New York Law Journal
A NEW YORK LAW JOURNAL SPECIAL SECTION
An ALM Publication

Cyber Security and Privacy

WWW.NYLJ.COM
MONDAY, MARCH 2, 2015

Wearable Technology: Taking Privacy Issues to Heart

SERGEY NIVENS / BIGSTOCK

BY KAREN H. BROMBERG AND DUANE A. CRANSTON

The debut of the Apple Watch in fall 2014 may mark a watershed moment not only in the technology industry, but also in the areas of privacy and health law. The technology embedded in the watch—and in competing devices, such as Fitbit and Jawbone—effectively shifts health care from the physical to the remote, and in the process creates a mechanism for the online collection of highly sensitive health information. The benefits are evident: Each device provides users with the ability to track their steps and calories burned throughout the day and to record their sleep history. As a general rule, the applications request the entry of detailed personal information such as age, height, weight, heart rate, and the users' residence, and also require the permissioning of geo-location in order to track a user's activity, thus recording his or her whereabouts—thereby creating data that advertisers, health plans, insurance companies and cyber criminals would clearly love to have. What happens to all this data on how and where we move about all day and night? At least for the moment, there is no clear legislative or judicial framework that squarely addresses all of the concerns raised by the development of these devices.

Use of Health Information

Some of the legal implications of the collection and use of health information have become clear in a recent Canadian court case involving the health activities of a Fitbit user. The case concerns a personal injury claim in which the plaintiff's attorneys used data collected by a Fitbit wristband as evidence of their assertion that the plaintiff's physical activities diminished since the accident in which she was allegedly injured. The case not only presents issues concerning the admissibility of such evidence, but also opens up the related potential issue of when the disclosure of such information can be compelled for the contrary purpose of undermining a plaintiff's or witnesses' statements regarding their physical activities and health status.

Outside of the legal context, this information could also be used by service providers in the health care field to evaluate the health of service recipients. This could include the use of this information as a type of health "credit check" by health care providers, insurance companies and other entities in the medical field seeking to verify health information for the purpose of determining the risks associated with patient care. Such information could potentially be used adversely to determine insurance pricing based on these risk assessments, or to restrict or deny certain treatment options entirely.

Legal frameworks, such as the one estab-

KAREN H. BROMBERG *is a partner at Cohen & Gresser and head of the firm's intellectual property and technology group.* DUANE A. CRANSTON *is an associate at the firm.*

lished under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), set out privacy and security rules that govern how certain entities in the health care field use and protect personal health information. This legal framework includes prescribing actions required to be taken by such entities in the event of a security or data breach that results in the disclosure of such information. However, HIPAA delineates certain distinct categories of entities to which its requirements apply for the purpose of protecting and regulating the use of this information. Companies such as Fitbit, Jawbone and Apple, which develop hardware and software applications that collect, store and analyze this data, are not expressly subject to HIPAA. Nor is the type of health data they collect formally considered Protected Health Information (PHI) unless it's shared with a doctor, hospital, or third party vendors. Accordingly, the protection of wearable fitness device users' privacy has thus far been left to private entities. The absence of any regulations that explicitly apply to these devices and related software applications points to a void in the law that could leave personal health information subject to unintended uses. This is an area rife with potential for new legislation and/or litigation.

Collection and Sale to Third-Party Users

Users of these wearable health monitoring devices are often contributing health information to a centralized database maintained by the device maker. Although users likely do not want third parties looking at their data, most fitness trackers' privacy policies disclose that they will share a user's data with third parties. And because HIPAA does not yet apply to this industry, unless you live in a state which treats this data as PHI, assume that the makers can legally share a user's sensitive medical data without a user's express consent (unless of course the device makers explicitly represents that it doesn't share such information.

The actual use of personal data became clear this past summer when Jawbone posted a graph showing how its users living in the Bay area woke up during the earthquake. The graph plotted users by location, and demonstrated how people who lived closer to the epicenter were likely to wake up while far fewer did so farther away. While this information was aggregated and did not publicly disclose the names or identities of any of their users, it shows how personal information can be collected, tracked and used.

Moreover, even if the device makers are not sharing a user's data with third parties, this is often the unintended consequence because it is not unusual for the default privacy to be set to public, thereby allowing a user's profile to be located in search results. Of course, a user can easily remedy this issue by privatizing the device's settings.

Security

Wearable health device users are entrusting the device makers to gather their personal health information, but it is unclear what measures the device makers or their third-party partners will take to ensure that a user's PHI is safe and secure. Many privacy policies indicate that they "protect your personal information from unauthorized access, use, or disclosure," but what does that really mean? Do they encrypt sensitive information, what industry standards do they follow when it comes to security, and what precise steps are taken to guard against unauthorized access and misuse of personal information?

The FDA requires mobile medical app developers to create a cyber security plan and submit it to the FDA along with their mobile medical app and medical device submission. But this only applies to mobile medical apps and not to wearable health technology generally.

The FTC also has an interest in regulating health care data privacy and security. This past January, the FTC issued a staff report entitled "Internet of Things: Privacy & Security in a Connected World," which highlighted some of the Commission's privacy and security concerns with respect to connected devices such as wearables, home thermostats, security cameras and car sensors with the capability to collect and transmit personal information on the activities, habits and health of their users. While the report stopped short of recommending legislation specifically addressing these connected devices, the staff noted that the emergence of these devices highlights the need for federal legislation that would enhance data security and breach notification requirements to protect consumers.

Conclusion

The progress of mobile technology from large, fixed machinery to wireless accessories capable of recording, analyzing, and transmitting private health and social information online opens up a range of unprecedented privacy concerns. Federal and state lawmakers and regulators will be challenged to keep pace with the development of applications with capabilities that are difficult for legislators to anticipate. In the absence of comprehensive legislation that addresses these new privacy concerns, consumers should be proactive in taking steps to protect their personal information. These steps include reviewing the privacy policies associated with the devices they use and, whenever practicable, opting out of sharing personal information or giving companies permission to do so. Users should also avoid connecting to third-party Wi-Fi and Bluetooth networks unless truly necessary. Finally, users should be mindful of when and how their devices track their activities and limit such tracking by turning off geolocation services, at least when they are not trying to track their activity. It may take a few well-publicized privacy breaches involving these devices to precipitate a sharper focus from governmental agencies on wearable privacy and security. In the end, it may be the public discussion of privacy concerns and the impact of this debate on the consumer market for these devices that has the greatest impact on regulating the collection and use of personal health information.

COHEN & GRESSER LLP