INTERNET OF THINGS

WHAT IS IT?

According to Wikipedia, the Internet of Things (IoT) encompasses the network of physical devices, vehicles, home appliances and other items embedded with software that enables these "things" to connect to the internet and collect and exchange data. It is estimated that the IoT will exceed 6.4 billion devices by the end of 2016, and as many as 30 billion objects by 2020. The wearables market alone is expected to be worth $25 billion by 2009, while home security market will be valued at $53 billion by 2022. See Motley Fool (11/25/17). Because IoT devices automate processes (such as turning on household appliances) and track and share data (think, Fitbits), some of the legal issues that these technologies raise intersect with two other topics covered - data & privacy law and robot law. But as discussed, there are other issues unique to Iot.

WHY NOW?

The law of IoT is a hot legal issue for a number of reasons. For starters, IoT encompasses range of diverse devices: medical devices, home security systems, children's technology and voice-activation home tools like Alexa and Google Home. The technology isn't expensive and many consumers have quickly integrated these devices into their everyday lives. This widespread use likewise means that there are many opportunities for something to go wrong - raising questions about which entity is to blame: the device developer? the user? or other third party technology that links the two?

Because the law is not clear, IoT doesn't just raise legal issues, but policy questions. In 2013, the FTC convened a workshop on security and privacy in IoT (online at which lead to publication of a report recommending best practices. See A few months ago, the Department of Commerce convened a working group to develop procedures by which IoT providers provide security updates to customers. See Department of Commerce Draft Doc on IoT. Even Congress has also taken a stab at increasing regulation of IoT with proposed legislation to require that IoT devices purchased by the U.S. government meet certain cybersecurity standards. See https://www.warner.senate.gov/public/index.cfm/2017/8/enators-introduce-bipartisan-legislation-to-improve-cybersecurity-of-internet-of-things-iot-devices.

KEY LEGAL ISSUES

Data Security - Any digital device with an internet connection is vulnerable to hacking. As IoT devices become more widespread, they have become a target for hackers. Perhaps to facilitate

connection, security on IoT devices is less than idea - few IoT devices encrypt data they collect and users employ weak access credentials. IoT manufacturers' lax security is already the subject of at least one lawsuit, *Toyota, Ford, and General Motors. Cahen v. Toyota Motor Corp.*, No. 3:15-cv-01104 (N.D. Cal. Mar. 10, 2015)(alleging that defendants sold unsafe cars because their Internet connectivity creates vulnerability to hackers,who could then gain control of the cars' operation). Moreover, when it comes to cybersecurity, what is the appropriate mechanism for assigning liability? Should manufacturers be strictly liable for damages flowing from an inherently insecure design, and if so, to what extent? Or should careless users bear the blame for IoT security breaches.

Privacy Issues - Because IoT technologies collect data, there's a potential for privacy violations if data isn't sufficiently secured and anonymized, or if users aren't aware that data is being collected to begin with. Two recent examples: In *NP v. Standard Innovation*, Case No. 1:16-cv-8655 (ND 2016), plaintiffs settled a class action lawsuit for privacy violations against a"smart" vibrator company for $3.75 million, where the company failed to disclose to its customers that it collected data on usage and other information that would allow for identification of the customer and further, was susceptible to hacking. See Chicago Tribune, (6/9/2016).

And pending at the 7th Circuit (No. 16-3766) is an appeal of a ruling in *Now Naperville v. Smart Meter Awareness*, 114 F.Supp. 3d 606 (ND Ill. 2015), where the court dismissed plaintiffs' claims that data collection by smart meters installed by the utility in their homes violated their privacy rights under the Fourth Amendment and the Illinois Constitution.

Consumer Protection/False Advertising Like any consumer product, IoT devices are subject to consumer protection laws. Using its authority under Section 5 of the FTC Act, the FTC has initiated enforcement actions against three different IoT companies. The FTC alleged that each company's representations about the first-rate security of their respective systems were deceptive when a hacker readily accessed on of the systems and posted 700 IP addresses to the company website, while in another case (involving among other things, baby monitors), the company failed to address obvious and and easy to fix security flaws. See e.g., FTC Website (1/2017). States have also pursued false advertising claims under state law: in May 2017, the New York AG's office settled a case with a company that provides insecure wireless doors and padlocks which had been marketed as secure.

Discovery Issues - Already, lawyers have found opportunities to make use of IoT data in both civil and criminal cases. In one case in Canada, Fitbit data was obtained and will be used to show that the plaintiff's activity levels deteriorated from her baseline after an accident. See In another case, a woman's claim that she had been asleep when an intruder entered her house was disproved by Fitbit data which showed that she was awake and walking around her house. http://abc27.com/2015/06/19/police-womans-fitness-watch-disproved-rape-report/

COPPA Issues - In October 2017, the FTC released guidance on the applicability of the Child Online Privacy Protection Act (COPPA) - which requires websites or online services to obtain parental consent before collecting personal information from children under 13 - applies to voice recordings. The new FTC regulations raise

issues about whether COPPA may apply to voice activated IoT devices, particularly those aimed at children. See https://www.lexology.com/library/detail.aspx?g=52e44267-270f-4503-8e98-e948cd3afe46 Concerns about children's use of IoT is not hypothetical in light of a recent study that found that most IoT toys for kids can be easily hacked. See Smart Toys Let Attackers Listen to Your Kids, Tech Dirt (11/04/2017)

Discovery Data from wearables and other IoT devices can be subpoenaed during discovery. In a recent case, Amazon moved to quash a subpoena seeking recordings from an Amazon echo, asserting that the responses are protected First Amendment speech (ultimately, the defendant consented to release of the data) See Evidence from Wearable Tech, ABA Journal (3/17/17).Even when data is made available, there may be obstacles to admissibility since Iot devices raise questions regarding (1) the reliability of the data, (2) what the data actually means (since different devices store raw data differently), and (3) whether the chain of custody was preserved.

Compliance Issues - Counsel for companies that develop IoT devices must be familiar with the above issues to help their clients comply with applicable law. The FTC has a useful interactive, online guide to help developers of mobile health apps identify applicable laws. Compliance is further complicated because as discussed above, IoT devices are subject not only to federal law but also to different state laws.

Future Opportunities & Trends:

Expect new rules to evolve over IoT and perhaps for Congress to step in. IoT providers will have a difficult time complying with different state consumer protection laws without some universal guidance. At some point, applicable privacy laws - such as HIPAA for health care devices - may be expanded to cover IoT devices In addition, attorneys will continue to push the envelope on the extent to which IoT companies may be held liable for privacy or security breaches, even where there is no harm. One final emerging issue is whether de-anonymization of data is sufficient to truly protect privacy, and how to strike a balance between permitting providers to aggregate data to improve a product and allowing users to retain full control and ownership of data they generate. The FCC's potential end to net neutrality is also expected to impact IoT - which requires substantial bandwidth - and could give rise to anti-trust actions as ISPs compete to offer exclusive service to specific providers in exchange for increased payments, or attempt to tie internet service to specific IoT apps.