to made it clear there is a hard division between wellness programs and underwriting.

4.2.2 Privacy Risks of Wellness Wearables in Insurance

The use of wellness wearables in interactive health and life insurance policies can also create challenges for consumer privacy. Oversight of the industry is shared between federal and provincial jurisdictions, with a large majority of insurers in Canada regulated by the federal government [129], [130]. In terms of privacy then, insurance firms, like other commercial actors, are subject to PIPEDA and, where relevant, the substantially similar provincial consumer privacy laws [131]. While insurers are not custodians under provincial health privacy laws like Ontario's PHIPA, these statutes contain provisions that apply to companies when they access health information from formal custodians. Additional protections are also provided under the Genetic Non-Discrimination Act, which prohibits requiring or sharing genetic test results as a precondition of insurance [132]. Within this context, wellness wearables still stand to generate unique privacy risks to policyholder and beneficiary information, consent, and associated rights.

Information Risks

Wellness wearables enable insurers to access greater volumes of granular personal and health-related information about policyholders and beneficiaries than ever before. By gathering this type of sensitive information directly from individuals, not formal medical information releases, these firms are able to bypass the laws and procedures in place that protect individuals when data is retrieved from health information custodians [25].

Policyholders may also not be aware of the extent to which their information is collected, how it can be used, and the types of inferences or insights that can be generated from their data. For instance, location tracking functions wellness wearables can suggest health conditions or lifestyle circumstances that users might not otherwise knowingly disclose to their insurance providers [55]. As above, it is clear some insurers create a division between wellness programs and underwriting. One best practice is to store the health data generated by wellness wearables and apps with outside partners, and limit insurers' access to the general health status ranking of each policyholder and aggregate information about customer segments. This is currently a voluntary, rather than a legislatively required, division.

Consent Risks

As it stands, interactive insurance policies and wearable use are voluntary. However, there is concern that these programs may become mandatory in the future or that in practice, users may have no real choice other than to participate as firms transition to these offerings [126]. For instance, John Hancock, a subsidiary of Manulife Financial and one of the oldest and largest insurers in the US, has already moved to offering interactive insurance policies only [133]. Additionally, there is concern that financial incentives such as discounts on premiums could become so large as to make non-participation in programs overly burdensome, undermining meaningful consent, although this is more of concern in the US where insurance takes the place of publicly funded healthcare.

Another consent issue is the impossibility that data and insights generated by these devices could be sold to third parties like advertisers and used for secondary purposes [25]. In the context of group plans, there is also concern that information about employee beneficiaries might be disclosed to employers. However, even with user consent, insurers, like employers are still subject to the "reasonable person" test when it comes to the collection, use, or disclosure of personal information [131]. Further, interviewees from the insurance sector were emphatic that in current practice, Canadian employers have no way of accessing the personal information generated by wellness wearables under insurance company-sponsored wellness programs. Rather, they have access to aggregate insights. This is not always the case in the US; employers in some cases have had access to detailed, identifiable worker information [115].

Rights Risks

Insurers in Canada are provided with a number of exemptions from anti-discrimination legislation. For instance, under the Ontario Human Rights Code, insurance plans for employee groups with less than 25 members may make distinctions based on disability, subject to certain conditions [134]. However, the use of wellness wearables in insurance has the potential to amplify bias and discrimination. The programs themselves may not be designed to be accessible to all users and individuals could be offered less favourable terms if they present an attribute that the insurer deems is a higher risk [133]. For instance, interviewees highlighted that reward programs may not account for different abilities and life events like pregnancy or injury.

While programs using wellness wearables are presently rewards based, there is concern that they could become punitive in the future [125]. For instance, there is the potential that information could be used to raise, instead of discount, premiums for policyholders who do not meet targets or to establish a breach of contract [25]. This is already the case for policyholders that opt-in to usage-based auto insurance. While these programs first used data from sensors in vehicles to reward drivers for good behaviour, many now also include penalties for poor driving habits [135].

5 Recommendations to Promote Privacy

The wellness wearable space has been rapidly changing. Industry is moving beyond small wrist worn devices to next generation wellness wearables like smart clothing and tattoos that create closer connections to our bodies, conduct more intimate surveillance, and use even more advanced algorithms [9]. Other developments are moving beyond wearable devices to even more intimate body technologies like embeddables and ingestibles [136]. However, Canadians are currently navigating these innovations without sufficient privacy protections in place. Urgent action is needed to close this gap and prepare for the future of wellness wearables and beyond.

Government needs to work in collaboration with industry and civil society to address the emerging privacy challenges of these devices and their associated apps. A mix of complementary tools – from legislation and regulation to voluntary standards and certification to education and awareness campaigns – can be used. Table 2 outlines several recommend action areas where policymakers can promote privacy for Canadians using wellness wearables. Specifically, government should lay a strong foundation of modernized privacy protections accounting for the risks of these devices. At the same time, more targeted supports are needed to help businesses in the wearables space embed best privacy practices in their offerings and to give users the tools needed to make more informed and meaningful choices about their use.

5.1 Modernizing Privacy Protections

As Canadian jurisdictions look to update privacy regimes, there is an opportunity to ensure that modernization responds to the health-related information generated by wellness wearables and the growing applications of these devices in workplace and insurance. Different approaches to strengthening privacy protections exist in these areas, from reforms under consumer privacy law, to amendments to sensitivity-specific legislation like health privacy law, to additions under sector-specific legislation.

5.1.1 Create Protections for Consumer Health-Related Information

Wellness wearables are designed to collect and analyze personal, health-related information. Yet, these devices typically fall outside of provincial health privacy laws, and the applicable consumer privacy laws do not sufficiently account for this type of information. The government should consider legislative amendments in these areas to create protections for health-related information from consumer products, such as wellness wearables and their associated apps.

Opportunities for Policymakers:

Adjust consumer privacy law to define sensitive health-related information and include inferences

Consumer privacy legislation could be reformed to include provisions that account for the way in which wearables generate a high volume of health-related information in a commercial context. Specifically, a

Table 2: Summary of recommended action areas to promote privacy

Modernizing privacy protections	Helping businesses bolster privacy	Promoting informed user choices
Create protections for consumer health-related information	Create standards and guidance for best practices	Require enhanced notice and consent mechanisms
Enhance and extend privacy protections to all employees	Change how businesses relate to regulators	Encourage certification and labelling
Limit the use of wellness wearable data in insurance	Develop a pipeline of privacy professionals	Promote digital literacy

legislative definition of sensitive information, linked to enhanced privacy obligations could be created and include a non-exhaustive list of examples, such as the health-related data collected by wellness wearables [137]. This type of approach has been taken in the GDPR, which defines "data concerning health" and includes it as a special category of information attached to specific processing restrictions and obligations [138], [139]. Given that inferences from the data generated by wellness wearables can reveal further sensitive information and transform anonymized insights into personally identifiable information [140], consumer privacy legislation should also be amended to explicitly include inferences in examples of health-related data and in the definition of personal information. This approach would be similar to other jurisdictions such as in the US under the *California Consumer Privacy Act* [137].

Amend health privacy law to include commercial actors that collect health-related information

There are opportunities under provincial health privacy laws to account for wellness wearables collecting health-related data. As previously noted, amendments to Ontario's PHIPA have introduced provisions governing "consumer electronic service providers." However, these provisions are not yet in force and regulations have not yet been developed to define scope nor requirements. While these provisions are meant to enable individuals to manage their health records using electronic services, this development may open the opportunity to bring wellness wearables, associated apps, and their applications in workplace and insurance contexts under health privacy laws. Other jurisdictions have also been considering amendments to health privacy legislation that would more generally cover consumer technologies outside health care. For instance, in California, a bill was introduced to expand the state's *Confidentiality of Medical Information Act* to include consumer products, devices, commercial internet websites, online services, and mobile applications individuals use that directly or indirectly collect and transmit health information [141].

5.1.2 Enhance and Extend Privacy Protections to All Employees

Electronic surveillance of employees is a growing issue in Canada, with the use of wellness wearables in the workplace as a contributing element of concern. However, consumer privacy laws do not account for the power imbalance between employers and employees when these technologies are used. At the same time, employment-specific legislation remains relatively silent on privacy issues. The government should consider amendments in these areas to enhance and extend protections for employees when wellness wearables are used at work.

Opportunities for Policymakers:

Develop consumer privacy law to enhance and extend protections to all workers

New or revised consumer privacy legislation could more evenly balance the privacy rights of employees with the legitimate business interests of employers in situations of electronic monitoring, including through wellness wearables. For instance, provisions allowing employers to collect, use, and disclose personal information without consent for purposes of managing an employment relationship could be removed [106]. Instead, a provision that explicitly classes workers as a vulnerable population not able to freely provide or withhold consent, and that calls for an assessment of proportionality, could be included [106]. In addition, while the OPC does offer guidance on the "reasonable person" provision that includes "inappropriate purposes or No-Go Zones" [112], legislative definitions of "electronic surveillance" and "unreasonable electronic surveillance" could be added with a non-exhaustive list of examples [106]. Further to these types of changes, provincial governments without provincial consumer privacy legislation should also consider adopting these statutes to extend protection to employees who do not work in federally regulated sectors and are thus not covered by federal legislation. These new laws could be made substantially similar across jurisdictions to aid the harmonization of protections for all workers and to help simplify the privacy regime for private sector organizations [142].

Create strong privacy provisions under employment and labour laws

Another potential avenue to providing stronger privacy protections for workers is via additions to employment and labour laws. Existing laws provide for workplace topics like compensation, yet remain relatively silent on privacy issues [106]. By updating the employment standards regime to include privacy and electronic monitoring, policymakers would be able to address privacy intrusions from the application of wellness wearables at work, such as in corporate wellness and health and safety programs [142], [143]. Bringing surveillance issues into the realm of employment law has been done in other jurisdictions. For example, in Australia the state of New South Wales has a *Workplace Surveillance Act* [144].

5.1.3 Limit the Use of Wellness Wearable Data in Insurance

Insurers in Canada already draw on a wealth of data about consumers to determine eligibility and premiums for health and life insurance policies. However, the possibility of new interactive policies that use wearables expand the magnitude and scope of this information, and the potential for further discriminatory practices. To address these issues, government should consider restricting how wellness wearable data can be used in insurance to prevent harms from arising.

Opportunities for Policymakers:

Adopt new legislation or regulations restricting the use of wellness wearable data

New legislation or regulation could limit how insurance companies can collect, use, disclose, and store data from wellness wearables. While insurers in Canada do not currently require wellness wearables use, have access granular wearable data, or use devices punitively, these types of privacy-promoting practices should be enshrined as requirements. Canada recently took a similar approach in the context of genetic information. Specifically, while the Canadian Life and Health Insurance Association had issued a Position Statement on limits to genetic testing [131], the 2017 *Genetic Non-discrimination Act* explicitly made it illegal for insurers (as well as employers and other companies) to demand the results of genetic tests and deny service based on results [145].

General Consumer Privacy Reforms Applicable to Wellness Wearables and Other Technologies

In addition to the targeted suggestions, there are more general ways to improve federal consumer privacy legislation that would benefit both users of wellness wearables and users of other emerging technologies under new business models.

Opportunities for Policymakers:

Adopt a Human Rights-Based Approach

Privacy legislation could adopt a human rights-based framework. This could include a provision that sets out the human rights basis of privacy protection, guiding the law's interpretation and application [137], [146]. This would help extend the law beyond data protection to the broader individual right to privacy, associated rights, and the collective dimensions of privacy [146]–[148].

Articulate Enhanced Data Subject Rights

Legislation could articulate enhanced data subject rights such as the right to reputation and the right to a meaningful explanation of automated decision-making [137], [149]. This would give positive obligations to companies and provide individuals with clarity [150]. Other legislation like the EU's GDPR give individuals these expanded rights relating to their personal data [151], [152].

Mandate Privacy by Design

Legislation should articulate a duty to apply Privacy by Design. This would place an obligation on organizations to ensure that privacy is baked into products and services from the start through technical measures, governance, and operations [46], [68]. Other legislation like the EU's GDPR make "Data protection by design and by default" a legal obligation for data controllers [139].

Require Privacy Impact Assessments

Legislation should require privacy impact assessments for higher risk activities to mitigate harm, such as in the case of processing of sensitive health related data by wellness wearables. The EU's GDPR require entities to conduct a Data Protection Impact Assessment (DPIA) if processing is likely to lead to high risk for the rights and freedoms of persons [139].

Account for Cross-Border Data Flows

Legislation could include specific provisions that explicitly address trans-border data flows [153], and specify methods to help organizations ensure that "substantially the same protection of personal information" exists [137]. Other jurisdictions have these types of measures to protect personal data flows across borders including Quebec, the EU, New Zealand, and Australia [154].

Strengthen Review and Enforcement

Legislation could enhance the OPC's ability to hold organizations accountable. This can include creating the authority to conduct proactive audits and order-making powers [137]. Order-making powers already have strong international precedent, including under the GDPR, and provincial authorities in Alberta, BC, and Quebec [149].

Provide Timely and Sufficient Penalties

Legislation should provide timely and appropriate administrative monetary penalties for privacy violations to ensure that fines are effective and do not just become "the cost of doing business."



"Policymakers need to create conditions and provide resources that enable businesses to meet their privacy obligations more easily, rather than to shirk them."

5.2 Helping Businesses Bolster Privacy

Interviewees for this report highlighted that meeting privacy requirements – or better yet, adopting leading practices – is hard for firms, especially those that lack resources or specialized knowledge. For example, smaller Canadian wellness wearable firms are less likely to have large legal teams or in-house expertise to rely on. To address these constraints and secure privacy for Canadians, policymakers need to create conditions and provide resources enabling businesses to meet their privacy obligations more easily, rather than shirk them.

5.2.1 Create Standards and Guidance for Best Practices

Regulations, guidance documents, and best practice guides can be effective tools to help businesses step up in protecting people's privacy rights. Although Canada already benefits from some of these resources, in particular the OPC's Privacy Guidance for Manufacturers of Internet of Things Devices [155], even more specific guidance around wellness wearables and their associated apps would help target the special risks posed by these products and services.

Opportunities for Policymakers:

Create a wellness wearable guidance document or code of practice

The aim of these types of documents would be to provide specific, timely, and tailored advice or rules that operationalize legislated privacy requirements and industry best practices specific to the development and implementation of wellness wearables. These tools should apply to wellness wearables generally, and, more specifically, to particular applications as workplace or insurance. Guidance or codes of practice would be even more useful if Canada's privacy legislation were revised with stronger protections in the near future.

These resources could highlight what is new and different in the legislative environment, and how organizations should comply. Such a document could come from government, regulators, or alternatively, from industry. It could also be provided for within new legislation itself, taking a co-regulatory approach combining the accountability of government regulation and adaptability of industry self-regulation [156]. For instance, the previously proposed CPPA would have created a framework for organizations such as non-profits or industry associations to apply to the OPC for approval of a code of practice that establishes compliance or better protections than provided for by the law at the level of implementation and practice [157].

Create standards for privacy and cybersecurity

To complement and support the implementation of legislative requirements, policymakers could also encourage the development of standards specifically concerned with the privacy and cybersecurity of wellness wearables and associated apps. These standards would provide clear, testable, and credible requirements and help build trust that devices are fit and safe to use in particular contexts [158], [159].

Standard development organizations already engage with tech manufacturers on issues surrounding security, safety, and hardware. They are well-placed to convene experts and stakeholders to develop foundations for privacy and security by design [160]. For example, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have created ISO/IEC DIS 27400, an international standard on information security and privacy controls that helps mitigate the risks of IoT technologies broadly [161]. These types of standards could be made a requirement under privacy or consumer product regulation. For instance, in the US, the *IoT Cybersecurity Improvement Act* of 2020 requires the National Institute of Standards and Technology to develop standards for the government's use of IoT devices, including minimum requirements for information security [162].

5.2.2 Change How Businesses Relate to Regulators

Research interviewees noted that many private actors take an avoidance approach to regulators like the OPC. Companies may try earnestly to meet their privacy obligations, but they try to avoid scrutiny from regulators in equal measure. This dynamic does not serve consumers' interests, and is especially dangerous in the context of wellness wearables, which involve the collection of large volumes of sensitive data. Policymakers could empower the federal and provincial privacy and information commissioners to expand their scopes of services and work more intimately with industry to ensure compliance. There are some leading practices to consider.

Opportunities for Policymakers:

Empower privacy bodies to offer advance rulings or advisory opinions

Policymakers could empower privacy regulators to provide technical interpretation, advanced rulings, and advisory opinions to help wearable manufacturers protect privacy in the first instance, rather than being sanctioned for failing to do so. Entities like the OPC have undertaken efforts to better relate to industry and offer guidance documents. However, these bodies are not resourced or organized to provide individual advice based on the realities manufacturers face. This needs to change. Already, advisory opinions are being considered in the context of modernizing the Privacy Act, Canada's public sector privacy law [163]. These opinions, which can either be binding on regulators or not, are already in place in Canada's lobbying, competition, and taxation oversight systems [164]. Advance rulings on privacy issues have a precedent in Canada. For instance, PEI's Information and Privacy Commissioner is empowered to give advice and recommendations to public bodies seeking an opinion on their rights or duties under Prince Edward Island's (PEIs) *Freedom of Information and Protection of Privacy Act* [163].

Consider a regulatory sandbox for wellness wearables

Highlighted in the Department of Justice's discussion paper on privacy act modernization [165], regulatory sandboxes are controlled periods of time where select businesses are invited to operate without the full force of regulation, while collaborating closely with a regulatory authority. They are appropriate in contexts where technology is disruptive and moving rapidly ahead of regulation, and where businesses are trying to innovate quickly, but are left uncertain how existing law applies to their work [166]. A hallmark of a good sandbox is strong collaboration and feedback that allows regulators to gather evidence of what needs to change in existing regulatory frameworks [167]. They benefit businesses because they offer direct feedback, guidance, and advice, while reducing regulatory uncertainty [168].

They benefit regulators and the public because they give regulators a close-up view of how innovating businesses operate and show areas of highest risk. Importantly, more exposure to the tough considerations and apparent gaps highlighted through this process can give regulators the deep understanding needed to protect the publics' rights. Wellness wearables are a promising area for this kind of policymaking since the privacy risks that they pose are not sufficiently accounted for under the existing distinction between consumer privacy and health privacy regulation in Canada.

5.2.3 Develop a Pipeline of Privacy Professionals

Privacy professionals like Privacy Officers provide organizations with the expertise needed to ensure compliance with legislative and regulatory requirements, and to promote best practices during design and deployment. There has been growing recognition of the important role that these professionals play in privacy protection regimes, with some countries adopting statutory requirements to encourage these positions within companies [169]. For instance, in Canada, PIPEDA requires organizations to designate an individual(s) responsible for data protection [40], while in the EU, the GDPR goes a step further and explicitly requires the appointment of Data Protection Officers in many instances [139]. However, companies face challenges finding suitable privacy professionals [169], and there is a lack of educational programs for these roles [170].

Opportunities for Policymakers:

Support specialized training and education programs for privacy professionals

To create a strong pipeline of privacy professionals that businesses like wellness wearable manufactures can draw from, policymakers should collaborate with industry and post-secondary institutions to create training and education programs designed specifically for these types of roles. Some associations and schools have started to develop and implement such programs, including the Privacy & Access Council of Canada's Professional Certification [171], and Ryerson University's Privacy, Access, and Information Management Certificate [172].

5.3 Promoting Informed User Choices

Canada's current consumer privacy legislation rests on individuals making informed choices about what information they are willing to share and under what conditions, and then offering their consent to use a product or receive a service. But the consent model for protecting privacy comes from a time when consumers were making these decisions in the context of single, understandable transactions. Today, new technology and business models means that one-time consent doesn't capture the reality of a networked world; exponentially more information is collected than before and often shared with a constellation of invisible players for multiple uses [68].

The experts we interviewed told us that today's context and power dynamics between users and manufacturers are such that meaningful privacy cannot be achieved by focusing only on individual consent in the context of wellness wearables. However, while the onus for promoting privacy should be placed on industry, not users, efforts to enhance consent and choice for individuals should not be abandoned; this mechanism remains a critical tool in promoting autonomy and agency. Rather, efforts to promote individual choice and organizational accountability can evolve in tandem: there are ways to help wearable users have the knowledge and information they need to make more informed choices about technologies, even as those technologies are redesigned to better promote privacy.

5.3.1 Require Enhanced Notice and Consent Mechanisms

Privacy policies are hard to get right because they have a constant tension between being complete and detailed for accuracy, and clear and simple for understandability. A balance of both is required for users to make real choices. When users face vague policies that they cannot understand, they may be less likely to object to the stated terms. To the extent that consent will remain a pillar of Canada's privacy regime, policymakers can work with manufacturers to address these issues and help improve privacy notices and user agreements.

Opportunities for Policymakers:

Require privacy notices to be more useful and easier to understand

Many different strategies can be used to make privacy policies and practices more meaningful to users. For instance, privacy notices should appear at relevant times. By offering choices about privacy options repeatedly and at different times — point of sale, or during device set up [173], or just-in-time (when data is about to be collected) or periodically during use [16] — manufacturers can give users the opportunity to re-engage with what they really want to share, rather than rely on a single, one-time grant of consent. To

ensure that individuals are not compelled to consent at these junctures, it is essential that users be able to refuse new conditions without losing access to the historical features they previously agreed to. In addition to timing, manufacturers should follow best practices in formatting to make privacy information accessible and appealing. "Layered" privacy policies, which can include pictograms or short videos, can supplement written policies to help users understand how their information is being used [68], [174]. Wellness wearables raise new possibilities in this area. For example, haptic technologies can transmit notices through touch such as vibrating to alert users when certain data is being shared [175].

Require privacy agreements and notices to be more dynamic and granular

To combat the special privacy risks posed by wellness wearables, users need the chance to move past all-or-nothing consent regimes and be able to consent to some, but not all, uses of their information. Users need to be able to set and revisit their baselines as opt-in or opt-out, across all or some categories [175]. This could mean opt-in consent for sharing information with third parties and enhanced consent for secondary uses (meaning not critical to the functioning of the device or app) [176]. Or it could mean clear and easy mechanisms for revoking consent and deleting data [176]. Such an approach would be in keeping with the requirements under GDPR that free consent must include consent to each purpose that information will be used for. To be most effective, these provisions could be supported by regular re-engagement, where organizations periodically notify individuals of how their data is being used, stored, and disclosed so users can reassess their privacy preferences.

5.3.2 Encourage Certification and Labelling

Experts interviewed for this report highlighted that it is untenable to expect consumers to dig deeply into all aspects of how their data is collected, used, and commercialized when it comes to wellness wearables, in part because people use many apps and devices at any given time. Certification and labelling can help address this issue by making it easier for users to identify best-in-class wellness wearables when it comes to promoting privacy. They also provide a competitive advantage for conscientious manufacturers, helping to incentivize stronger privacy practices.

Opportunities for Policymakers:

Support certification and labelling

Policymakers can help in this space by facilitating the development of labels and certifications, as well as considering opportunities to adopt some of these in regulation. Certification and labelling are related practices that are often tied to standards, wherein product manufacturers either earn the right to show they comply with a set of rules, or agree to display certain information about the products. Labelling can be purely informational [158], such as privacy nutrition labels [177], which present the ways in which companies collect, use, and disclose personal information [178]. Other types of labelling include binary seals of approval or different grades [158]. Forms include industry self-regulation, third party accreditors, or even endorsement from privacy bodies. However, to be most effective and ensure privacy claims are accurate, accountability structures and assessment by independent intermediaries should be required for labelling and certification schemes [159]. For instance, the proposed CPPA would have enabled entities to apply to the OPC for approval of a certification program that could include specified privacy requirements, mechanisms to certify and audit compliance, and disciplinary measures for non-compliance [156].

5.3.3 Promote Digital Literacy

Digital literacy means having the skills knowledge and attitudes to access, use and evaluate digital information effectively [179]. This includes privacy management [180]. This literacy is foundational to navigating the privacy implications of wellness wearables. However, Canada lags behind other countries in promoting digital literacy [181]. Moreover, there is a digital divide within Canada, across geography and other intersecting dynamics like race, class, gender, and age [182]. The following methods would have to be developed to account for these intersecting dynamics to effectively help bolster Canadian digital literacy.

Opportunities for Policymakers:

Create a digital literacy strategy

As part of Canada's Innovation and Skills Plan, the federal government has launched a Digital Literacy Exchange program to teach digital literacy to Canadians seeking to join the digital economy [183]. By expanding this approach to a full digital literacy strategy, aiming beyond economic development, and including helping Canadians understand potential risks and exercise their privacy rights, federal policymakers can collaborate with provincial governments to improve users' privacy in relation to wellness wearables.

Develop digital skills and privacy education for kids

Canada's Privacy Commissioner has endorsed international resolutions and joint letters supporting privacy education [184], [185]. To be most effective and support real choices, provincial governments and school boards could provide a robust digital literacy curriculum addressing privacy rights and risks in the wearables environment. This education should engrain an understanding of the digital environment, including its business models, uses of data and algorithms, and systems of governance [186]. This education can happen across formal education in schools [187] and through community organizations, to use existing networks to reach youth [188]. There are strong resources from which to draw, including MediaSmarts' Digital Literacy Framework for Canadian Schools,[189] the Canadian Civil Liberties Education Trust's educational programs and materials [190], and the OPC's resources for teachers and tips for parents [191], [192].

Conclusion

Policymakers need to take concerted action to protect the privacy of Canadians who use wellness wearables. Always on, and ever-present, wellness wearables rely on unprecedented measuring and monitoring of intimate personal information. Because of this, they pose information, consent, and rights-based risks to people's privacy. The troubling aspects of these privacy risks are especially clear in the workplace, where there are distinct power dynamics influencing why users adopt wellness wearables, and the insurance industry, where products and services could change dramatically based on information generated by wellness wearables.

Securing privacy for Canadians who use wellness wearables will mean modernizing Canada's privacy now. This modernization needs to account for both the unique volume of health-related information generated by wellness wearables, and the growing application of these devices in workplace and insurance contexts. It will also require policymakers to support businesses in meeting their obligations, through standards and guidance, new relationships with regulators, and a strong pipeline of privacy professionals. Policymakers can take further action to promote informed user choices by requiring improved notice and consent mechanisms from wellness wearable manufacturers, by encouraging certification and labelling, and by promoting digital literacy in Canada.

Government must act now, collaborating with industry and civil society, to address existing problems and future-proof Canadians' privacy rights. These technologies are ever-evolving, and it seems that a next generation of wellness wearables is always on the horizon. Careful work to protect privacy today can ensure that privacy becomes an integral feature, rather than an accessory, to wellness wearables devices.

References

[1] B. Rody, "Gen X loves wearables, tablets and traditional TV: study," *Media in Canada,* Nov. 09, 2016. [Online]. Available: https://mediaincanada.com/2016/11/09/gen-x-loves-wearables-tablets-and-traditional-tv-study/.

[2] S. Loomba and A. Khairnar, "Fitness trackers market: Global opportunity analysis and industry forecast, 2017-2023," *Allied Market Research,* Mar. 2018. [Online]. Available: https://www.alliedmarketresearch.com/fitness-tracker-market.

[3] Consumer Technology Association, "Tech spending among Canadians, driven by the pandemic, remains strong, says CTA," *Newswire,* Jun. 29, 2021. [Online]. Available: https://www.newswire.ca/news-releases/tech-spending-among-canadians-driven-by-the-pandemic-remains-strong-says-cta-890560265.html.

[4] Fitbit, "Home," *Fitbit.* [Online]. Available: https://www.fitbit.com/global/en-ca/home (accessed Dec. 03, 2021).

[5] Hexoskin, "Home," *Hexoskin.* [Online]. Available: https://www.hexoskin.com/ (accessed Dec. 03, 2021).

[6] Muse, "Home," *Muse.* [Online]. Available: https://choosemuse.com/ (accessed Dec. 03, 2021).

[7] L. H. Segura Anaya, A. Alsadoon, N. Costadopoulos, and P. W. C. Prasad, "Ethical implications of user perceptions of wearable devices," *Sci. Eng. Ethics*, vol. 24, no. 1, pp. 1–28, 2018, doi: 10.1007/s11948-017-9872-8.

[8] S. Ananthanarayan and K. A. Siek, "Persuasive wearable technology design for health and wellness," in *6th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth) and Workshops,* 2012, pp. 236–240, doi: 10.4108/icst.pervasivehealth.2012.248694.

[9] M. De Mooy and S. Yuen, "Toward privacy aware research and development in wearable health," Center for Democracy & Technology, Washington, DC, USA, May 2016. [Online]. Available: https://cdt.org/wp-content/uploads/2017/07/2016-05-17-Fitbit-FNL1.pdf.

[10] E. Wissinger, "Blood, sweat, and tears: Navigating creepy versus cool in wearable ciotech," *Information, Commun. Soc.*, vol. 21, no. 5, pp. 779–785, 2018, doi: 10.1080/1369118X.2018.1428657.

[11] J. Kitain, "Beware of wearables: Protecting privacy in a data-collecting world," *Drexel Law Rev.,* vol. 9, no. 1, pp. 1–29, 2017. [Online]. Available: https://drexel.edu/law/lawreview/issues/Archives/v9-web/kitain/.

[12] M. Lee, B. Boudreaux, R. Chaturvedi, S. Romanosky, and B. Downing, "The Internet of Bodies: Opportunities, Risks, and Governance," Rand Corporation, Santa Monica, CA, USA, Oct. 2020. [Online]. Available: https://www.rand.org/pubs/research_reports/RR3226.html.

[13] M. S. Gross, R. C. Miller, and A. Pascalev, "Ethical implementation of wearables in pandemic response: A call for a paradigm shift," Edmond J. Safra Center for Ethics, Cambridge, MA, USA, May 2020. [Online]. Available: https://ethics.harvard.edu/files/center-for-ethics/files/18ethicalwearables.pdf?m=1590163395.

[14] B. Lowens, V. G. Motti, and K. Caine, "Wearable privacy: Skeletons in the data closet," in *2017 IEEE International Conference on Healthcare Informatics (ICHI),* 2017, pp. 295–304, doi: 10.1109/ICHI.2017.29.

[15] L. Piwek, D. A. Ellis, S. Andrews, and A. Joinson, "The rise of consumer health wearables: Promises and barriers," *PLoS Med.,* vol. 13, no. 2, p. e1001953, 2016, doi: 10.1371/journal.pmed.1001953.

[16] G. Rosner and E. Kenneally, "Privacy and the Internet of Things: Emerging frameworks for policy and design," Center for Long-Term Cybersecurity, Berkeley, CA, USA, Jun. 2018. [Online]. Available: https://cltc.berkeley.edu/wp-content/uploads/2018/06/CLTC_Privacy_of_the_IoT-1.pdf.

[17] S. Richardson and D. Mackinnon, "Left to their own devices? Privacy implications of wearable technology in Canadian workplaces," Surveillance Studies Centre, Kingston, ON, Canada, Apr. 2017. [Online]. Available: http://www.sscqueens.org/publications/left-to-their-own-devices.

[18] Institute of Medicine (US) Committee on Health Research and the Privacy of Health Information, "The value and importance of health information privacy," in *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research,* S. J. Nass, L. A. Levit, and L. O. Gostin, Eds. Washington, DC, USA: National Academies Press, 2009. [Online]. Available: https://www.ncbi.nlm.nih.gov/books/NBK9579/.

[19] P. W. Woźniak *et al.*, "Creepy technology: What is it and how do you measure it?," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 2021,* pp. 1–13, doi: 10.1145/3411764.3445299.

[20] K. Hill, "Fitbit moves quickly after users' sex stats exposed," *Forbes,* Jul. 05, 2011. [Online]. Available: https://www.forbes.com/sites/kashmirhill/2011/07/05/fitbit-moves-quickly-after-users-sex-stats-exposed/?sh=c53ab3a4327a.

[21] D. Fuller *et al.,* "Reliability and validity of commercially available wearable devices for measuring steps, energy expenditure, and heart rate: Systematic review," *JMIR mHealth uHealth,* vol. 8, no. 9, p. e18694, 2020, doi: 10.2196/18694.

[22] K. C. Montgomery, J. Chester, and K. Kopp, "Health wearable devices in the big data era: Ensuring privacy, security, and consumer protection," Center for Digital Democracy, Washington, DC, USA, Aug. 2017. [Online]. Available: https://www.democraticmedia.org/sites/default/files/field/public/2016/aucdd_wearablesreport_final121516.pdf.

[23] N. Wetsman, "Data from health apps offers opportunities and obstacles to researchers," *The Verge,* Jul. 03, 2019. [Online]. Available: https://www.theverge.com/2019/7/3/20681254/data-health-apps-clue-period-tracking-sleep-fitness-research.

[24] J. M. Radin *et al.,* "Assessment of prolonged physiological and behavioral changes associated with COVID-19 infection," *JAMA Netw. Open,* vol. 4, no. 7, p. e2115959, Jul. 2021, doi: 10.1001/jamanetworkopen.2021.15959.

[25] C. Gidaris, "Surveillance capitalism, datafication, and unwaged labour: The rise of wearable fitness devices and interactive life insurance," *Surveill. Soc.,* vol. 17, no. 1/2, pp. 132–138, 2019, doi: 10.24908/ss.v17i1/2.12913.

[26] I. Pedersen, "Will the Body Become a Platform? Body Networks, Datafied Bodies, and AI Futures," in *Embodied Computing: Wearables, Implantables, Embeddables, Ingestibles,* I. Pedersen and A. Iliadis, Eds. Cambridge, MA, USA: MIT Press, 2020, pp. 21–48. [Online]. Available: https://direct.mit.edu/books/book/4639/chapter-abstract/212557/Will-the-Body-Become-a-Platform-Body-Networks?redirectedFrom=fulltext.

[27] Health Canada, "Medical devices," *Government of Canada,* Jul. 22, 2021. [Online]. Available: https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices.html.

[28] Health Canada, "Safe medical devices in Canada," *Government of Canada,* Mar. 19, 2021. [Online]. Available: https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/activities/fact-sheets/safe-medical-devices-fact-sheet.html.

[29] Health Canada, "Guidance document: Pre-market requirements for medical device cybersecurity – Summary," *Government of Canada,* Ottawa, ON, Canada, Jun. 2019. [Online]. Available: https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/application-information/guidance-documents/cybersecurity.html.

[30] Health Canada, "It's your health: Buying medical devices from the internet," *Government of Canada,* Ottawa, ON, Canada, Apr. 2011. [Online]. Available: https://www.canada.ca/content/dam/hc-sc/migration/hc-sc/hl-vs/alt_formats/pdf/iyh-vsv/med/med_mat-eng.pdf.

[31] Health Canada, "Notice: Health Canada's approach to digital health technologies," *Government of Canada,* Apr. 10, 2018. [Online]. Available: https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/activities/announcements/notice-digital-health-technologies.html.

[32] *Canada Consumer Product Safety Act,* SC 2010, c 21. [Online]. Available: https://canlii.ca/t/8p21.

[33] Office of the Privacy Commissioner of Canada, "Provincial and territorial privacy laws and oversight," *OPC,* Jun. 11, 2020. [Online]. Available: https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/provincial-and-territorial-privacy-laws-and-oversight/.

[34] *Personal Health Information Protection Act,* 2004. SO 2004, c 3, s A. [Online]. Available: https://canlii.ca/t/32t.

[35] *Health Information Act,* RSA 2000, c H-5. [Online]. Available: https://canlii.ca/t/81pf.

[36] *Bill 188, An Act to enact and amend various statutes,* 1st Session, 42nd Legislature Ontario, 2020. [Online]. Available: https://www.ola.org/en/legislative-business/bills/parliament-42/session-1/bill-188.

[37] Information and Privacy Commissioner of Ontario, "Incremental but consequential: 2020 changes to PHIPA," *IPC,* Dec. 03, 2020. [Online]. Available: https://www.ipc.on.ca/incremental-but-consequential-2020-changes-to-phipa/.

[38] D. Ammerman and G. Shaw, "Significant expansion of Ontario's personal health information protections amid COVID-19: What you need to know," *McMillan LLP,* Jul. 15, 2020. [Online]. Available: https://mcmillan.ca/insights/significant-expansion-of-ontarios-personal-health-information-protections-amid-covid-19-what-you-need-to-know/.

[39] Information and Privacy Commissioner of Ontario, "Digital health under PHIPA: Selected overview," *IPC,* Toronto, ON, Canada, May 2021. [Online]. Available: https://www.ipc.on.ca/wp-content/uploads/2021/05/digital-health-under-phipa.pdf.

[40] *Personal Information Protection and Electronic Documents Act,* SC 2000, c 5. [Online]. Available: https://canlii.ca/t/7vwj.

[41] *Personal Information Protection Act,* SA 2003, c P-6.5. [Online]. Available: https://canlii.ca/t/81qp.

[42] *Personal Information Protection Act,* SBC 2003, c 63. [Online]. Available: https://canlii.ca/t/84mg.

[43] *Act respecting the protection of personal information in the private sector,* CQLR, c P-39.1. [Online]. Available: https://canlii.ca/t/xpm.

[44] Office of the Privacy Commissioner of Canada, "PIPEDA in brief," *OPC,* May 2019. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/.

[45] S. Adams, "Quebec's Bill 64: The first of many privacy modernization bills in Canada?," *IAPP,* Nov. 23, 2021. [Online]. Available: https://iapp.org/news/a/quebecs-bill-64-the-first-of-many-privacy-modernization-bills-in-canada/.

[46] Office of the Privacy Commissioner of Canada, "Consent and privacy: A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act," *OPC,* Gatineau, QC, Canada, May 2016. [Online]. Available: https://www.priv.gc.ca/media/1806/consent_201605_e.pdf.

[47] Office of the Privacy Commissioner of Canada, "OPC updates guidance regarding sensitive information," *OPC,* Aug. 13, 2021. [Online]. Available: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/an_210813/.

[48] *Bill C-11, An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts,* 2nd Session, 43rd Parliament, 2020. [Online]. Available: https://parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading.

[49] Office of the Privacy Commissioner of Canada, "Commissioner: Reform bill 'a step back overall' for privacy," *OPC,* May 11, 2021. [Online]. Available: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/nr-c_210511/.

[50] C. Parsons, "Canada's proposed privacy law reforms are not enough: A path to improving organizational transparency and accountability," *Citizen Lab,* Apr. 23, 2021. [Online]. Available: https://citizenlab.ca/2021/04/canadas-proposed-privacy-law-reforms-are-not-enough-improving-organizational-transparency-and-accountability-bill-c11/.

[51] T. Scassa, "The gutting of consent in Bill C-11," *Teresa Scassa,* Dec. 21, 2020. [Online]. Available: https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=336:the-gutting-of-consent-in-bill-c-11&Itemid=80.

[52] S. Villeneuve and S. Fielding, "Blood, sweat, and megabytes," *Brookfield Institute for Innovation + Entrepreneurship,* Nov. 12, 2019. [Online]. Available: https://brookfieldinstitute.ca/blood-sweat-and-megabytes/.

[53] L. Lowenstein, M. Paterson, and R. Carson, "Supreme Court of Canada revamps the test for jurisdiction over foreign defendants," *Osler, Hoskin & Harcourt LLP,* Apr. 19, 2012. [Online]. Available: https://www.osler.com/en/resources/regulations/2012/supreme-court-of-canada-revamps-the-test-for-juris.

[54] G. Tomimbang, "Wearables: Where do they fall within the regulatory landscape?," *IAPP,* Jan. 22, 2018. [Online]. Available: https://iapp.org/news/a/wearables-where-do-they-fall-within-the-regulatory-landscape/.

[55] A. Troiano, "Wearables and personal health data: Putting a premium on your privacy," *Brooklyn Law Rev.,* vol. 82, no. 4, pp. 1715–1753, 2017, [Online]. Available: https://brooklynworks.brooklaw.edu/blr/vol82/iss4/6.

[56] S. Spann, "Wearable fitness devices: Personal health data privacy in Washington State," *Seattle Univ. Law Rev.,* vol. 39, pp. 1411–1432, 2016, [Online]. Available: https://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=2354&context=sulr.

[57] State of California Department of Justice, "California Consumer Privacy Act (CCPA)," *Office of the Attorney General.* [Online]. Available: https://oag.ca.gov/privacy/ccpa (accessed Nov. 24, 2021).

[58] M. Becker, "Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy," *Ethics Inf. Technol.,* vol. 21, pp. 307–317, 2019, doi: 10.1007/S10676-019-09508-Z.

[59] A. Hilts, C. Parsons, and J. Knockel, "Every step you fake: A comparative analysis of fitness tracker privacy and security," *Open Effect,* Toronto, ON, Canada, Feb. 2016. [Online]. Available: https://openeffect.ca/reports/Every_Step_You_Fake.pdf.

[60] A. Raij, A. Ghosh, S. Kumar, and M. Srivastava, "Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* 2011, pp. 11–20, doi: 10.1145/1978942.1978945.

[61] S. R. Peppet, "Regulating the Internet of Things: First steps toward managing discrimination, privacy, security, and consent," *Tex. Law Rev.,* vol. 93, pp. 85–176, 2014, [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409074.

[62] Broadband Internet Technical Advisory Group, "Internet of Things (IoT) security and privacy recommendations," BITAG, Denver, CO, USA, Nov. 2016. [Online]. Available: https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf.

[63] Consumers International, "Testing our trust: Consumers and the Internet of Things 2017 review," Consumers International, London, United Kingdom, 2017. [Online]. Available: https://www.consumersinternational.org/media/154746/iot2017review-2nded.pdf.

[64] C. Wang, X. Guo, Y. Wang, Y. Chen, and B. Liu, "Friend or foe?: Your wearable devices reveal your personal PIN," in Proceedings of the *11th ACM on Asia Conference on Computer and Communications Security,* 2016, pp. 189–200, doi: 10.1145/2897845.2897847.

[65] Binghamton University, "Your smartwatch is giving away your ATM PIN," *ScienceDaily,* Jul. 06, 2016. [Online]. Available: https://www.sciencedaily.com/releases/2016/07/160706131951.htm.

[66] G. Corser *et al.,* "Internet of Things (IoT) security best practice," *IEEE,* New York, NY, USA, Feb. 2017. [Online]. Available: https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf.

[67] J. Scott-Railton and A. Hilts, "Fit leaking: Citizen Lab research on fitness tracker privacy," *Citizen Lab,* Jan. 2018. [Online]. Available: https://citizenlab.ca/2018/01/fit-leaking-citizen-lab-research-fitness-tracker-privacy/.

[68] Office of the Privacy Commissioner of Canada, "Consent and privacy: A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act," *OPC,* Gatineau, QC, Canada, May 2016. [Online]. Available: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/.

[69] M. Becker, "Understanding users' health information privacy concerns for health wearables," in Proceedings of the *51st Hawaii International Conference on System Sciences,* 2018, pp. 3261–3270, doi: 10.24251/hicss.2018.413.

[70] K. Maltseva, "Wearables in the workplace: The brave new world of employee engagement," *Bus. Horiz.,* vol. 63, no. 4, pp. 493–505, 2020, doi: 10.1016/J.BUSHOR.2020.03.007.

[71] I. Ajunwa, "Algorithms at work: Productivity monitoring applications and wearable technology as the new data-centric research agenda for employment and labor law," *St. Louis Univ. Law J.*, vol. 63, pp. 21–54, 2018, [Online]. Available: https://ssrn.com/abstract=3247286.

[72] F. Schaub, R. Balebako, A. L. Durity, and L. F. Cranor, "A design space for effective privacy notices," in *SOUPS 2015: Symposium on Usable Privacy and Security,* 2015, pp. 1–17, [Online]. Available: https://www.usenix.org/conference/soups2015/proceedings/presentation/schaub.

[73] Internet Society, "Internet Society policy brief: IoT privacy for policymakers," Internet Society, Washington, DC, USA, Sep. 2019. [Online]. Available: https://www.internetsociety.org/wp-content/uploads/2019/09/IoT-Privacy-Brief_20190912_Final-EN.pdf.

[74] L. Ackerman, "Mobile health and fitness applications and information privacy: Report to California Consumer Protection Foundation," Privacy Rights Clearinghouse, San Diego, CA, USA, Jul. 2013. [Online]. Available: https://privacyrights.org/sites/default/files/pdfs/mobile-medical-apps-privacy-consumer-report.pdf.

[75] K. Litman-Navarro, "We read 150 privacy policies. They were an incomprehensible disaster," *The New York Times,* Jul. 12, 2019. [Online]. Available: https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.

[76] Office of the Privacy Commissioner of Canada, "Results of the 2016 Global Privacy Enforcement Network Sweep," *OPC,* Sep. 22, 2016. [Online]. Available: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2016/bg_160922/.

[77] S. Banerjee, T. Hemphill, and P. Longstreet, "Wearable devices and healthcare: Data sharing and privacy," *Inf. Soc.,* vol. 34, no. 1, pp. 1–9, 2018, doi: 10.1080/01972243.2017.1391912.

[78] "Fuel of the future: Data is giving rise to a new economy," *The Economist*, May 06, 2017. [Online]. Available: https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy.

[79] B. Beamish, "Privacy with your wearable devices and your friends: Alexa, Siri, and Google," *IPC,* Toronto, ON, Canada, Nov. 2019. [Online]. Available: https://www.ipc.on.ca/wp-content/uploads/2019/11/2019-11-07-born-web.pdf.

[80] Office of the United Nations High Commissioner of Human Rights, "Special Rapporteur on the right to privacy," *OHCHR.* [Online]. Available: https://www.ohchr.org/en/issues/privacy/sr/pages/srprivacyindex.aspx (accessed Oct. 18, 2021).

[81] J. Buolamwini and T. Gebru, "Gender shades: Intersectional accuracy disparities in commercial gender classificiation," in *Proceedings of the 1st Conference on Fairness, Accountability and Transparency,* 2018, vol. 81, pp. 77–91, [Online]. Available: https://proceedings.mlr.press/v81/buolamwini18a.html.

[82] Deloitte Canada, "Canada's AI imperative: Public policy's critical moment," Deloitte Canada, Toronto, ON, Canada, 2019. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/deloitte-analytics/ca-public-policys-critical-moment-aoda-en.pdf?location=top.

[83] J. P. Elman, "'Find Your Fit': Wearable technology and the cultural politics of disability," *New Media Soc.,* vol. 20, no. 10, pp. 3760–3777, 2018, doi: 10.1177/1461444818760312.

[84] P. J. Colvonen, P. N. DeYoung, N. O. A. Bosompra, and R. L. Owens, "Limiting racial disparities and bias for wearable devices in health science research," *Sleep,* vol. 43, no. 10, pp. 1–3, 2020, doi: 10.1093/sleep/zsaa159.

[85] Technology Safety, "Connected health & medical devices: Survivor privacy risks & strategies," *Technology Safety.* [Online]. Available: https://www.techsafety.org/iot-health-privacy (accessed Sep. 24, 2021).

[86] S. Javed, "'Keep your whereabouts to yourself!': Women discuss whether it is safe to share running routes online," *The Independent,* Jun. 16, 2021. [Online]. Available: https://www.independent.co.uk/life-style/women/run-social-media-women-strava-b1866880.html.

[87] B. Caddy, "From cheating to pregnancy reveals, wearables know what you're doing intimately," *Inverse,* Mar. 21, 2020. [Online]. Available: https://www.inverse.com/mind-body/from-cheating-to-pregnancy-reveals-wearables-know-what-you-are-doing-intimately.

[88] C. Nyst, "Children's rights and busines in a digital world: Privacy, protection of personal information and reputation rights," UNICEF, New York, NY, USA, Mar. 2017. [Online]. Available: https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf.

[89] C. Nyst, "Industry toolkit: Children's online privacy and freedom of expression," UNICEF, New York, NY, USA, May 2018. [Online]. Available: https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf.

[90] K. Rose, S. Eldridge, and L. Chapin, "The Internet of Things: An overview – Understanding the challenges of a more connected world," *Internet Society,* Washington, DC, USA, Oct. 2015. [Online]. Available: https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf.

[91] H. Nissenbaum, "Privacy as Contextual Integrity," *Washingt. Law Rev.,* vol. 79, no. 1, pp. 119–158, 2004, [Online]. Available: https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/#:~:text=Washington Law Review&text=It posits a new construct,challenges posed by information technologies.

[92] S. Villeneuve and D. Elias, "Surveillance creep: Data collection and privacy in Canada during COVID-19," *Brookfield Institute for Innovation + Entrepreneurship,* Sep. 02, 2020. [Online]. Available: https://brookfieldinstitute.ca/surveillance-creep-data-collection-and-privacy-in-canada-during-covid-19/.

[93] M. Ravindranath, "Coronavirus opens door to company surveillance of workers," *POLITICO,* Jun. 26, 2020. [Online]. Available: https://www.politico.com/news/2020/06/26/workplace-apps-tracking-coronavirus-could-test-privacy-boundaries-340525.

[94] K. MacDonald, "Are wearables the cure for rising health costs?," *Benefits Canada,* Oct. 17, 2014. [Online]. Available: https://www.benefitscanada.com/benefits/health-wellness/are-wearables-the-cure-for-rising-health-costs/.

[95] Sprout Wellness Solutions, "The Sprout At Work difference," *Sprout Wellness Solutions.* [Online]. Available: https://www.sproutatwork.com/hubfs/Sprout At Work I The Sprout Difference.pdf.

[96] National Research Council Canada, "Sprout turns the tables on workplace wellness with data-driven results and fun," *Government of Canada,* Oct. 14, 2016. [Online]. Available: https://nrc.canada.ca/en/stories/sprout-turns-tables-workplace-wellness-data-driven-results-fun.

[97] S. Richardson and D. Mackinnon, "Becoming your own device: Self-tracking challenges in the workplace," *Can. J. Sociol.,* vol. 43, no. 3, pp. 225–250, 2018, doi: 10.29173/cjs28974.

[98] D. Beeby, "Federal agency looking at fitness trackers for public sector workers," *CBC News,* Mar. 12, 2019. [Online]. Available: https://www.cbc.ca/news/politics/fitbit-trackers-fitness-wearable-premiums-health-insurance-rewards-points-1.5046724.

[99] D. Jones, D. Molitor, and J. Reif, "What do workplace wellness programs do? Evidence from the Illinois workplace wellness study," 24229, 2018. doi: 10.1093/qje/qjz023.

[100] C. Garden, "Labor Organizing in the Age of Surveillance," *St. Louis Univ. Law J.,* vol. 63, no. 55, pp. 55–68, 2018, [Online]. Available: https://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=1817&context=faculty.

[101] Deloitte Canada and NORCAT, "Future of mining with wearables: Harnessing the hype to improve safety." Deloitte Canada, Toronto, ON, Canada, [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Energy-and-Resources/gx-eri-norcat-report.pdf.

[102] P. Van den Bossche, C. Simpson, D. Weiser, and N. Anderson, "Wearable technology in the warehouse," *Supply Chain 24/7,* Feb. 01, 2016. [Online]. Available: http://www.supplychain247.com/article/wearable_technology_in_the_warehouse.

[103] D. Cox, "The rise of employee health tracking," *BBC,* Nov. 10, 2020. [Online]. Available: https://www.bbc.com/worklife/article/20201110-the-rise-of-employee-health-tracking.

[104] T. Scassa, "Privacy in the precision economy: The rise of AI-enabled workplace surveillance during the pandemic," *Centre for International Governance Innovation,* Jul. 08, 2021. [Online]. Available: https://www.cigionline.org/articles/privacy-in-the-precision-economy-the-rise-of-ai-enabled-workplace-surveillance-during-the-pandemic/.

[105] R. Kattapuram, "An employer's guide to privacy in the workplace," *Canadian Employment & Labour Law,* Aug. 09, 2018. [Online]. Available: https://www.employmentandlabour.com/an-employers-guide-to-privacy-in-the-workplace/.

[106] C. Catenacci, "Privacy and surveillance in the workplace: Closing the electronic surveillance gap," Electronic Thesis and Dissertation Repository, Western University, 2020. [Online]. Available: https://ir.lib.uwo.ca/etd/7117/.

[107] M. J. Masoodi, N. Abdelaal, S. Tran, Y. Stevens, S. Andrey, and K. Bardeesy, "Workplace Surveillance and Remote Work: Exploring the Impacts and Implications," *Cybersecure Policy Exchange,* Toronto, ON, Canada, Sep. 2021, [Online]. Available: https://static1.squarespace.com/static/5e9ce713321491043ea045ef/t/6166d5e131d8606af68eccf9/1634129758502/Workplace+Surveillance+and+Remote+Work.pdf.

[108] A. Mateescu and A. Nguyen, "Explainer: Workplace Monitoring & Surveillance," *Data & Society,* New York, NY, USA, Feb. 2019. [Online]. Available: https://apo.org.au/sites/default/files/resource-files/2019-02/apo-nid218571.pdf.

[109] K. A. Hughes and E. Dixon, "Ignored and misunderstood: Privacy rights and medical information in the Canadian workplace," *Cavalluzzo LLP,* Toronto, ON, Canada, Nov. 2013. [Online]. Available: https://www.cavalluzzo.com/docs/default-source/publications/2013-11-01-ignored-and-misunderstood---privacy-rights-and-medical-information-in-the-canadian-workplace-(kate-hughes-and-emily-dixon)-labour-health-pension-benefits-law.pdf?sfvrsn=13c855d5_2.

[110] Office of the Privacy Commissioner of Canada, "PIPEDA fair information principle 3 – consent," *OPC,* Aug. 2020. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_consent/.

[111] M. R. Bueckert, "Watching workers: A critical review of the law regarding electronic employee monitoring in non-unionized workplaces in Canada," Electronic Theses & Dissertations, University of Manitoba, 2008. [Online]. Available: http://hdl.handle.net/1993/3086.

[112] Office of the Privacy Commissioner of Canada, "Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)," *OPC,* May 2018. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/.

[113] M. A. Geist, "Computer and e-mail workplace surveillance in Canada: The shift from reasonable expectation of privacy to reasonable surveillance," *Can. Bar Rev.,* vol. 82, no. 2, pp. 151–169, 2003, [Online]. Available: https://cbr.cba.org/index.php/cbr/article/view/3968/3961.

[114] Canadian Centre for Diversity and Inclusion, "Overview of human rights codes by province and territory in Canada," *CCDI,* Toronto, ON, Canada, Jan. 2018. [Online]. Available: https://ccdi.ca/media/1414/20171102-publications-overview-of-hr-codes-by-province-final-en.pdf.

[115] C. Rowland, "With fitness trackers in the workplace, bosses can monitor your every step – and possibly more," *The Washington Post,* Feb. 16, 2019. [Online]. Available: https://www.washingtonpost.com/business/economy/with-fitness-trackers-in-the-workplace-bosses-can-monitor-your-every-step--and-possibly-more/2019/02/15/75ee0848-2a45-11e9-b011-d8500644dc98_story.html.

[116] S. Behm, U. Deetjen, S. Kaniyar, N. Methner, and B. Münstermann, "Digital ecosystems for insurers: Opporunities through the Internet of Things," *McKinsey & Company,* Feb. 04, 2019. [Online]. Available: https://www.mckinsey.com/industries/financial-services/our-insights/digital-ecosystems-for-insurers-opportunities-through-the-internet-of-things.

[117] A. Spender et al., "Wearables and the internet of things: Considerations for the life and health insurance industry," *Br. Actuar. J.,* vol. 24, no. 22, pp. 1–31, 2019, doi: 10.1017/S1357321719000072.

[118] B. Nayak and S. S. Bhattacharyya, "The changing narrative in the health insurance industry: Wearables technology in health insurance products and services for the COVID-19 world," *J. Health Manag.,* vol. 22, no. 4, pp. 550–558, 2020, doi: 10.1177/0972063420983112.

[119] A. Chen, "What happens when life insurance companies track fitness data?," *The Verge,* Sep. 26, 2018. [Online]. Available: https://www.theverge.com/2018/9/26/17905390/john-hancock-life-insurance-fitness-tracker-wearables-science-health.

[120] Randall Anthony Communications, "Insurance models as incentives for positive change," *The Globe and Mail,* Nov. 27, 2019. [Online]. Available: https://www.theglobeandmail.com/business/adv/article-insurance-models-as-incentives-for-positive-change/.

[121] Manulife Financial, "Manulife Vitality," *Manulife Financial.* [Online]. Available: https://www.manulife.ca/personal/vitality/vitality-for-individuals.html (accessed Oct. 13, 2021).

[122] J. Nelson, "Manulife turns to fitness, rewarding customers for healthy habits," *The Globe and Mail,* May 03, 2015. [Online]. Available: https://www.theglobeandmail.com/report-on-business/manulife-turns-to-fitness-rewarding-customers-for-healthy-habits/article24233375/.

[123] Manulife Financial, "Rewards and benefits," *Manulife Financial.* [Online]. Available: https://www.manulife.ca/personal/vitality/rewards-and-benefits.html (accessed Oct. 13, 2021).

[124] H. Salah, E. MacIntosh, and N. Rajakulendran, "Wearable tech: Leveraging Canadian innovation to improve health," MaRS Discovery District, Toronto, ON, Canada, Mar. 2014. [Online]. Available: https://healthwatchtech.com/wp-content/uploads/2017/08/Global-market-for-wearables.pdf.

[125] A. Robeznieks, "Insurers want patients to use wearables. That could be a problem," *American Medical Association,* Aug. 26, 2019. [Online]. Available: https://www.ama-assn.org/practice-management/digital/insurers-want-patients-use-wearables-could-be-problem.

[126] CBC News, "Privacy experts say choosing life insurance tied to fitness tracking could have unintended consequences," *CBC News,* Sep. 21, 2018. [Online]. Available: https://www.cbc.ca/news/business/privacy-life-insurance-john-hancock-1.4833193.

[127] S. Verma, L. van Deel, R. Nadimpalli, D. Sahoo, and M. Vervuurt, "Wearable devices and their applicability in the life insurance industry," Capgemini, Paris, France, Jul. 2017. [Online]. Available: https://www.capgemini.com/wp-content/uploads/2017/07/wearable_devices_and_their_applicability_in_the_life_insurance_industry.pdf.

[128] P.-I. Bernard, K. Ellingrud, J. Godsall, B. Kotanko, and A. Reich, "The future of life insurance: Reimagining the industry for the decade ahead," *McKinsey & Company,* Sep. 29, 2020. [Online]. Available: https://www.mckinsey.com/industries/financial-services/our-insights/the-future-of-life-insurance-reimagining-the-industry-for-the-decade-ahead.

[129] G. A. Badali, D. Ammerman, and C. Garrah, "Insurance and reinsurance in Canada: overview," *Practical Law,* Apr. 01, 2021. [Online]. Available: https://uk.practicallaw.thomsonreuters.com/2-501-7810?transitionType=Default&contextData=(sc.Default).

[130] Office of the Superintendent of Financial Institutions, "Who we regulate," *Government of Canada.* [Online]. Available: https://www.osfi-bsif.gc.ca/Eng/wt-ow/Pages/wwr-er.aspx?sc=2&gc=1&ic=1 (accessed Nov. 22, 2021).

[131] Office of the Privacy Commissioner of Canada, "Genetic information, the life and health insurance industry and the protection of personal information: Framing the debate," *OPC,* Gatineau, QC, Canada, Dec. 2012. [Online]. Available: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2012/gi_intro/.

[132] D. Ammerman, "Supreme Court of Canada affirms the Genetic Non-Discrimination Act, weighing autonomy, privacy, and accessibility of insurance," *McMillan LLP,* Jul. 2020. [Online]. Available: https://mcmillan.ca/insights/supreme-court-of-canada-affirms-the-genetic-non-discrimination-act-weighing-autonomy-privacy-and-accessibility-of-insurance/.

[133] E. Dans, "Insurance, wearables and the future Of healthcare," *Forbes,* Sep. 21, 2018. [Online]. Available: https://www.forbes.com/sites/enriquedans/2018/09/21/insurance-wearables-and-the-future-of-healthcare/?sh=720b98591782.

[134] Ontario Human Rights Commission, "Insurance-related provisions of the Code," *Ontario Human Rights Commission.* [Online]. Available: http://www.ohrc.on.ca/en/discussion-paper-human-rights-issues-insurance/insurance-related-provisions-code (accessed Nov. 23, 2021).

[135] L. Rainie and M. Duggan, "Scenario: Auto insurance discounts and monitoring," *Pew Research Center,* Jan. 14, 2016. [Online]. Available: https://www.pewresearch.org/internet/2016/01/14/scenario-auto-insurance-discounts-and-monitoring/.

[136] Federal Communications Commission, "Ingestibles, wearables and embeddables," *Federal Communications Commission.* [Online]. Available: https://www.fcc.gov/general/ingestibles-wearables-and-embeddables (accessed Nov. 28, 2021).

[137] Office of the Privacy Commissioner of Canada, "Submission of the Office of the Privacy Commissioner of Canada on Bill C-11, the Digital Charter Implementation Act, 2020," *OPC,* Gatineau, QC, Canada, May 2021. [Online]. Available: https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ethi_c11_2105/.

[138] G. G. Fuster, "Wearables, health and privacy: A European perspective," in *Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection,* K. C. Montgomery, J. Chester, and K. Kopp, Eds. Washington, DC, USA: Center for Digital Democracy, 2017. [Online]. Available: https://www.democraticmedia.org/sites/default/files/field/public/2016/aucdd_wearablesreport_final121516.pdf.

[139] *Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the procesing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (General Data Protection Regulation), OJ L 119, 4.5.2016, p 1. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[140] S. E. Trosow, L. Taylor, and A. Hanam, "The Internet of Things: Implications for consumer privacy under Canadian law," *Western University,* 2017. [Online]. Available: https://ir.lib.uwo.ca/lawpub/91/.

[141] L. D. Compton and S. A. John, "California health privacy information legislation update," *Natl. Law Rev.,* vol. 11, no. 333, 2021. [Online]. Available: https://www.natlawreview.com/article/california-health-privacy-information-legislation-update.

[142] M. R. Bueckert, "Electronic Employee Monitoring: Potential Reform Options," *Manit. Law J.,* pp. 99–116, 2009. [Online]. Available: http://themanitobalawjournal.com/wp-content/uploads/articles/UTGB_6/Electronic-Employee-Monitoring:-Potential-Reform-Options.pdf.

[143] I. Ajunwa, K. Crawford, and J. Schultz, "Limitless Worker Surveillance," *Calif. Law Rev.,* vol. 105, no. 3, pp. 735–776, 2017. [Online]. Available: https://www.jstor.org/stable/44630759.

[144] W. Ellis, "Workplace Surveillance Act NSW," *Privacy Australia,* Apr. 06, 2021. [Online]. Available: https://privacyaustralia.net/workplace-surveillance-act-nsw/.

[145] Canadian Civil Liberties Association, "The Genetic Non-Discrimination Act: An overview," *CCLA,* 2018. [Online]. Available: https://ccla.org/get-informed/talk-rights/the-genetic-non-discrimination-act-an-overview/.

[146] T. Scassa, "A human rights-based approach to data protection in Canada," in *Citizenship in a Connected Canada: A Research and Policy Agenda,* E. Dubois and F. Martin-Bariteau, Eds. Ottawa, ON, Canada: University of Ottawa Press, 2020. [Online]. Available: https://ssrn.com/abstract=3620450.

[147] Office of the Privacy Commissioner of Canada, "Privacy law reform – A pathway to respecting rights and restoring trust in government and the digital economy," *OPC,* Gatineau, QC, Canada, Dec. 2019. [Online]. Available: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201819/ar_201819/.

[148] B. Ballard, A. Cutinha, and C. Parsons, "Pandemic privacy: A prelimary analysis of collection technologies, data collection laws, and legislative reform during COVID-19," *Citizen Lab,* Toronto, ON, Canada, Sep. 2021. [Online]. Available: https://citizenlab.ca/wp-content/uploads/2021/09/092721_pandemic-privacy_v3.pdf.

[149] I. Cofone, "Policy proposals for PIPEDA reform to address artificial intelligence," *Office of the Privacy Commissioner of Canada,* Nov. 2020. [Online]. Available: https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pol-ai_202011/.

[150] Privacy International, "Part 4: Rights of data subjects," Privacy International, London, United Kingdom, Sep. 2018. [Online]. Available: https://privacyinternational.org/sites/default/files/2018-09/Part 4 - Rights of Data Subjects.pdf.

[151] UK Information Commissioner's Office, "Individual rights ," *ICO.* [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/ (accessed Oct. 19, 2021).

[152] L. Irwin, "What are the data subject rights under the GDPR?," *IT Governance,* Mar. 10, 2021. [Online]. Available: https://www.itgovernance.co.uk/blog/what-are-the-data-subject-rights-under-the-gdpr.

[153] T. Scassa, "Bill C-11's treatment of cross-border transfers of personal tnformation," *Office of the Privacy Commissioner of Canada,* May 2021. [Online]. Available: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/tbdf_scassa_2105/#fn5.

[154] T. Scassa, "Appendix 3: Cross-border data flows and transfers for processing - Jurisdictional analysis," *Office of the Privacy Commissioner of Canada,* Sep. 2020. [Online]. Available: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/tbdf_app3/.

[155] Office of the Privacy Commissioner of Canada, "Privacy guidance for manufacturers of Internet of Things devices," *OPC,* Aug. 2020. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/technology/gd_iot_man/.

[156] H. Cheng, "The rise of co-regulation, from GDPR to Canada's Bill C-11," *IAPP,* Dec. 17, 2020. [Online]. Available: https://iapp.org/news/a/the-rise-of-co-regulation-from-gdpr-to-canadas-bill-c-11/.

[157] W. Mee, E. Marshall, and I. Ahmad, "New federal bill set to reform Canada's private-sector privacy law," *Blake, Cassels & Graydon LLP,* Nov. 18, 2020. [Online]. Available: https://www.blakes.com/insights/bulletins/2020/new-federal-bill-set-to-reform-canada-s-private-se.

[158] Internet Society, "Enhancing IoT security: Final outcomes and recommendations report," Internet Society, Washington, DC, USA, May 2019. [Online]. Available: https://www.internetsociety.org/wp-content/uploads/2019/05/Enhancing-IoT-Security-Report-2019_EN.pdf.

[159] T. Capel and A. Shalabi, "The Role of Standardization in Emerging Technologies," CSA Group, Toronto, ON, Canada, Mar. 2019. [Online]. Available: https://www.csagroup.org/wp-content/uploads/CSA-Group-Research-Emerging-Technologies.pdf.

[160] K. Alwani and M. C. Urban, "The digital age: Exploring the role of standards for data governance, artificial intelligence and emerging platforms," CSA Group, Toronto, ON, Canada, May 2019. [Online]. Available: https://www.csagroup.org/wp-content/uploads/CSA-Group-research-Digital-Economy.pdf.

[161] *Cybersecurity — IoT security and privacy – Guidelines.* ISO/IEC DIS 27400. [Online]. Available: https://www.iso.org/standard/44373.html.

[162] Congressional Research Service, "Summary of H.R. 1668 (116th): IoT Cybersecurity Improvement Act of 2020," *GovTrack,* Dec. 05, 2020. [Online]. Available: https://www.govtrack.us/congress/bills/116/hr1668/summary.

[163] Department of Justice, "A modern and effective compliance framework with enhanced enforcement mechanisms," *Government of Canada,* Sep. 01, 2021. [Online]. Available: https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/modern_4.html.

[164] Centre for Information Policy Leadership, "Comments by the Centre for Information Policy Leadership on Justice Canada's technical engagement with experts on the modernization of Canada's federal Privacy Act," Centre for Information Policy Leadership, Washington, DC, USA, Aug. 2019. [Online]. Available: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_justice_canadas_technical_engagement_with_experts_on_the_modernization_of_canadas_federal_privacy_act__21_augu.pdf.

[165] Department of Justice, "Privacy Act modernization: A discussion paper," *Government of Canada,* Ottawa, ON, Canada, Sep. 2021. [Online]. Available: https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/pdf/dp-1.pdf.

[166] P. Bruening, "An emerging tool: Regulatory sandboxes for privacy," *IAPP,* Apr. 27, 2021. [Online]. Available: https://iapp.org/news/a/regulatory-sandboxes-for-privacy/.

[167] C. Rosemberg *et al.,* "Regulatory sandboxes and innovation testbeds: A look at international experience and lessons for Latin America and the Caribbean," Inter-American Development Bank, New York, NY, USA, 2020. [Online]. Available: https://publications.iadb.org/publications/english/document/Regulatory-Sandboxes-and-Innovation-Testbeds-A-Look-at-International-Experience-in-Latin-America-and-the-Caribbean.pdf.

[168] Business at OECD, "Regulatory sandboxes for privacy: Analytical report," *BIAC,* Paris, France, Nov. 2020. [Online]. Available: https://biac.org/wp-content/uploads/2021/02/Final-Business-at-OECD-Analytical-Paper-Regulatory-Sandboxes-for-Privacy.pdf.

[169] Organization for Economic Co-operation and Development, *OECD Digital Economy Outlook 2015.* OECD, Paris, France: OECD Publishing, 2015. [Online]. Available: https://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-outlook-2015_9789264232440-en.

[170] A. Fineberg, "What does it take to be a privacy professional?," *Ryerson University.* [Online]. Available: https://continuing.ryerson.ca/contentManagement.do?method=load&code=CM000167 (accessed Nov. 29, 2021).

[171] Privacy and Access Council of Canada, "Certification," *Privacy and Access Council of Canada.* [Online]. Available: https://pacc-ccap.ca/certification/ (accessed Nov. 29, 2021).

[172] The Chang School of Continuing Education, "Privacy, access, and information management," *Ryerson University.* [Online]. Available: https://continuing.ryerson.ca/public/category/courseCategoryCertificateProfile.do?method=load&certificateId=171736 (accessed Nov. 29, 2021).

[173] Federal Trade Commission, "Internet of Things: Privacy and security in a connected world," Government of the United States, Washington, DC, USA, Jan. 2015. [Online]. Available: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[174] L. Fadrique, A. Kuang, L. U. Mazza, and P. P. Morita, "Rethinking privacy agreements," CSA Group, Toronto, ON, Canada, Mar. 2020. [Online]. Available: https://www.csagroup.org/wp-content/uploads/CSA-Group-Research-Privacy-Agreements.pdf.

[175] H. C. Pöhls and N. Rakotondravony, "Dynamic consent: Physical switches and feedback to adjust consent to IoT data collection," in *Distributed, Ambient and Pervasive interactions. HCII 2020. Lecture Notes in Computer Science,* N. Streiz and S. Konomi, Eds. Cham, Switzerland: Springer Nature Switzerland, 2020, pp. 322–335. doi: 10.1007/978-3-030-50344-4_23.

[176] Future of Privacy Forum, "Best practices for consumer wearables & wellness apps & devices," *FPF,* Washington, DC, USA, Aug. 2016. [Online]. Available: https://fpf.org/wp-content/uploads/2016/08/FPF-Best-Practices-for-Wearables-and-Wellness-Apps-and-Devices-Final.pdf.

[177] M. Weir, "What are Apple's Privacy Nutrition Labels? Here's what you need to now about the new App Store feature that prioritizes user privacy," *Business Insider,* Jan. 20, 2021. [Online]. Available: https://www.businessinsider.com/what-are-apple-privacy-nutrition-labels.

[178] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder, "A 'nutrition label' for privacy," in *Proceedings of the 5th Symposium on Usable Privacy and Security,* 2009, pp. 1–12, doi: 10.1145/1572532.1572538.

[179] B. Deltor, "Promoting digital literacy in the 21st century," *DeGroote School of Business,* Sep. 08, 2021. [Online]. Available: https://www.degroote.mcmaster.ca/articles/digital-literacy/.

[180] A. Huynh and N. Malli, "Levelling up: The quest for digital literacy," Brookfield Institute for Innovation + Entrepreneurship, Toronto, ON, Canada, Jun. 2018. [Online]. Available: https://brookfieldinstitute.ca/wp-content/uploads/Level-Up-report-FINAL-online-1.pdf.

[181] T. Hadziristic, "The state of digital literacy in Canada: A literature review," Brookfield Institute for Innovation + Entrepreneurship, Toronto, ON, Canada, Apr. 2017. [Online]. Available: https://brookfieldinstitute.ca/wp-content/uploads/BrookfieldInstitute_State-of-Digital-Literacy-in-Canada_Literature_WorkingPaper.pdf.

[182] K. Brisson-Boivin and S. McAleese, "How digital literacy can help close the digital divide," *Policy Options,* Apr. 13, 2021. [Online]. Available: https://policyoptions.irpp.org/magazines/april-2021/how-digital-literacy-can-help-close-the-digital-divide/.

[183] Innovation Science and Economic Development Canada, "Digital literacy exchange program," *Government of Canada,* Nov. 22, 2019. [Online]. Available: https://www.ic.gc.ca/eic/site/102.nsf/eng/home.

[184] "Resolution for the Adoption of an International Competency Framework on Privacy Education," *38th International Conference of Data Protection and Privacy Commissioners,* Oct. 2016, [Online]. Available: https://edps.europa.eu/sites/default/files/publication/16-10-18_resolution-2016-on-privacy_education_en.pdf.

[185] Canadian Privacy Commissioners, "Joint letter to the Council of Ministers of Education on privacy education," *Information and Privacy Commissioner of Ontario.* Nov. 03, 2017, [Online]. Available: https://www.ipc.on.ca/wp-content/uploads/2017/11/joint-fpt-letter_en-005.pdf.

[186] S. Livingstone, M. Stoilova, and R. Nandagiri, "What's the role of the school in educating children in a datafied society?," *London School of Economics and Political Science,* Oct. 23, 2019. [Online]. Available: https://blogs.lse.ac.uk/parenting4digitalfuture/2019/10/23/whats-the-role-of-the-school-in-educating-children-in-a-datafied-society/.

[187] University of Bath, "Expand school digital literacy lessons to cover health technologies used by young people," *Science Daily,* Jul. 16, 2020. [Online]. Available: https://www.sciencedaily.com/releases/2020/07/200716101615.htm.

[188] A. Huynh and N. Malli, "Plugging in: Empowering communities to ensure digital literacy access for youth," Brookfield Institute for Innovation + Entrepreneurship, Toronto, ON, Canada, Sep. 2020. [Online]. Available: https://brookfieldinstitute.ca/wp-content/uploads/Plugging-In-Report-2.pdf.

[189] MediaSmarts, "Use, understand & create: A digital literacy framework for Canadian schools," MediaSmarts, Ottawa, ON, Canada, 2019. [Online]. Available: https://mediasmarts.ca/sites/mediasmarts/files/pdfs/digital-literacy-framework.pdf.

[190] Canadian Civil Liberties Association, "We are the Canadian Civil Liberties Education Trust," *Canadian Civil Liberties Association.* [Online]. Available: https://cclet.org/ (accessed Nov. 28, 2021).

[191] Office of the Privacy Commissioner of Canada, "Resources for teachers," *OPC,* Jul. 31, 2019. [Online]. Available: https://www.priv.gc.ca/en/about-the-opc/what-we-do/awareness-campaigns-and-events/privacy-education-for-kids/resources-for-teachers/.

[192] Office of the Privacy Commissioner of Canada, "Tips for parents," *OPC,* Nov. 03, 2017. [Online]. Available: https://www.priv.gc.ca/en/about-the-opc/what-we-do/awareness-campaigns-and-events/privacy-education-for-kids/tips-for-parents/.

CSA Group Research

In order to encourage the use of consensus-based standards solutions to promote safety and encourage innovation, CSA Group supports and conducts research in areas that address new or emerging industries, as well as topics and issues that impact a broad base of current and potential stakeholders. The output of our research programs will support the development of future standards solutions, provide interim guidance to industries on the development and adoption of new technologies, and help to demonstrate our on-going commitment to building a better, safer, more sustainable world.

CSA GROUP™

© 2022 Canadian Standards Association. All Rights Reserved.