InsideCounsel.com
BUSINESS INSIGHTS FOR LAW DEPARTMENT LEADERS
FEBRUARY 12, 2015



Taking the pulse of digital health: Key legal issues surrounding wearable technology

Wearable devices present obvious privacy and security challenges for developers and manufacturers

BY ANDREA L. GOTHING, SETH A. NORTHROP, LI ZHU

Imagine waking up to find your most intimate activities posted on the Internet for the entire Googling world to see (including your mom). In 2011, this was a reality for users who purchased a FitBit that not only tracked every step, but also logged every type of «exercise,» from cuddling and kissing to more. While Fitbit quickly secured the data, it was a wake-up call for companies developing wearable devices that track information related to health and fitness. Analysts estimate the retail market for wearables generated $1.4 billion in 2013, and that the industry will surpass $70 billion by 2024. To date, these wearables have appeared in different shapes and sizes — from fitness bands that monitor heart rate to glucose monitors for diabetics. Given the personal nature of the information at risk, these devices present obvious privacy and security challenges for developers and manufacturers. Just ask FitBit.

An easy operation?

A recent survey indicated that only 50 percent of users activate the security features on their mobile devices. This is not surprising. Given the number of devices and accounts consumers deal with on a daily basis, typical security measures and consent policies have become overwhelming and difficult to track. Moreover, recent highly-publicized data breaches demonstrate just how difficult it is to protect customer data from determined hackers. The industry need look no further than the father who, in 2014, "hacked" into his daughter›s glucose monitor so that he could monitor her blood-sugar levels on his smartwatch. While this individual had good intentions, many do not. In fact, data breaches hit a record high in 2014, with the greatest percentage of these occurring in the medical and healthcare industry. Accordingly, security exposures will rise as the number and sophistication of wearables increases.

Many cooks in the kitchen

While no one set of privacy and security regulations govern health and fitness devices, various government and state agencies have promulgated regulations to protect consumer and health information. Companies offering wearable devices must become familiar with these regulations. Some of the more prominent regulations include the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act), which govern health information shared with medical providers. In addition, the Federal Trade Commission (FTC), as well as some states — notably California — have issued rules governing the use and protection of customer data.

At the federal level, companies that track, store, and share users' health information with healthcare providers such as doctors, hospitals and some third-party vendors must be aware of HIPAA — the seminal regulations on health care data and privacy. While personal health data stored on a wearable device, such as calories burned, is not subject to HIPAA, HIPAA may apply if the device transmits the same information to a doctor or other healthcare provider. In this case, the company must comply with a number of security measures, including passwords, firewalls and updated security software. Otherwise, the company may be subject to steep financial penalties, among other things.

The HITECH Act supplements the HIPAA requirements by imposing mandatory penalties for "willful neglect" leading to exposure of health information. The Act requires a company to notify patients regarding certain breaches.

In addition to legislative regulations, the Federal Trade Commission Act has been used to punish companies who have failed to implement "commonly-used" and "readily available" data security measures to safeguard consumer data, such as firewalls, password protection and data encryption. Notably, the FTC has pursued companies that do not follow their own published security policies and has settled privacy claims with multiple companies over this issue. The FTC may levy financial penalties, regulatory restrictions and mandatory FTC reviews of security operations spanning decades.

And the states have also gotten into the mix. Take for example California, which recently amended its data breach notification laws to require businesses to use reasonable security measures to protect personal information that they merely maintain, such as names, social security numbers and driver's license numbers. Further, Silicon Valley companies must remember to "offer to provide appropriate identity theft prevention and mitigation services" for at least a year to customers affected by a breach. In addition, the California Online Privacy Protection Act (CalOPPA) requires businesses that collect personally identifiable information over the Internet to disclose their privacy policies. And with respect to children, California's Student Online Personal Information Protection Act (SOPIPA) prohibits companies with "actual knowledge" that their products are being used for K-12 school purposes from using or selling student data for non-educational purposes.

Preventative measures

So how can an organization avoid falling into a security or regulatory pitfall? First, seek out experts familiar with these privacy rules to determine the company's exposure. Does your wearable device communicate with software from a healthcare provider such that you would be subject to HIPAA? Which state regulations must you comply with?

[InsideCounsel].com
BUSINESS INSIGHTS FOR LAW DEPARTMENT LEADERS
FEBRUARY 12, 2015

From there, the company should work with its experts to analyze and update the company's privacy measures to comply with federal and state regulations. This means implementing a policy that includes "commonly-used" and "readily available" data security measures to protect consumer data, such as restrictions requiring consumers to use complex passwords, setting up basic firewalls, encrypting data, installing updates and security patches for operating systems, monitoring the network for malware used in previous intrusions and restricting third-party access to the network. The company must stick to the security policies it advertises or risk being brought into court by the FTC for "unfair" and "deceptive" trade practices.

Finally, the company should launch an internal campaign stressing the importance of designing secure technologies. Technical leads are often more focused on driving a project to completion or turning out a minimum viable product, and security may not receive the necessary attention before release.

Data privacy concerns will increase as wearable technology becomes more mainstream. Companies selling wearables can, however, place themselves in the best position to comply with the complex web of federal and state regulations

About the Authors

Andrea L. Gothing
Andrea Gothing is an attorney at Robins Kaplan LLP. She assists clients with complex technology-centric challenges including intellectual property, business, cybersecurity, and privacy litigation. algothing@robinskaplan.com

Seth A. Northrop
Seth Northrop is a trial attorney at Robins Kaplan LLP. whose practice focuses on intellectual property and global business and technology sourcing. He has substantial experience with complex business litigation involving various technologies including software and hardware design, analytics, networking, database, and E-commerce systems. sanorthrop@robinskaplan.com

Li Zhu
Li Zhu is an attorney at Robins Kaplan LLP. He assists clients with complex technology-centric challenges including intellectual property, business, cybersecurity, and privacy litigation. lzhu@robinskaplan.com