Bloomberg BNA

Privacy and Security
Law Report®

Internet of Things

The increasing integration of connected devices into our lives promises enormous benefits for U.S. consumers and businesses. Policymakers should modulate their approaches to reflect the distinct features of the Internet of things, and affected companies should monitor policy developments as they develop privacy and security policies for the connected devices they produce or operate, the authors write.

The Internet of Things: Questions for Policymakers and Implications for Businesses

By Kendall Burman & Stephen Lilley

The increasing integration of connected devices into our lives—what is commonly referred to as the ''Internet of things'' or ''IoT''—promises enormous benefits for U.S. consumers and businesses. Some estimates predict that over 50 billion physical devices will have embedded network connectivity by 2020, with associated economic value reaching into the trillions of dollars annually. And broader social benefits are widely expected, whether in the form of more efficient electrical service, safer cars or smarter cities. Consumers have welcomed these innovations: products as diverse as personal health trackers and connected home security systems have already proven enormously popular. Regulators also have recognized their value: the Food and Drug Administration (FDA) approved a pacemaker able to transmit data wirelessly as early as 2001, for example, and the Secretary of Transportation hailed vehicle-to-vehicle communications in 2014 as ''the next great advance in saving lives.''

Kendall Burman is a cybersecurity & data privacy counsel at Mayer Brown LLP in Washington. Prior to joining Mayer Brown she served in the administration of President Barack Obama, most recently as a deputy general counsel for the U.S. Department of Commerce.

Stephen Lilley is a senior associate in the cybersecurity & data privacy practice at Mayer Brown LLP in Washington. Prior to joining Mayer Brown he served as Chief Counsel to the Subcommittee on Crime and Terrorism, U.S. Senate Judiciary Committee, where he focused on cybersecurity and data privacy issues.

The increased connectivity of our devices and the resulting data flows raise a variety of implementation questions, particularly around privacy and security, as well as spectrum. Congressional and regulatory policymakers have taken note. Businesses should expect an increase in government attention to IoT in the coming years and should factor the policy landscape into their development decisions. To that end, here we describe essential federal policymakers' actions to date, as well as five aspects of the Internet of things—device and data volume, data content, communications with end-users, accessibility of devices post-market, and the nexus between digital and physical worlds—that are likely to inform future policymaking.

IoT Growth and the Policy Response to Date

While most of the attention around IoT has been focused on consumer devices, much of the economic potential from IoT derives from commercial and public-sector uses such as data-driven management of factory operations, or ''smarter'' cities that deliver resources in the most cost-effective way. We are entering a world in which everything from real-time inventory tracking to intelligent street lighting is connected, and the possible efficiencies are vast.

The industry evolving around IoT thus is wide-ranging, and includes companies that, up to this point, haven't focused on technology or spectrum issues. Traditional manufacturers suddenly are finding themselves disproportionately focused on software development, and technology companies are branching out with new products, not just new code.

What these businesses have in common is a need for connectivity. Most IoT devices and systems operate in unlicensed radio frequencies that deliver Wi-Fi Internet connections. But concern is growing that those unlicensed bands are unduly crammed, resulting in network congestion.

Congressional policymakers have recognized the importance of this spectrum question, while focusing broadly on the innovative potential of these products. They also have recognized the important security, privacy and safety questions these products raise. This interest has taken the form of incremental steps—such as hearings on IoT topics in the relevant committees and the introduction of targeted, sector-specific legislation. One common theme has been the recognition of the need for a careful approach that takes advantage of collaboration among stakeholders. For example, the Senate passed a resolution on March 24, 2015 calling for a national strategy for the development of IoT . This resolution recognized the wide range of policies and laws that govern the various technologies that constitute the IoT, as well as the importance of ''consensus-based best practices and communication among stakeholders.''

We are entering a world in which everything from real-time inventory tracking to intelligent street lighting is connected, and the possible efficiencies are vast.

Taking the Senate resolution a step further, Sens. Deb Fischer (R-Neb.); Kelly Ayotte (R-N.H.); Cory Booker (D-N.J.); and Brian Schatz (D-Hawaii.) recently introduced the Developing Innovation and Growing the Internet of Things Act (DIGIT Act). This bill would require the Secretary of Commerce to convene a working group of representatives from the Department of Transportation, the Federal Communications Commission, the Federal Trade Commission (FTC), the National Science Foundation, the Department of Commerce, the Office of Science and Technology Policy and other agencies. This group would be tasked with wrestling with critical questions related to IoT devices, such as spectrum availability, consumer safety and privacy and cybersecurity. The group would consult with a variety of industry stakeholders, as well as consumer groups, to inform their recommendations to congress.

A number of regulators also have acted. The FTC alleged in a 2013 enforcement action that vulnerabilities in home security monitors had led to the compromise of consumers' privacy. More generally, it called in a 2015 staff report for companies to embrace security by design while also calling on companies to lead the way in establishing security and privacy practices. For example, the report urged companies to assess security risks and test device security before launch, to impose reasonable limits on data collection and retention, and to support consumer choice through appropriate notices. The FDA has issued guidance for manufacturers of medical devices, both with respect to pre-market approval and post-market management. And the National Highway Transportation Safety Administration has overseen a cybersecurity-related recall and joined with the Federal Bureau of Investigation in issuing a public service announcement to consumers on the possibility of hacks upon connected cars.

To date, regulators haven't suggested that products should be less smart or less connected. Indeed, many regulators actively embrace the benefits of connected devices—for example, with respect to the safety and environmental benefits of communications among cars or with infrastructure. The regulatory response consequently appears likely to reflect the competing interests and benefits at stake for users. And, given the congressional calls for collaboration and consensus, it appears that regulators will be encouraged to work together to avoid unnecessary and unproductive conflict among approaches on the state, national, and global levels.

Key Factors For Policymaking in the Internet of Things

Policymakers of course should proceed in a thoughtful manner, but that begs the question of what factors they should consider as they approach IoT. To some extent, IoT supports the application of existing risk-based approaches to security and familiar privacy frameworks. But there are crucial differences. A desktop that stores data on a local hard drive presents different security and privacy questions than a retinal scanner at a worksite. In fact, the wide range of IoT devices presents an array of privacy and security questions that defy easy categorization. However, generally speaking, businesses can expect five aspects of IoT to inform policymakers as they think through its implications for security and privacy in the upcoming years:

- device and data volume;
- data content;
- communications with end-users:
- accessibility of devices post-market; and
- nexus between digital and physical worlds.

Device and Data Volume

The volume of data created by the Internet of things raises novel privacy questions. To give an analogy, in *United States v. Jones*,[1] Justice Samuel Alito's concurrence (joined by three other Justices) noted the difference between a single, public observation of an indi-

[1] 132 S. Ct. 945 (2012).

vidual's physical location and sustained monitoring over a four-week period. While each individual data point could be readily gathered, advances in technology had dramatically increased the scale and ease of the data collection, raising new privacy concerns under Justice Alito's analysis. Likewise, consumer expectations of privacy may change as data scales with IoT, particularly as data flows are combined and users leave an increasingly rich trail of ''data exhaust.'' Moreover, users of many different devices may not understand how the various privacy policies apply to the resulting data.

The sheer volume of connected devices also raises cybersecurity risks. The huge number of connected devices presents a correspondingly large attack surface to prospective hackers as well as an ever-larger number of access points to existing networks. Monitoring that increased number of devices, assessing the vulnerabilities of an increased number of supply chains, and attempting to audit policy compliance may present challenges as IoT grows.

Data Content

The Internet of things also promises to capture new forms of data (or to routinely capture data that previously was collected in only limited circumstances). A personal monitoring device, for example, may measure an individual consumer's breathing rate (and, derivatively, stress level). Smart locks at a construction site may gather fingerprints or other biometric data. Geolocation data gathered by a car may reveal substantial information, including whether the user frequents certain businesses, hospitals or places of worship. While an individual piece of data gathered about an individual through an IoT device may not be significant (particularly if it never leaves the device or if data minimization techniques are used), the aggregation of individual data streams may increase data sensitivity. And even anonymized data can, in some cases, be tied back to an individual through aggregation with other data. This raises privacy issues that may not have been apparent to a single entity responsible for one particular dataset.

The wide range of Internet of things devices presents an array of privacy and security questions that defy easy categorization.

The nature of this data also creates new risks for data holders. The compromise of a trove of personal data may cause significant reputational harm to a company, for example, or lead to litigation. Shifting user expectations around new devices also may produce significant uncertainty as businesses assess, prioritize and respond to security risks.

Communication With End-Users

Connected devices also can pose unique challenges for communicating with consumers. A substantial and increasing number of IoT devices don't have any consumer interface through which privacy policies and security fixes can be communicated. A consumer won't use an IoT-enabled kitchen appliance in the same way as a smart phone. The privacy policies that a consumer may (or may not) read that come with smart phone apps may not be displayable on a smart toaster. Regulators have sanctioned the notice and consent model as the legal foundation for privacy across numerous industries. But that approach may not translate if ''notice'' is simply not noticeable, raising the question whether industry-generated best practices or another approach provides a better solution. (Thisisn't a universal challenge. Some ''things'' have large touch screens through which privacy policies can be communicated; others are accompanied by owner's manuals that customers typically review; and still others must be connected to a computer for initial setup.)

Accessibility of Devices Post-Market

Connected ''things'' also are more likely than phones or laptops to be inaccessible to manufacturers after they have been sold or otherwise put into operation. Technical and legal impediments may prevent a manufacturer from addressing identified vulnerabilities. To use a light-hearted example, imagine that a security researcher demonstrated the ability to hack into a smart coffee-maker and to siphon off coffee-consumption data. The solution might be as simple as changing a single line of code, but there may be numerous impediments to addressing the vulnerability. The manufacturer may not have an ongoing relationship with the customer and thus may not be able to solicit and receive his or her consent to patch the device. Moreover, even if it could secure consent, the manufacturer might be unable to deliver an over-the-air update or to enable the consumer to otherwise patch the device. And would a coffee-maker be subject to recall simply because it allowed disclosure of coffee-drinking habits?

This light-hearted example illustrates a serious point about connected devices: Patching these devices may prove challenging. And while much of standard cybersecurity frameworks may apply in some respects, the relative inaccessibility of many connected ''things'' is likely to fundamentally reshape how businesses respond to vulnerabilities and threats. Indeed, challenges in the response function will put more pressure upon the security designed into the product. In turn, information sharing—and engagement with security researchers—may have more value in the design process than after connected devices have been put into the field.

While the attacks on connected ''things'' themselves aren't fundamentally different from more familiar hacking, their unique consequences set them apart.

Nexus Between Digital and Physical Worlds

The possibility of real-world harm presented by attacks on connected ''things'' has dominated the headlines. While the attacks themselves aren't fundamentally different from more familiar hacking, their unique consequences set them apart. A ransomware attack that turns a phone into an expensive paperweight may not be different in kind from an attack that shuts down a smart sprinkler system that protects a house from fire, but the latter attack understandably raises more concern. Such attacks that reach into the physical world bring risk-based security approaches into tension with safety-oriented regulatory regimes that have little tolerance for risk. Developers, industry stakeholders and regulators will need to navigate this dynamic carefully in the coming years. If it's true that every system is hackable, then a vast array of ''things'' must pose at least some miniscule risk of an unintended consequence or danger in the physical world. But it also cannot be the case that such a miniscule risk justifies taking every connected product off the market.

Conclusion

If innovative companies have sought to change our lives with disruptive technologies, policymakers to date have sought not to disrupt the growth in the innovative IoT. As congress and regulatory agencies grapple with the policy issues that IoT raises, they should take care not to force ill-fitting existing regulatory regimes on new technologies. Rather, they should modulate their approaches to reflect the distinct features of IoT. Affected companies in turn should monitor policy developments carefully and keep them in mind as they develop privacy and security policies for the connected devices they produce or operate. Anticipating how changing policies will apply to emerging technologies and responding strategically and proactively is sure to benefit companies as the landscape continues to evolve in the coming years.