Health-Tracking Bracelets and Privacy Issues

Éloise Gratton
Partner
Borden Ladner Gervais LLP

Health-tracking bracelets are growing in popularity,[1] and many industry players have introduced these types of devices and apps in the last few years. We can think of the Apple Watch[2] and Healthkit[3] as well as the Fitbit App.[4] Personal fitness bracelets can track users' steps and calories burned and collect information on health, heart rate, and sleep. Gartner's recent study suggests that Smart clothing with advanced sensors is also expected to gain popularity by 2015–16.[5] These wearables may have the ability to track an individual's heart rate and workout regimens, and even take photos and videos. These devices and wearables may therefore also have the capability of collecting geolocation information (photos of running routes, *etc*.)

In the U.S., the Future of Privacy Forum[6] published a paper in January 2015 entitled *A Practical Privacy Paradigm for Wearables*[7] in which it examines how wearable technologies are challenging traditional applications of the *Fair Information Privacy Principles*, which are at the core of our Canadian data protection laws,[8] including the federal *Personal Information Protection and Electronic Documents Act*[9] and the substantially similar laws from Quebec,[10] Alberta,[11] and B.C.[12], and why policy-making in this area requires a forward-thinking, flexible approach to address privacy concerns.

What are some of the privacy concerns with these types of self-tracking devices?

Disclosing Sensitive Information

These self-tracking devices are collecting information pertaining to health and lifestyle (and potentially location), and may therefore reveal sensitive information in cases of privacy breaches. For example, it was reported in 2011 that Fitbit accidentally shared users' sexual activity online.[13] Using the App, a user can manually keep track of his/her exercise (including sexual activity) ranging from "passive, light effort" to "active and vigorous". Someone noticed that the self-trackers the company catered to were disclosing sexual activity statistics online. Because the company had historically made users' profiles and activity "public" by default (to encourage social sharing and competitiveness), some Fitbit users may not have realized this. Fitbit has, since then, updated the default settings for activity sharing for new users to "private".

Making Health Data Available to Third Parties

Although the health and location information generated by these devices may be of interest to advertisers, it is interesting to note that both Apple HealthKit and Google Fit prohibit applications from gathering data from their respective platforms for certain purposes, such as advertising.[14]

It was recently suggested that, without adequate protections, users' health information obtained via these self-trackers could be sold to insurers, mortgage lenders, or employers.[15]

In Canada, our data protection laws would prohibit companies from selling personal information to third parties, such as insurance companies or employers, without the users' prior consent. The tracking device's terms of use agreement and privacy policy could disclose the data sharing with third parties, in which case users could be said to have agreed to such sharing of their information. Since location or health information is considered as sensitive information, users will usually expect to be adequately informed of the sharing and provide their express consent to such sharing.

Using Health Information as Evidence in a Litigation

Can health information collected by these self-tracking devices be used as evidence in a litigation? These health devices may collect photos and track health and lifestyle information, which may be recoverable in litigation if the evidence is relevant to the case at hand.

The information may be willingly turned over by a plaintiff, following an accident in order to prove its detrimental effects. For instance, it was reported in the news last fall that a Canadian law firm will use information from a Fitbit fitness tracker for the first time in court as an objective measure of activity.[16] The information will be provided by the plaintiff, in a personal injury lawsuit, in an attempt to demonstrate life-affecting reduced activity post injury. The information is being willingly provided by the plaintiff and processed by data company Vivametrica,[17] which collects data from wearables and compares it with the activity and health of the general population.

The information collected via these self-tracking devices could be subpoenaed by courts if relevant for a case: an employer attempting to demonstrate the location of its employee at a given time and date, an insurer attempting to demonstrate the physical health of an insured before or following an insurance claim, *etc*.

If the information is collected by a third party, in situations in which the user has an expectation of privacy, the information may be more difficult to use as evidence, at least in some jurisdictions. For instance, in Quebec, s. 2858 of the *Civil Code*[18] prohibits the use of any evidence obtained under such circumstances that fundamental rights and freedoms are violated and whose use would tend to bring the administration of justice into disrepute. This could be the case, for instance, if the user has installed privacy settings to limit the sharing of its information, and these settings were circumvented by an employer or insurance company to access the information.

Requiring an Individual to Be Tracked via the Bracelet

Third parties, such as insurance companies or employers, could require that employees, insured, or claimants undergo assessment via fitness tracker. For instance, insurance companies could offer better premiums to individuals that agree to be tracked, similar to what we have seen with car-tracking devices, which have sparked privacy concerns.[19] Organizations could also decide to provide their employees with fitness trackers in order to potentially reduce its corporate plan insurance premiums.

These types of activities would have to comply with Canadian data protection laws (and, as the case may be, human rights laws). As a general principle, under such laws, consent is generally required before collecting and using personal information (these types of activities would therefore be prohibited if the information is collected without the knowledge of the individual), and an organization cannot collect or use information which is not "necessary".[20] This means that personal information collected and used has (1) to be directly linked to (and relevant for) the employees' position (if collected by an employer) or (2) to evaluate the insured's risk or claim (if collected by an insurance company).

Some jurisdictions may also prohibit the tracking of individuals without their prior consent. For example, under s. 43 of the Quebec *An Act to establish a legal framework for information*,[21] a person may not be required to be connected to a device that allows the person's whereabouts to be known unless authorized by law, either for health protection or public security reasons.

Conclusion

While these self-tracking devices may create new opportunities and benefits, they may also trigger

privacy concerns. The more information is collected, the greater the risk is that this information be inadvertently exposed or used by unauthorized third parties. Therefore, organizations marketing these types of self-tracking devices, including device manufacturers or app developers, will have to be transparent about (1) the ways in which they intend to use device users' personal information, (2) their willingness to share their information with employers, insurers, or any other party making an eligibility decision, as well as (3) their intentions to respond to government or law enforcement requests for wearable data. Given that these devices may contain detailed records of users' behaviours and, sometimes, their location, activity levels, and health information, adequate security measures should be used in order to ensure that these devices are appropriately secured against both internal and external threats. Given these self-tracking devices' potential for high-level connectivity, users' information will have to be adequately protected while on the device, in transit, or anywhere else, including while in the cloud.

1 *See* "Smartwatches and Smart Bands Dominate Fast-Growing Wearables Market", *CCS Insight* (August 2014), <http://www.ccsinsight.com/press/company-news/1944-smartwatches-and-smart-bands-dominate-fast-growingwearables-market>.

2 *See* <http://www.apple.com/ca/watch/?cid=wwa-ca-kwg-watch-com> (last visited March 5, 2015).

3 *See* <https://developer.apple.com/healthkit/> (last visited March 5, 2015).

4 *See* <http://www.fitbit.com/ca> (last visited March 5, 2015).

5 "Gartner Identifies Top 10 Mobile Technologies and Capabilities for 2015 and 2016", *Gartner*, February 24, 2014, <http://www.gartner.com/newsroom/id/2669915>. *See also* Juniper Research, *Smart Wearable Devices: Fitness, Glasses, Watches, Multimedia, Clothing, Jewellery, Healthcare & Enterprise 2014–2019* (August 9, 2014), <http://www.juniperresearch.com/researchstore/devices-wearables/smart-wearables/fitness-glasses-watches-multimedia-healthcare>.

6 The Future of Privacy Forum is a Washington, D.C.–based think tank whose mission is to advance responsible data practices. The forum is led by Internet privacy experts Jules Polonetsky and Christopher Wolf and includes an advisory board of leading figures from industry, academia, law, and advocacy groups.

7 Christopher Wolf, Jules Polonetsky, and Kelsey Finch, *A Practical Privacy Paradigm for Wearables*, Future of Privacy Forum (January 8, 2015), <http://www.futureofprivacy.org/wp-content/uploads/FPF-principles-for-wearables-Jan-2015.pdf>.

8 *See* Éloïse Gratton, "Still about Control: Canadian and French Data Protection Laws", in *Understanding Personal Information: Managing Privacy Risks* (LexisNexis, 2013), s. 1.1.2.2.

9 *PIPEDA*, S.C. 2000, c. 5.

10 *An Act Respecting the Protection of Personal Information in the Private Sector*, CQLR c P-39.1 (formely R.S.Q. 1993, c. P-39.1).

11 *Personal Information Protection Act* (Alberta), SA 2003, c. P-6.5.

12 *Personal Information Protection Act* (British Columbia), S.B.C. 2003, c. 63.

13 Kashmir Hill, "Fitbit Moves Quickly after Users' Sex Stats Exposed", *Forbes*, May 7, 2011, <http://www.forbes.com/sites/kashmirhill/2011/07/05/fitbit-moves-quickly-after-users-sex-stats-exposed/>.

14 *See* HealthKit, Apple Developer, <https://developer.apple.com/healthkit/> (last visited March 5, 2015); Google Fit Platform Overview, Google Developers, <https://developers.google.com/fit/overview (last visited March 5, 2015).

15 Hunter Walker, "Senator Warns Fitbit Is a 'Privacy Nightmare' and Could Be 'Tracking' Your Movements", *Buisness Insider*, August 10, 2014, <http://www.businessinsider.com/senator-warns-fitbit-is-a-privacy-nightmare-2014-8?IR=T#ixzz3MRZI63tK>; *see also* Parmy Olson, "Wearable Tech Is Plugging into Health Insurance", *Forbes*, June 19, 2014, <http://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance/>.

16 Samuel Gibbs, "Court Sets Legal Precedent with Evidence from Fitbit Health Tracker", *Guardian*, November 18, 2014, <http://www.theguardian.com/technology/2014/nov/18/court-accepts-data-fitbit-health-tracker>.

17 *See* <http://vivametrica.com/> (last visited March 5, 2015).

18 CQLR c C-1991.

19 Mark Gollom, "Car-Tracking Devices Spark Privacy Concerns: Insurance Company Says Fears Misplaced", *CBC News*, June 13, 2013.

20 Data protection laws generally provide that an organisation may collect and store data that is only required or necessary (see principles 4.4.1 and 4.5 *PIPEDA*, *supra* note 9, and articles 5 and 9 of the *Act Respecting the Protection of Personal Information in the Private Sector*, *supra* note 10. In case of doubt, personal information is deemed to be non-necessary. The *Civil Code of Quebec* at s. 37 also provides that an organisation establishing a file on an individual may gather information that is only *relevant* to the stated objective of the file.

21 CQLR, c. C-1.1.