Privacy, Security, and Wearable Technology

By Janice Phaik Lin Goh

Janice Phaik Lin Goh is an attorney at Arent Fox LLP in New York. She is also a Certified Privacy Professional (CIPP).

Not so long ago, a polo shirt was made of cotton, synthetic wool, and maybe silk. Today, a polo shirt can come equipped with bio-sensing silver fibers that can track the number of calories you burn and your heart rate, and stream this real-time biometric data directly to your phone. In today’s world of wearable devices, our day-to-day apparel and accessories are turning into networked mobile electronic devices that attach to our body. The market is now flooded with wearable devices that include wristbands such as Fitbit and Jawbone, attachable baby monitors such as Mimo and Sproutling, watches such as the Apple Watch, and jewelry such as Cuff and Ringly. The wearable market is rapidly growing; according to the International Data Corporation (IDC), shipments of wearables will reach up to 45.7 units in 2015, a 133.4 percent increase from 2014. Morgan Stanley has predicted that the wearables market will eventually become a $1.6 trillion business.

Wearables have been touted to improve efficiency, productivity, and engagement. Unlike a mobile phone or laptop computer, wearables are usually worn or incorporated into the body, thus providing sensory and scanning features that facilitate biofeedback and tracking. In a recent PwC study, 57 percent of the individuals surveyed believed that people will rely more on wearables for support than their friends and family, 73 percent of participants expect wearables to make media and entertainment more immersive and fun, and 70 percent of consumers reported they would wear employer-provided wearables that streamed data in exchange for breaks on insurance premiums.

While wearables can provide consumer benefits in the areas of health care and wellness, wearables also raise privacy and security concerns. The more devices and sensors introduced into our clothes, shoes, and accessories, the greater the volume and sensitivity of data that will be collected through these devices. As mentioned above, wearable devices are generally designed to be worn on the body, therefore allowing for the collection of new and sensitive data. For example, a Fitbit can collect data on the number of calories you burn, the PillCam can detect bleeding in the gastrointestinal tract, and ADAMM can collect your breathing and coughing patterns to predict asthma attacks. As Federal Trade Commission (FTC) Chairwoman Edith Ramirez has noted, while these devices are capable of providing increased convenience and improved health services, they are also “collecting, transmitting, storing, and often sharing vast amounts of consumer data,” thus creating a number of privacy risks. In particular, wearable devices challenge traditional privacy principles and pose a distinct challenge to the collection, use, and storage of health, location, financial, and other sensitive information.
Challenges to Traditional Privacy Principles

Wearables may present challenges to traditional privacy practices and principles, such as the Fair Information Practice Principles (FIPPs).\(^\text{18}\) The basic FIPPs include principles such as (1) collection limitation, (2) purpose specification, (3) use limitation, (4) accountability, (5) security, (6) notice, and (7) choice.

Principles of notice and choice, in particular, will be difficult for wearables in that they are screenless or simply lack input mechanisms; thus, users are unlikely able to access a privacy policy through these devices or provide affirmative consent to a privacy policy.\(^\text{19}\) Consent would have to be obtained through an associated website or mobile app, or through the box.\(^\text{20}\) On the other hand, it is also possible that wearable technology could lead to greater innovation in notice and choice mechanisms.\(^\text{21}\)

Wearables also present potential security risks that are heightened due to the various vulnerabilities created through the increased means of collecting, storing, and processing data.\(^\text{22}\) With wearable devices, data can be stored locally, or transmitted and stored on a cloud. When stored locally, data is vulnerable to being attacked by malware or being stolen by physical theft.\(^\text{23}\) When data is sent from a wearable to the cloud or a mobile phone, this is a weak point for hacking, and unlike a computer or mobile phone the compact nature of wearables makes it harder to secure data flows.\(^\text{24}\)

Use limitation and data minimization principles are also challenged in light of the pervasive collection of data and the nature of use of personal data.\(^\text{25}\) While consumers may be limiting the use of data from wearables for health monitoring or entertainment, the data collected by the device could be used by third parties such as insurance companies without the consent of the consumer.\(^\text{26}\)

The challenge in this area lies in balancing the interests of various stakeholders. Companies may need to collect and use data to satisfy business or research purposes and be able to innovate around new uses of data.\(^\text{27}\) But, it is possible, and encouraged, to adopt best practices to stay in line with these privacy principles. Such practices can include minimizing the collection, storage, and use of data; adopting de-identification procedures; conducting risk/benefit analyses around the use of data; and providing clear notice and consent mechanisms.\(^\text{28}\) By keeping traditional privacy principles in mind, companies can build consumer trust and minimize security vulnerabilities.

Location Information

The wearables market is flooded with devices that collect location information with gadgets such as Fitbit, Jawbone, Moov Now, and GPS SmartSole, to name a few. Wearables generally track user movements through accelerometers and gyroscopic sensors that generate data.\(^\text{29}\) In order for these devices to tell a consumer how many steps he or she has taken, or how many calories were burned, these devices have to collect data from various sensors, store the data, and process the data locally or transmit the data to a cloud server and/or mobile app in order to present the data to the user in a comprehensible format.\(^\text{30}\) For example, the GPS SmartSole, a device that fits into one’s shoes, tracks the whereabouts of individuals who are prone to getting lost due to conditions such as memory impairment by sending a signal to a central monitoring website that shows the exact location of the user.\(^\text{31}\)
In one study, Symantec found that all wearable activity tracking devices it surveyed are vulnerable to location tracking. Because location information discloses a user’s movements in real time and creates a record of a user’s movements, this information can raise a host of privacy concerns. While this information can be beneficial for personal use, consumers are not always aware of where this information is going and with whom it may be shared. According to Symantec, 52 percent of self-tracking apps do not have privacy policies or statements that inform consumers about the device’s processes around data collection and use.

In June 2014, Jessica Rich, director of the FTC Bureau of Consumer Protection, testified before the Senate Judiciary Committee’s Subcommittee for Privacy, Technology and the Law about the FTC’s efforts to address the protection of geolocation data, and the concerns raised by tracking customer locations. In Rich’s testimony, she discussed how location data can disclose very personal details about an individual, such as whether an individual visited an AIDS clinic, a physician’s office, or places of worship. Such data can be misused and mishandled, especially if accessed by hackers, sold to companies that can build user profiles without consumer consent, or collected by stalking apps. Geolocation information can also facilitate criminal behavior such as stalking, domestic violence, burglary, and kidnapping, as such information can easily identify an individual’s present or future location.

Despite the sensitivity around the collection and use of location information, there is currently a lack of federal regulations that address tracking technology. Senator Al Franken re-introduced the Location Privacy Protection Act in March 2014 that, if passed, would prohibit a covered entity (nongovernmental individual or entity) from knowingly collecting or disclosing geolocation information from an electronic communications device without the consent of the user, except if under a court order or request by law enforcement, to allow a parent to locate a minor child, or to provide emergency services. The bill defines “geolocation information” as specific information not in the contents of a communication that is generated or derived from the operation or use of an electronic communications device and is sufficient to identify the street and city or town in which the device is located and does not include the IP address or the home, business, or billing address of the individual. The bill also bans the development and distribution of GPS “stalking apps” and would criminalize the unauthorized disclosure of geolocation data that would aid interstate domestic violence or stalking.

The proposal of the Location Privacy Protection Act and similar bills, such as the Geolocation Privacy and Surveillance Act (GPS Act), demonstrate that lawmakers are increasingly concerned about location information. In fact, the FTC also considers precise geolocation information to be sensitive personal information and has settled cases relating to the collection of geolocation information. For example, Nomi Technologies recently agreed to settle FTC charges that it misled consumers with promises to provide a mechanism for consumers to opt out of tracking. According to the FTC complaint, Nomi used mobile device tracking technology to provide analytics services to brick and mortar retailers; Nomi’s sensors at retail locations could detect media access control addresses broadcast by mobile devices, and Nomi collected information about each mobile device that was within range of its sensors or clients’ Wi-Fi access points. Between January and September 2013, Nomi had collected information for about approximately nine million mobile devices. Nomi, however, did not provide any in-store opt out mechanism to consumers, and consumers were never informed when the tracking was taking place.
Despite the company’s promise to provide an opt out mechanism. Under the terms of the settlement, Nomi will be prohibited from misrepresenting consumer’s options for controlling whether information is collected, used, disclosed, or shared, as well as the extent to which consumers will be notified about information practices.

Similarly, in April 2014, the FTC approved a final order settling charges against Goldenshores Technologies LLC for deceiving customers with a privacy policy that did not accurately reflect the app’s use of personal data. According to the complaint, tens of millions of users had downloaded Goldenshores Technologies’ Brightest Flashlight Free app. The complaint alleged that Goldenshores’ privacy policy and end user license agreement did not adequately disclose to consumers that the app transmitted or allowed the transmission of device data, including geolocation data, to third parties such as advertising networks. Under the terms of the settlement, Goldenshores was prohibited from misrepresenting its use and collection of consumer information and required to provide just-in-time disclosure to fully inform consumers when, how, and why their geolocation information is collected, shared, and used. The settlement also required Goldenshores to obtain consumers’ affirmative consent before collecting geolocation information.

Although these FTC enforcement actions have not been directed specifically at wearable devices, it is likely that the FTC can assert its authority to enforce actions in the wearables space. In fact, the FTC has already taken action in the Internet of Things arena in its settlement with TRENDnet Inc. over its failure to provide reasonable security to prevent unauthorized access to sensitive information from live camera feeds. In addition to FTC enforcement, industry self-regulation can also help mitigate these risks through security by design, using secure protocols to transmit data, providing users with privacy policies that accurately describe the collection and use of consumer data, and implementing technical and administrative safeguards for backend systems and servers.

Health Information

A recent Mobile Ecosystem Forum (MEF) report on the use of wearable devices in the health sector found that the current global health and fitness app market is worth $4 billion and is slated to be worth $26 billion by 2017. Wearables are now being touted as the revolution in health care. Wearables such as insulin pumps allow individuals to record, track, and monitor their own vital signs without having to go to a doctor’s office. With connected health devices that facilitate the access and transmission of health data to doctors, or that allow users to passively track vital data points, such devices are capable of improving the quality of life and safety.

The flip side of the coin is that the ubiquitous collection of such healthcare information creates a number of security and privacy risks. In an FTC study of 12 health-related mobile apps, the FTC found that these apps transmitted sensitive health conditions such as pregnancy, gender information, and ovulation information to 76 third parties such as ad networks and analytics firms. A recent study by EMC Corporation shows that data obtained from health records is about 50 times more valuable than credit card information on the black market, as such data can be easily used for fraud and identity theft.
The privacy and security risks associated with healthcare information lead to a melee of problems: bad credit, inaccurate health records, higher premiums, loss of insurance coverage. In addition, someone could hack into your computer and change patient medical information. Yet, in spite of the risks involved with health information, privacy and security laws may not apply in these arenas.\(^6\)

HIPAA generally sets national standards for the protection of health information, which includes electronic and other forms of mediums containing identifiable demographic and other information relating to an individual’s past, present, or future physical or mental health or condition, or information concerning the provision of health care to an individual that is created or received by a healthcare provider, health plans, employer, or healthcare clearinghouse.\(^6\) Under HIPAA, “covered entities” are required to implement standards to protect individually identifiable health information: the HIPAA privacy rule defines and limits the circumstances under which an individual’s protected health information may be used or disclosed by covered entities.\(^6\) The security rule addresses the technical and nontechnical safeguards that covered entities are required to have in place to secure protected health information, such as breach notification obligations, workforce training, and mandatory audits.\(^6\)

While HIPAA standards provide some safeguards for healthcare information, HIPAA applies only to “covered entities,” which are essentially medical providers and their related business associates. Thus, with a lot of wearables where information is collected, used, or processed by individuals and entities outside the definition of a “covered entity,” HIPAA obligations and regulations do not apply. In fact, a recent study found that most data flows from mobile health apps are not covered by HIPAA.\(^6\) In the absence of appropriate controls over user-generated health information, companies have greater leeway to collect and use this sensitive data from consumers outside the context in which consumers provide such information.\(^6\)

Conclusion
As the wearables market continues to expand and grow, questions still remain as to the legal and regulatory framework that applies to the wearable industry. In the absence of express legislation or regulations around consumer privacy and security in the wearables space, industry solutions can step in to help safeguard privacy and security. For example, FTC Chairwoman Edith Ramirez has pointed out that companies can protect consumer privacy and security by (1) adopting security by design, (2) engaging in data minimization, and (3) increasing transparency and providing consumers with notice and choice for unexpected data uses.\(^6\) By providing greater transparency and choice and implementing adequate safeguards, the wearables industry can help promote and build trust in this burgeoning marketplace.

Endnotes


23. *Id.*


ABA Section of Intellectual Property Law

27. *Id.* at 33.
28. *See id.* at 27–46; *WOLF ET AL.*, *supra* note 18; *Ramirez*, *supra* note 16.
30. *Id.* at 13.
37. *Id.*
38. *Id.*
41. *Id.*
42. *Id.*
43. FTC Geolocation Privacy, *supra* note 35.
46. *Id.* at 2.
47. *Id.*
51. *Id.* at 3.
53. *Id.*

57. FTC STAFF REPORT, supra note 25, at 7.

58. Id. at 7–8.


62. 45 C.F.R. § 160.103.

63. Id. § 164.502(a).

64. Id. §§ 164.312, .314(a)(1).

65. FTC Health Data Seminar, supra note 58, at 15 (comments of Latanya Sweeney).
