Eloïse Gratton Partner
egratton@blg.com

Borden Ladner Gervais LLP,
Montréal

Privacy best practices for mHealth apps

In August 2016 the Washington think-tank the Future of Privacy Forum ('FPF') released Best Practices for consumer wearables and wellness apps and devices, a baseline of responsible privacy practices, while in June 2016 the European Commission ('EC') Code of Conduct on privacy for mobile health apps ('Code') was submitted to the Article 29 Working Party after being developed by a working group. Eloïse Gratton, Partner at Borden Ladner Gervais LLP, describes these initiatives and compares and contrasts their approaches.

Wearable and mobile devices that help users track physiological information can greatly improve consumers' lives. Wearable technologies - and related apps and services - can use sensors to collect environmental, behavioural, and social data from consumers. Users can monitor, evaluate, and improve something as simple as a fitness routine or as serious as a medicine schedule.

Data generated by wearables is also useful to others. It can help manufacturers improve their products. Researchers can use data collected by wearables to reveal insights, cure diseases, and provide other broad societal benefits. Insurance agencies or employers could also use the data to allocate benefits and costs.

Some information produced by wearables is explicitly sensitive. Some data sets that may not seem very sensitive at first blush can reveal more sensitive information if they are combined with other data. Yet much data derived from wearables is not medical information regarding treatment by physicians; rather, it relates to health and fitness activities chosen by consumers. Wearables data raises serious questions for global privacy regimes - how should privacy frameworks treat this information in light of the varying contexts in which it is collected and used? Data produced from wearables exists on a privacy spectrum. The lack of bright line standards to separate sensitive and non-sensitive lifestyle data means that holding all lifestyle data to a high standard would impede innovation, while holding that data to a low standard will create privacy risks for consumers.

In August 2016, the FPF published a set of Best Practices for consumer wearables and wellness apps and devices[1]. The document articulates a baseline of responsible practices intended to support a targeted FIPPs-based trust framework for the collection and use of consumer-generated wellness data. The Best Practices build on existing legal expectations and requirements established by leading mobile app platforms, providing organisations with practical guidance that can enhance compliance with legal and contractual norms.

The Best Practices follow the EC Code[2], which was drafted to be easily understandable and useful to small companies and individual developers who may not have access to legal expertise. The EC expects the Code to raise awareness of the data protection rules in relation to mHealth apps and facilitate compliance at the EU level for app developers.

The Best Practices provide consumer choice, support interoperability, and elevate data norms

The Best Practices require opt-in consent for data sharing with third parties. Opt-in consent for third party data sharing promotes meritorious use of data by app providers while ensuring that consumers will not be surprised by any third party data use. The Best Practices also require wearables app makers to provide users with the opportunity to opt-out of tailored first-party advertisements. The document permits apps to employ ad-supported models, and wearables providers can deliver tailored advertisements based on wellness data by default as long as users have the ability to opt-out of tailored ads.

The Best Practices also provide users with access, correction, and deletion rights. These options make sure that users can use and control wearable data after collection. Some wearables are collecting new and sensitive forms of data. The Best Practices advise that companies provide consumers with

continued

reasonable means to access, correct, and delete data. Access and correction tools can help promote consumer trust, data portability, and accuracy.

Under the Best Practices, companies are encouraged to provide enhanced notice and obtain express consent for incompatible secondary uses of wearables data. Enhanced notice is a process of providing effective notice outside of a traditional privacy policy. Wearable devices oftentimes lack traditional interfaces with which consumers are familiar interacting with. Because of this, consumers need a mechanism to learn about privacy practices - enhanced notices can play a key role. In addition, consumers expect to be asked for express consent when wearables data is used in ways that are incompatible with the primary purpose of collection.

Interoperability is key for the long-term growth of wearables. Companies that do business globally must be able to comply with a number of privacy frameworks developed or overseen by the FTC, EU, and APEC. The FPF's Best Practices support interoperability with global privacy regimes. Additionally, businesses must comply with the rules created by platforms that distribute wearables apps such as the Apple App Store and Google Play Store. The FPF guidance promotes compliance with current app platform requirements.

The Best Practices support sharing data for scientific research with informed consent. Valuable new data and means of processing and analysing data from wearables are constantly being developed. This data can be a very valuable resource for researchers. Insights gleaned from this data could provide significant societal benefits. However, users may not expect their data to be shared for research, and the best practices urge wearables developers to obtain informed consent from users prior to sharing data for research.

The Best Practices also support strong de-identification standards. De-identification refers to processes that anonymise or obscure direct and indirect identifiers in data such that it cannot be reasonably associated with a particular consumer or a particular device associated with a customer. This can be done after collection through an internal process or before collection through techniques including differential privacy. If a de-identification technique is robust enough, then de-identified data can be more widely used and shared under the best practices. This promotes beneficial uses of de-identified data - including for research purposes - while providing incentives for companies to protect user data through de-identification. The Best Practices urge companies to implement comprehensive data security programs. Programs should be reasonably designed to protect the security, privacy, and confidentiality of covered data. Administrative, technical, and physical safeguards must be in place, however, the robustness of the particular safeguards should be proportionate to the sensitivity of the covered data. Such programs would include, among other things, data encryption and systems testing. This guidance is valuable to all companies, but particularly to organisations new to the wellness and fitness market.

The Code provides guidance for EU wearables that collect and use wellness data

The Code provides guidance regarding privacy issues arising from consumers' use of mHealth apps. The Code discusses: user consent, purpose limitation and data minimisation, privacy by design and by default, data subject rights and information requirements, data retention, security measures, principles on advertising in mHealth apps, use of personal data for secondary purposes, disclosing data to third parties for processing operations, data transfers, personal data breach, and data gathered from children. The Code aims to provide consumers with clear and prominent information concerning the way in which their data will be used in order for them to have the ability to make an informed decision prior to using the app. The EC wants health data to be used in a way that is fair and transparent to consumers.

The Best Practices and Code attempt to achieve similar results through somewhat different means

The Best Practices and Code have similar goals - to build trust in wellness and fitness technologies while supporting innovation and beneficial uses of devices and apps. They share many priorities, including similar approaches to security and user consent for data sharing. For example, the Best Practices recommend a comprehensive security program; similarly, the Code recommends appropriate technical and organisational security measures. Both documents recognise that de-identified or anonymised data can be used for beneficial purposes and ought to be subject to more permissive use and sharing norms. In addition, the Best Practices and Code both permit use of wellness data for research if certain rules are followed. The Best Practices require specific, informed consent for research use, unless such use is approved by an ethical review panel. The Code allows the processing of data for historical, statistical or scientific purposes, even when such uses are not authorised by the user, provided that it is done in accordance with national and EU rules for secondary processing. Finally, the documents take similar approaches to sensitive data - both the Best Practices and the Code urge enhanced mechanisms for providing notices and obtaining consent for wellness data that is particularly sensitive.

However, there are differences between the approaches regarding advertising and third party data sharing. The Best Practices focus on the use of consumer wellness data for advertising, while the Code is focused on advertisements made to consumers generally. The Code requires explicit opt-in authorisation from the consumer when advertising is not compatible with the original purpose of collection or processing. The Best Practices establish similar guidance for third party sharing generally - it is permissible with users' opt-in consent. However the Best Practices forbid sharing covered data with data brokers and ad networks, even if the user explicitly consents. In contrast, the Code permits sharing with data brokers and ad networks as long as opt-in consent is obtained.

1. The Future of Privacy Forum (FPF), Best Practices for Consumer Wearables and Wellness Apps and Devices, 17 August 2016, available at: https://fpf.org/wp-content/uploads/2016/08/FPF-Best-Practices-for-Wearables-and-Wellness-Apps-and-Devices-Final.pdf
2. European Commission, Code of Conduct on privacy for mHealth apps, 7 June 2016, available at: https://ec.europa.eu/digital-single-market/en/news/code-conduct-privacy-mhealth-apps-has-been-finalised