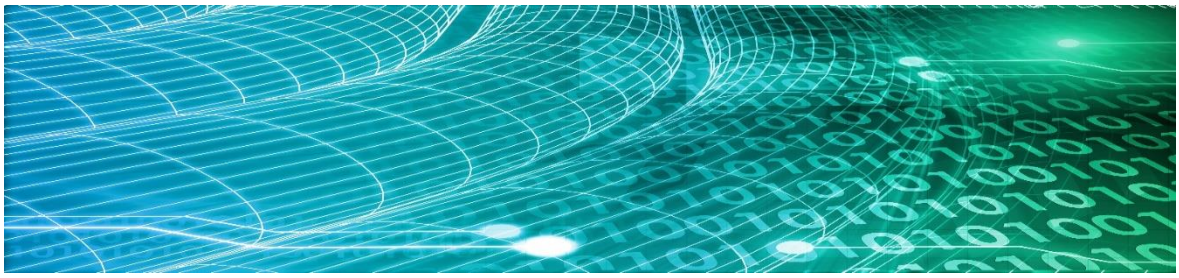

Expanding the Internet of Things:
Four Key Legal Issues

October 2020

David Verhey

Web-enabled sensors and devices with broad data-collection capabilities promise to transform life and business, but the law hasn't kept pace and could hinder development. What are the key legal issues that need to be addressed?

Technology development is occurring at a breakneck speed and it only seems to be getting faster. In the past five years alone, we've watched the introduction of the tablet, the worldwide revolution in social media, the creation of an "app" economy, and the expansion of the Android operating system as the majority choice for mobile applications. The next big leap ahead appears to be the Internet of Things (IoT), an environment of data-collecting sensors and devices with unique identifiers that have the ability to transfer data over the internet without requiring human-to-human or human-to-computer interaction. Gartner estimates that connected devices will grow from 4.9 billion in 2015 to 25 billion by 2020. In the same span of years, spending for IoT services could grow from $69.5 billion to $263 billion.

A number of Fortune 500 companies have already announced new lines of business servicing the IoT, including IBM's IoT foundation, Amazon Web Service's managed cloud platform, and General Electric's industrial IoT platform and home energy company. The federal government is active too, with the General Services Agency (GSA) fielding a network of sensors to manage buildings and the Department of Veteran Affairs developing wearable technology for healthcare applications.[1] On Capitol Hill, the U.S. Senate adopted a unanimous resolution in March 2015 which states, among other things, that the

[1] The Department of Defense has long fielded sensor technologies that could be integrated into the IoT for a wide range of missions and functions, including advanced situational awareness. See Denise Zheng and William Carter, *Leveraging the Internet of Things for a More Efficient and Effective Military*, Center for Strategic and International Studies (September 2015), p. 3.

IoT "has the potential to generate trillions of dollars in economic opportunity" and that the United States should "develop a strategy to incentivize development of the IoT for connected technologies to empower consumers, foster future economic growth, and improve collective social well-being…"

If these and similar efforts gain traction in today's market, the IoT will soon be fully integrated with daily life and commerce, transforming homes, energy delivery, business services, manufacturing, and future military requirements. But even as the IoT promises new markets and expanded benefits for business and consumers, the pace of development is racing far in front of legal and policy standards for security, privacy, government access, and product liability.

The longer those matters are left outstanding, the more likely IoT development will be slowed by contradictory judicial decisions, consumer uncertainty, and stalled investment.[2] This article briefly highlights the key issues and explains why Government and Industry need to work together to solve them.

1. Security

The first issue in the evolving IoT market is security—a subject that bears on almost every aspect of this growing technology.

For starters, the sheer size of the IoT network presents an "attack surface" that may not be readily defended with conventional firewalls and tools. In addition, a significant number of consumer devices connected to the IoT often lack basic security controls and are readily susceptible to cyber-attacks. In 2014, researchers at Hewlett Packard published a study on the security of 10 popular IoT devices that identified hundreds of vulnerabilities, including lack of transport encryption, insecure firmware updates, and poorly protected access credentials. Industry is working to address these vulnerabilities, but those efforts take time and a lot of investment.

But security issues aren't just an engineering problem. They can also generate consumer complaints and federal investigations by the Federal Trade Commission (FTC), which has statutory authority to investigate and prevent unfair or deceptive methods or acts that affect commerce. See 15 U.S.C. §§ 41-58. In 2013, for example, the FTC acted on this power and brought an enforcement action against TRENDnet, a company that marketed IoT devices for home use, alleging that the company's "lax security practices exposed the private lives of hundreds of consumers to public viewing on the Internet." Under a settlement later reached with the FTC, the company is now prohibited from misrepresenting the security of its devices and must obtain third-party assessments of its

[2] The same concern applies to the Government's role in providing adequate spectrum for the growth of the IoT—a subject that the Federal Communications Commission (FCC) is currently working to address.

security programs every two years for the next 20 years. The FTC has brought similar enforcement actions against other technology companies, many of which are described in the Commission's June 2015 publication, Start with Security: A Guide for Business.

So what does this mean? Can manufacturers produce devices that are absolutely secure and entirely free from the risk of hacking? Experts say no—and it is unlikely that the government would impose such a standard. Even so, regulators often respond to general risks with broad requirements or recommendations that do not account for the specific type and function of every device. An example is the FTC's recently published report on the IoT, which proposes a set of helpful—but nonetheless general—steps that businesses can take to enhance and protect consumers' privacy and security.

Dissenting from that approach, then-Commissioner Joshua Wright stated that the FTC's findings on a range of issues related to IoT security were made on the basis of general suspicions rather than on economic and empirical analysis, and that it may have been better to wait to see how some of the issues will actually evolve in the marketplace before acting. Similar points were raised by a number of industry experts at a July 2015 hearing on the IoT before a House Subcommittee with responsibility for matters involving the internet. See U.S. House, Committee on Judiciary, Subcommittee on Courts, Intellectual Property, and the Internet. *The Internet of Things*, Hearing, July 29, 2015 (Serial No. 114-38). As witness Gary Shapiro suggested, imposing overly "prescriptive" requirements that are not based on a proper cost-benefit analysis might unintentionally harm innovation or delay the development of a product that requires a different approach. See Hearing Statement, at p. 23 ("Government should not attempt to regulate based on hypothetical concerns, but should proceed slowly with targeted solutions to actual problems").

These are weighty concerns. If we want to adopt security standards that will promote innovation and consumer protection, Government and Industry need to jointly develop regulations that are tailored to the specific function of a device, the risks it poses from hacking or data loss, and the nature of the device's data collection (including who gets to see it). See, e.g., the President's National Security Telecommunications Advisory Committee, *Report to the President on the Internet of Things* (November 2014), p. ES-4 (recommending standing Government and industry body to develop and maintain cybersecurity guidelines). A similar method is used by the National Security Agency (NSA), which works cooperatively with the National Institutes of Standards and Technology (NIST) to develop "protection profiles" for certain types of mobile phones and other communication tools.

The key point here is that security must be incorporated into the design and function of IoT devices—and that standards should be developed with industry involvement and on the basis of empirical evidence and a rigorous cost benefit analysis. Doing this kind of

work at the front end will help maintain industry innovation and promote a solid economic and technical rationale for each standard. And that will help promote more development.

2. Privacy

The second issue presented by IoT devices is privacy—a concept that bears on a consumer's relationship with industry and on industry's relationship with Government. The focus here is consumer privacy as it pertains to industry's collection of data through the IoT. Government access to this data will be considered more fully below.

The IoT's operating principle is connectivity. Although connectivity promises good things, it also creates a market for data brokerage and data distribution. Why is this? Connected devices produce massive amounts of data, which is then collected by the manufacturer or some other third party. The data may take many forms, but it often contains very useful or interesting information about the consumer or user. When that fact is realized, the collector is then in a position to monetize the data by selling it or sharing it. Sensor data is leveraged for business purposes and profit.

Data collection can be a legitimate commercial goal—and companies use it for a wide range of business purposes. But the problem is that consumers may not fully understand that a device manufacturer (or third party company) is collecting and potentially selling personal information that is sensed or tracked on his IoT device. If he discovers that fact down the line, he may feel misled and conclude that his privacy has been invaded. That perception may lead to a lawsuit or a government investigation.

Companies that produce IoT devices must tell consumers what they do—and how they will collect and distribute or sell their data.[3] When that is done effectively and the consumer approves the terms and conditions, the manufacturer may in most cases maintain and disseminate the information, subject to applicable federal and state statutes.[4] But if a manufacturer hides these facts and fails to secure consumer agreement to the terms, the consumer might sue the company for violation of his privacy. In addition, the FTC could find that the inducement to the sale was unfair and contrary to fairness. Such a conclusion might lead to major investigation or a costly enforcement action similar to the case pursued against TRENDnet.

---

[3] See Jesse Brody and Donna Wilson, *The Next Big Thing: Enforcing Terms of Service in an Internet of Things World*, 20 ECLR 379 (3/11/2015) (discussing the need for enforceable agreements with customers addressing all relevant issues, including privacy and data collection).

[4] See generally, Scott Peppet, *Regulating the Internet of Things: First Steps to Managing Discrimination, Privacy, Security, and Consent*, 93 Texas. L. Rev. 85, 139 (arguing that consumer consent notices for IoT often confuse "notice and choice" and that consumer protection law is largely unprepared for the IoT).

3. Government Access

The third key issue in the evolving IoT is government access to data collected by IoT devices—and to what extent, if any, an agency must obtain a warrant or judicial order in order to see that information.

As a preliminary matter, companies need to recognize that Government agencies will have legitimate—if not compelling—needs for this information from time to time. A consumer that uses devices connected to the IOT may commit crimes. He may be a terrorist. Where agencies have sufficient cause to believe these things, they will use appropriate methods to acquire the information from the company, including an application for a court order authorizing access to the data under a statute such as the Stored Communication Act (18 U.S.C. §§ 2701 et seq.).

But doesn't the Fourth Amendment prohibit this sort of thing? Probably not. The Supreme Court has determined that a person may have a "reasonable expectation of privacy" protected by the Fourth Amendment when he has both a subjective expectation of privacy and that expectation is one that society recognizes as reasonable. See *United States v. Katz*, 389 U.S. 361 (1967) (Harland, J. concurring). Under that standard, a computer user may have a legitimate expectation of privacy in the content of email communications. *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004). But where a person chooses to transmit that information to a third party, a person's "reasonable" expectation of privacy may come to an end. *Smith v. Maryland*, 442 U.S. 735 (1979).

That may be the case here. Most consumer IoT devices transmit personal information as part of the product's normal operating function. With some exceptions, the data transmission takes place through wireless transmissions and or internet networks and not by means of encrypted communications. In that scenario, the consumer's decision to transmit that information to the manufacturer could expose the information to third parties and thus trigger the loss of his Fourth Amendment protections. See *Reporters Comm. for Freedom of Press vs. Am. Tel. & Tel. Co.*, 593 F.2d 1030, 1043 (D.C. Cir. 1978) ("[t]o the extent an individual exposes his activities to third parties, he surrenders Fourth Amendment protections"). When that occurs, the Government doesn't need a warrant to look at the information and use it for an investigation or prosecution.

There are a number of commentators and courts that disagree with the "third party" doctrine and the way that it applies in today's hyper-connected world. In fact, Supreme Court Justice Sonya Sotomayor recently questioned its viability in U.S. v. Jones, 132 S. Ct 935 (2012)—suggesting that the rule "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." But until the doctrine is rejected by a majority of the Court, the Government will continue to have broad authority to access personal information collected

by IoT devices for law enforcement or intelligence purposes. Companies should be prepared to work with agencies for this purpose and address consumer expectations and consent in their product terms and conditions.

4. Product Liability

The rapid emergence of the IoT presents one final issue: manufacturer liability for product defects, negligent data loss, and other related claims for damages.

IoT devices are like any other products sold on the market. They are designed for a certain type of use and consumers should be able to enjoy that function for a set period of time. That's where normal product liability and warranty principles apply.

But IoT devices are also unique. Unlike other products, most of these devices are connected to a massive worldwide network and regularly collect potentially sensitive or personal information. In that respect, the risks of use may not be as apparent to a consumer as the danger of a lawnmower' spinning blade, but an IoT device could cause damage in other drastic ways, including loss of data, loss of privacy, and identity theft. In addition, an IoT device could malfunction and produce unintended damages to another device or to the consumer's physical wellbeing.

All of this means that device manufacturers need to think carefully about how they market their products, frame their warranties, and craft liability provisions that are included in consumer use agreements. It also means that they need to think carefully about supply chain issues and whether subcontracted components meet all appropriate standards. See William B. Bierce, *Managing Liability from the Internet of Things*, National Law Journal (October 5, 2015) (smart devices leave parties in the supply chain vulnerable to lawsuits).

What Next?

The IoT promises to be a leap ahead technology, but the market may be slow to take off without more regulatory certainty in the key areas of security, privacy, government access, and product liability. Some business leaders and policymakers may be tempted to believe that these issues will be sorted out over time, and that the best course is to patiently wait for the issuance of standards and rules *before* moving forward with production or deployment. That kind of caution might seem safe, but it probably won't lay a foundation that will protect consumers while simultaneously promoting innovation, investment, and market growth.

The U.S. Senate was correct in its resolution that "the United States should recognize the importance [of] consensus-based best practices and communication among stakeholders, with the understanding that businesses play an important role in the future development of

the Internet of Things." In line with that direction, Government and Industry need to work cooperatively and *jointly shape* regulatory standards and requirements that address a wide range of issues, including data collection rules, terms and conditions, supply chain integrity, and government access policies.

Industry associations are already taking steps in this direction, including the Online Trust Alliance (OTA), which in August 2015 issued an IoT Trust Framework for public comment, followed by the publication of a Revised Framework in October 2015. Other industry groups and stakeholders are pursuing similar efforts. But more Government-Industry interaction is necessary if we have any hope of building rules that are based on sector-specific requirements, empirical evidence, risk-management principles, and the limitations of product engineering. Taking proactive steps now will go a long way to accelerate the development of the IoT and ensure its continued viability for decades to come.

David M. Verhey | Partner | 202-731-1697
dverhey@dbllawyers.com

David Verhey is a partner in the Government and National Security practice at Dunlap, Bennett & Ludwig, PLLC, an AV-rated law firm in Washington, D.C. and Tyson's Corner, VA. His practice concentrates on counseling and representation of clients with business interests in national security, information technology, cybersecurity, and government contracts. David is a frequent conference speaker and an author of articles on security and technology, including big data, the internet of things, insider threat mitigation, and privacy policy. He is also the founder and principal of SDS Advisors LLC, a technology consulting firm. He is cleared TS/SCI.