Key IP and Data Privacy Issues in the Internet of Things

Chris Anderson and Tricia Brauer
Neal, Gerber & Eisenberg, LLP

The Internet of Things ("IoT") is taking over and driving much of the future of the consumer technology economy. At its core, the IoT is simple: it refers to everyday objects connecting via the Internet and talking to users, applications and each other. For example, IoT shoes allow users to adjust their foot temperatures while tracking their fitness information.\(^1\) According to some estimates, by the year 2020, over 25 billion IoT devices will be online.\(^2\)

While the various legal issues presented by the IoT are not independently novel, the IoT brings together multiple, previously unrelated, legal issues – data security and privacy, intellectual property, and consumer protection, together with other legal issues typically encountered by growing companies – corporate governance, labor, benefits, tax and others. Below are some key legal issues that have taken center stage through the recent growth of the IoT market and should be considered by growing IoT companies.

1. Data Security & Privacy: One of the primary concerns pertaining to the use and provision of IoT devices is the direct collection, protection and use of sensitive personal information (including precise geolocation, financial account numbers, health information, and habits over time). Innovation in the realm of IoT means that businesses must put into place and comply with robust privacy policies, terms of use, and customer agreements to ensure that consumers are regularly and consistently offered the opportunity to control the flow of their own data and confirm such data is adequately protected. Failure to adequately address these issues may lead to severe reputational harm and consequences from the FTC.

2. Clearing and Protecting IP Rights: Patent infringement issues are unique in the IoT space because of the convergence of multiple disparate technologies in a single device. While many IoT companies prioritize going-to-market as quickly as possible, such companies should consider taking defensive precautions to minimize risk that their products do not run afoul of third party patent rights, and offensive precautions to ensure they’ve protected key product features so that a competitor doesn’t copy a product’s “secret sauce” and take valuable market share. Also, as with other consumer products, brand strategy and protection is central to successfully marketing IoT devices. It can be very expensive to take a product to market only to later find that trademark protection is unavailable for product’s key brand(s). Accordingly, IoT companies should consider trademark clearances and registrations before investing heavily in particular brands.

3. Consumer Protection: In January 2015, the FTC released a report on IoT space noting risks to consumers that are focuses on the FTC’s radar, including: (1) unauthorized access and misuse of personal information; (2) attacks on other systems; and (3) risks to personal safety. As providers of IoT devices, companies bear the burden of addressing these risks and providing reasonable solutions that minimize the impact of such risks on consumers. The FTC’s Fair

\(^1\) www.digitsole.com
\(^2\) http://www.gartner.com/newsroom/id/2905717
Information Practice Principles (FIPPs) provide guidelines for key areas on which the FTC focuses to identify risks to consumers, including: security, data minimization, notice and choice. Though the FTC has yet to provide a comprehensive set of guidelines or enforcement criteria with respect to IoT devices, considering these factors and designing products to address these factors will minimize companies’ risk of FTC enforcement or complications.³

The IoT of presents a complex legal landscape that has the potential to implicate businesses and consumers. A strategic solution should consider intellectual property issues, data privacy issues and consumer protection issues, and should include knowledgeable counsel as part of the strategic team.

Chris Anderson, an attorney with Neal, Gerber & Eisenberg LLP in Chicago, focuses his practice on all intellectual property and commercial issues that arise in commercial contexts, including searching, clearing, procuring and enforcing intellectual property rights; structuring, drafting and negotiating all sorts of commercial, branding and technology related agreements; and counseling clients regarding data privacy, intellectual property, open source software and other key legal issues. He has experience counseling clients in a wide variety of fields and industries.

Tricia Brauer is an attorney practicing in Chicago. She graduated from The John Marshall Law School in 2013, with her J.D./LL.M. in Intellectual Property Law and focuses her practice on technology and real estate issues that arise in commercial contexts.