Exercising Privacy: Policy Options for Privacy and Wellness Wearables

Summary for Policymakers

Wellness wearables are playing an increasing role in the lives of Canadians. These consumer products are worn on the body and use sensors to collect real-time information directly from users. This data is then analyzed to generate health and wellness insights that help users track and take action on their well-being. Because these technologies capture a high volume of sensitive and health-related information, they have significant implications for privacy. However, policy and law have generally not kept pace with these challenges despite widespread adoption.

Wellness wearables occupy a regulatory grey area, with insufficient protections for users in place. New research from CSA Group highlights some of the distinct privacy risks of these devices and promising responses to help address this public policy gap.

The emerging challenge of wellness wearables

Wellness wearables are a growing class of consumer products – from wristbands that track steps to headbands that assess emotions. While these devices are part of the broader Internet of Things, they have unique characteristics that current policy is not well equipped to address:

Wellness wearables generate information in a way that poses distinct privacy challenges

Consistently worn and uniquely connected to the body, wellness wearables, unlike other consumer technologies, generate a distinct amount and type of information:

- **Wellness wearables collect a high volume of information.** These devices enable the pervasive and passive monitoring of users, and direct collection of their data.
- **Wellness wearables collect sensitive health-related information.** These devices sense biometric, physiological, and behavioural data that is similar to medical information.

About the Exercising Privacy: Policy Options for Privacy and Wellness Wearables report

This brief is based on a CSA Group research report entitled *Exercising Privacy: Policy Options for Privacy and Wellness Wearables* written by Alannah Dharamshi and Adrienne Lipsey. The report builds on CSA Group's previous work on privacy and emerging technologies. It was developed with support from the Office of the Privacy Commissioner of Canada's Contributions Program.

Wellness wearables have high-stakes applications

While wellness wearables are largely marketed for consumer use, these are increasingly being applied in diverse contexts where power asymmetries and potential misuses may occur:

- **Workplaces are using wellness wearables** in wellness initiatives and health and safety programs. These devices, such as helmets that assess vitals and wristbands that track health conditions, are increasing the scale, scope, and intrusiveness of workplace surveillance.
- **Insurers are incorporating wellness wearables** into new interactive health and life insurance polices. These devices are enabling insurers to collect health-related information about policyholders in real-time, outside of the point of purchase and formal medical releases.

The privacy challenges

Policymakers need to consider three main categories of privacy challenges regarding wellness wearables:

Risks to information: Wellness wearables, by design, generate vast quantities of sensitive health-related and location information. Further analysis of this data, especially when combined with other sources, can generate detailed inferences about users and re-identify previously anonymized information. These insights may be vulnerable to hackers due to the weak cybersecurity practices of many wellness wearable devices and their associated apps.

Risks to consent: Wellness wearables may challenge informed consent, a cornerstone of privacy. Users often do not understand how these devices work and their privacy implications. Data may also be shared or sold to third parties and used for secondary purposes in ways that are opaque to users. Privacy policies provided by manufacturers often fail to help fill these knowledge gaps, can be difficult to find, and do not typically provide users with granular consent options.

Risks to other rights: Wellness wearables can impact other human and civil rights enabled by privacy. These devices can be designed in biased ways and reveal information that can be used for profiling and discrimination. Wearables can be misused in other ways to compromise the safety of individuals and security of states. The constant use of these devices can also restrict autonomy, weaken the boundary of private spaces, and have chilling effects on behaviour.

The current policy landscape

Although wellness wearables pose potential harms, they occupy a legislative and regulatory grey area in the Canadian policy landscape with limited safeguards from these risks. Neither true medical devices nor low-stakes consumer products, wellness wearables are presently:

- ✗ **Excluded from medical device regulations,** which provide clear cybersecurity standards, licensing requirements, and review for devices that diagnose or treat specific conditions.
- ✓ **Included under consumer product legislation,** which applies generally to all kinds of products but focuses more on physical safety and has no specific regulations for wellness wearables.
- ✗ **Excluded from health privacy legislation,** which prescribes and limits how specific custodians, typically formal health authorities, can collect, use, and disclose personal health information.
- ✓ **Included under consumer privacy legislation,** wwhich applies to commercial entities but does not directly address wellness wearable information and the applications of these devices.

Recommendations to promote privacy

Governments should collaborate with industry and civil society to ensure the privacy of wellness wearable users. Immediate interventions are needed in three areas: modernizing privacy protections, helping businesses bolster privacy, and promoting informed user choices.

Modernizing privacy protections

Legislated protections need to be strengthened and reformed with attention to the privacy risks and applications of products like wellness wearables. Policymakers should:

- **Create explicit protections for consumer health-related information** to account for the data generated by wearables. Opportunities include adjusting consumer privacy law to define sensitive information and making health privacy law applicable to consumer providers.
- **Enhance and extend privacy protections to all employees** to manage wearable workplace surveillance. Opportunities include revising consumer privacy law to better balance worker rights with business interests and creating strong privacy provisions under employment law.
- **Limit the use of wellness wearable data in insurance** to mitigate potentially unfair, discriminatory, and/or punitive uses of wearables. Opportunities include turning the privacy-promoting practices that some insurers have adopted into legislative requirements.

Helping businesses bolster privacy

Businesses, especially smaller wearable firms lacking in-house resources and expertise, need supports that enable compliance and adoption of privacy practices. Policymakers should:

- **Create standards and guidance for best practices** to help companies operationalize privacy-promotion from wearable design through to implementation. Opportunities include codes of practice and standards for privacy and cybersecurity that reflect modernized protections.
- **Change how businesses relate to regulators** to create an environment conducive to cooperation rather than avoidance. Opportunities include creating a regulatory sandbox for wearables and empowering privacy bodies to provide advance rulings or advisory opinions.
- **Develop a pipeline of privacy professionals** to equip wearable companies with the human resources they need to comply with and adopt privacy practices. Opportunities include developing more specialized training and education programs for privacy professionals.

Promoting informed user choices

Users of wellness wearables need to be equipped with the right tools to make informed and meaningful privacy choices, as a complement to other measures. Policymakers should:

- **Require enhanced notice and consent mechanisms** to give users more meaningful information and choices about their wearables. Opportunities include implementing requirements that make privacy notices and agreements more accessible and granular.
- **Encourage certification and labelling** to help make it easier for users to identify best-in-class wearables when it comes to privacy. Opportunities include facilitating the development of these types of signifiers and mandating accountability structures for their assessment.
- **Promote digital literacy** to provide users with the knowledge and skills they need to navigate wearables and manage their privacy preferences. Opportunities include creating a digital literacy strategy and developing digital skills and privacy education for children.

© 2022 CSA Group Testing & Certification Inc. All Rights Reserved.
02/2022