New York Law Journal
A NEW YORK LAW JOURNAL SPECIAL SECTION
An ALM Publication
Regulatory Reform
WWW.NYLJ.COM
MONDAY, DECEMBER 16, 2013

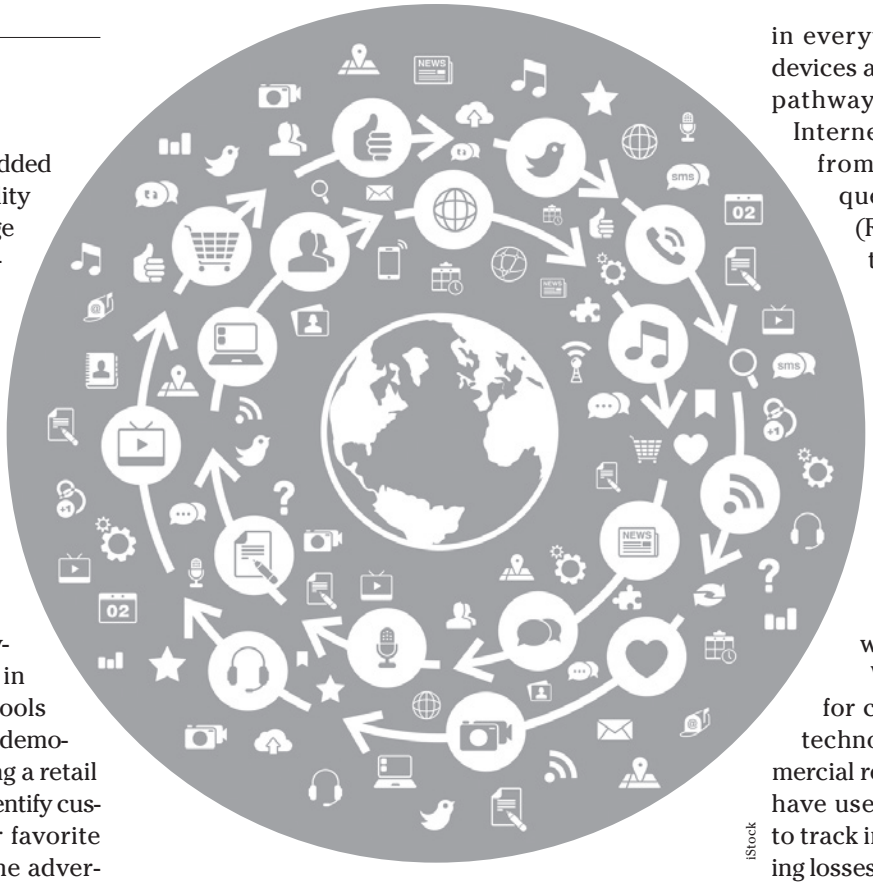
Regulating **Interconnectivity** On the **'Internet of Things'**

New technologies bring privacy, security risks.

BY KELLY T. CURRIE AND CHERYL A. FALVEY

Consumer products, embedded with sensors and the ability to communicate, challenge traditional methods of managing the risks to privacy and security presented by these innovative offerings.[1] Yet the rewards of capitalizing on these networks to create new marketing avenues and business models may give retailers the competitive edge they need to survive.

Technology now exists to enable consumers to purchase the products they see in a movie on their wireless devices in real-time. Facial recognition tools in mannequins can profile the demographics of customers entering a retail store and smart phones can identify customers as they walk by their favorite items and send them real-time advertisements and discount coupons. At the heart of the policy debate, and the regulatory activity surrounding this new technology, is whether a consumer can remain anonymous or opt out as various devices communicate and sometimes store consumer preference and location data. To succeed in this new world, consumer businesses will need to navigate turbulent and uncertain waters in consumer privacy and technology security.



iStock

Commonly referred to as the "Internet of things," sensors and actuators embedded in everything from tires to medical devices allow data to flow on the same pathways that connect data on the Internet. This connectivity comes from wireless use of radio-frequency electromagnetic fields (RFID) and other sound waves transmitted and received from chips embedded in different devices. These chips potentially expose both the identity and the location of the consumers who use these products. Consumers often have no idea that the products they buy contain these transmitters or that their identity and location can be accessed without their knowledge.

With adequate safeguards for consumer privacy, these new technologies offer significant commercial rewards for business. Retailers have used RFID technology for years to track inventory and reduce shoplifting losses. Newer applications can drive sales, target marketing based on consumer preference, and prevent counterfeits. Aggregating this data can also provide social benefits. Energy conservation trends might be observed by combining energy usage statistics with building operational information. Agricultural production might be increased by studying the data from sensors on farm equipment in combination with information

KELLY T. CURRIE *is a partner at Crowell & Moring in New York.* CHERYL A. FALVEY *is a partner in the firm's Washington, D.C. office and former general counsel of the U.S. Consumer Protection Safety Commission.*

on weather and crop conditions. Scientific research may benefit from combining electronic medical records with lifestyle choices reflected in data on grocery store purchases and physical activity monitors.[2] These innovative uses depend on the ability to combine data sources that contain personally identifiable information in a safe and secure manner without risk to personal privacy.

Watching, Not Waiting

Federal regulators are keeping a close watch on these developments. On Nov. 19, 2013, the Federal Trade Commission held a public workshop on the Internet of Things to learn more about the technology breakthroughs in this area and explore the consumer privacy and security issues associated with these networks of data. The FTC's workshop notice acknowledged the penetration these technologies have already made in consumer activities:

> Consumers already are able to use their mobile phones to open their car doors, turn off their home lights, adjust their thermostats, and have their vital signs, such as blood pressure, EKG, and blood sugar levels, remotely monitored by their physicians.[3]

Many of the technologies employed in consumer products today do not involve any interface with the consumer, and consequently, provide no opportunity for traditional methods of notice and choice that a consumer ordinarily uses to control access to sensitive data. Consumers may have no idea what data a device collects and how such information might be used. Yet consumers enjoy the convenience these technologies provide and the industry appears poised to respond to continued consumer demand. Indeed, Intel recently formed its Internet of Things Solutions Group combining its embedded chips division with the group responsible for building the systems needed to allow those chips to communicate with smart phones and tablets.[4]

Speaking to an audience at the Brand Activation Association Marketing Law Conference the day after the FTC's workshop, FTC Commissioner Julie Brill indicated that the FTC has "no plan to do regulations in this area." She stated that the goal is to enter the policy debate early, as market penetration is just beginning, and encourage best practices from the start. In pointing to the need for businesses to act without waiting for regulation, Brill referenced the story of a hacker able to take control of the speed of an automobile performing on a test track. The driver lost the ability to operate the gas pedal or brake as the hacker brought the vehicle up to a speed of over 140 miles per hour. Brill argued that manufacturers must partner their product engineers with privacy and security experts and employ best practices to prevent the damage consumers may face without robust protections.

Commonly referred to as the **"Internet of things,"** sensors and actuators embedded in everything from tires to medical devices allow data to flow on the same pathways that connect data on the Internet.

What might those best practices be? The FTC has already engaged in one enforcement action, which provides some clues. The Commission's case against TRENDnet alleged that certain video baby monitors were vulnerable to cyber-hacking over the Internet and therefore did not sufficiently protect consumer privacy. The FTC wrote: "TRENDnet failed to use reasonable security to design and test its software, including a setting for the cameras' password requirement."[5] In its consent decree ordering TRENDnet to address security risks that could result in unauthorized access to its products, the FTC requires, among other things:

- designation of an employee or employees accountable for security practices and administering a written security program;
- assessment and continued auditing of risks in hardware and software design as well as vulnerabilities caused by employees or human error;
- engagement of service providers capable of maintaining the security of the devices in operation;
- testing and monitoring of potential failure modes including necessary adjustments to account for material changes in business operations going forward;
- retention of all relevant records for five years including all advertisements and promotional materials and packaging.[6]

The agreement further obligates the company to initial and biennial assessments of its security measures by independent, third-party professionals qualified as "Certified Secure Software Lifecycle Professionals." The agreement reflects the FTC's expectations that companies build security and privacy tools into their products and test that they work using third parties to provide a measure of independence that ensures objectivity. While the FTC may not have the authority to mandate product testing for security vulnerabilities, their enforcement actions require costly initial and continued testing to a constantly evolving standard of care.

The FTC is not the only federal agency following the development of these new technologies. The Food and Drug Administration (FDA) works with manufacturers of medical devices to ensure that adequate testing exists for adverse effects and interference in transmissions by embedded chips.[7] FDA also uses the technology to identify and quarantine counterfeit drugs and track legitimate, approved medications throughout the supply chain, which should ensure their safety from the point of manufacture to the point of dispensing.[8] The Environmental Protection Agency (EPA) has recognized the value the technology can bring to the tracking and management of hazardous waste transport.[9] The Consumer Product Safety Commission (CPSC) has also explored the use of tracking technology to ensure product safety and increase recall effectiveness when it withdraws defective products from the market. Indeed, consumers are calling for its use. Concerned Mothers, a coalition of young mothers "that share a public interest in protecting children from hazardous products," asked the CPSC to use RFID technology to identify all retailers of a recalled products and modernize the recall process by "holding the manufacturing industry" to "progressive standards."[10]

State AG Activity on the Rise

The state attorneys general regulate by use of their enforcement powers to protect consumer privacy interests. Terms of injunctive relief in these cases set the standard of care. New York participated in a multistate settlement with Google, announced

Nov. 18, 2013, over unauthorized tracking of consumer Internet behavior. The agreement prohibits the use of codes to override privacy settings without consumer consent unless necessary to prevent fraud or for other security reasons.[11]

Recently, the state AGs have turned their attention to mobile devices as a potential vulnerability for consumers when lost or compromised by hacking. New York Attorney General Eric T. Schneiderman, as part of the Secure Our Smartphones Initiative coalition of state Attorneys General, District Attorneys and other law enforcement officials, took an aggressive stance to require greater theft deterrent software when Apple launched its latest operating system, iSO7.[12] Aimed primarily at the risk of iPhone theft, the Initiative is equally concerned that phone thefts do not compromise consumer data stored on the phone. Drawing battle lines in the debate over the use of kill switches to deactive phones when lost or stolen, Schneiderman said, "Manufacturers and carriers need to put public safety before corporate profits and stop this violent epidemic, which has put millions of smartphone users at risk. While we are encouraged by the new, anti-theft security features presented by some smartphone makers, the seriousness of this issue demands a more robust response."[13]

The state AGs have been equally aggressive in protecting children from mobile devices collecting personal information including geolocation information allowing the device to triangulate the exact location of the child. The state of New Jersey brought an action to enjoin violations of the Children's Online Privacy Protection Act of 1998 (COPPA) against Dokogeo, a company that provides its Dokobots scavenger hunt downloadable app for mobile devices rated for four and up and featuring animated cartoon characters. In addition to enforcing the requirements for notification and verifiable parental consent, the agreement also requires the app developer to "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."[14] Companies must follow these developments to know the standard of care expected as they develop new offerings.

Policy Questions Abound

At the FTC's November 19th workshop, Vincent Cerf, Google Vice President and Chief Internet Evangelist, cautioned regulators to use restraint and avoid regulating without understanding the technology and its risks. There are reasons regulators ought to slow down. Regulators need a strong understanding of the technology before entering the regulatory fray. Agencies can face difficulty enforcing the regulations they write if they finalize those regulations before defining robust test methods that can be replicated in multiple laboratories using round robin testing. The FDA has been leading by example with its work with the Association for Automatic Identification and Mobility to develop methods to test medical devices for their vulnerability to electromagnetic interference from RFID systems.[15]

Some question whether a delay in regulating will lead to the use of data in ways that unreasonably expose consumers to privacy risks. Moreover, legislatures and regulators must answer the major policy question of who owns the data collected by these devices. The purchase of a product containing a chip would seemingly pass the title to the product and all of its components to the consumer. However, the data transmitted by the product may be collected and stored elsewhere. Who owns that data? Can ownership of the data collected be retained by the product manufacturer by agreement or otherwise? Will consumers be willing to forfeit that data and their privacy for the convenience offered by these new devices or for a lower price?

Regulators face additional challenges as well. Just like consumers, agencies may not know when these technologies are being used and where. Security programs that work when a product is tested in isolation may become vulnerable or not work at all when that same product is combined into a network. Given the broad array of applications and products, there is no one-size-fits-all approach. Notice and choice, the stalwarts of consumer privacy protection, may not be feasible when the consumer does not interface directly with the embedded technology. The cost of compliance to industry norms and agency expectations may be crippling to small businesses or hinder innovation. Whether privacy is or is not an anomaly in our technology- dependent world will remain a regulatory focus in the coming year.

1. Special thanks are due to our colleague, Dina Epstein, who attended the FTC's workshop on the Internet of things and provided key contributions for this article.

2. *In the Matter of the Privacy and Security Implications of the Internet of Things*, Comments of CTIA—The Wireless Association, June 1, 2013, at 9-11.

3. FTC, "FTC Seeks Input on Privacy and Security Implications of the Internet of Things," April 17, 2013, available at http://www.ftc.gov/opa/2013/04/internetthings.shtm.

4. Mohana Ravindranath, "Intel forms 'Internet of things' division," Washington Post, Monday, Nov. 18, 2013.

5. FTC, "Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy," Sept. 4, 2013, available at http://ftc.gov/opa/2013/09/trendnet.shtm.

6. *In the Matter of TRENDnet*, FTC File No. 1223090, available at http://www.ftc.gov/os/caselist/1223090/130903trendnetorder.pdf.

7. FDA, "Radio Emitting Frequencies," available at http://www.fda.gov/radiation-emittingproducts/radiationsafety/electromagneticcompatibilityemc/ucm116647.htm.

8. FDA, "RFID: Ensuring the Supply Chain," available at http://www.fda.gov/drugs/drugsafety/ucm169918.htm.

9. See, e.g., Sheldon, Kopsick and Pantaleo, et al., "Tracking Radioactive Sources in Commerce," 2005, available at http://www.epa.gov/radiation/docs/source-management/rad-i-ncommerce-0305.pdf.

10. Comments of Concerned Mothers on the Mandatory Recall Notice of Proposed Rule, dated April 19, 2009, found at http://www.cpsc.gov/PageFiles/127403/manrecall2.pdf.

11. N.Y. State Attorney General's Office, "A.G. Schneiderman Announces $17 Million Multistate Settlement With Google Over Tracking of Consumers," Nov. 18, 2013, available at http://www.ag.ny.gov/press-release/ag-schneiderman-announces-17-million-multistate-settlement-google-over-tracking.

12. N.Y. State Attorney General's Office, "Secure Our Smartphones Coalition Statement on Release of Apple's iOS 7," Sept. 18, 2013, available at http://www.ag.ny.gov/press-release/secure-our-smartphones-coalition-statement-release-apples-ios-7.

13. http://www.ag.ny.gov/press-release/ag-schneiderman-ag-biden-lead-31-attorneys-general-urging-smartphone-industry-protect.

14. *In the Matter of Dokogeo*, Consent Order dated Nov. 13, 2013, available at http://nj.gov/oag/newsreleases13/Dokogeo-Inc_&_Dokobots.pdf.

15. FDA, Radio Emitting Frequencies, available at http://www.fda.gov/radiation-emittingproducts/radiationsafety/electromagneticcompatibilityemc/ucm116647.htm.