ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Getting Up to Speed on the Internet of Things

Technology, Privacy, and eCommerce

CHEAT SHEET

- ***A new term for an old idea.*** First conceptualized in the 1970s, the Internet of Things (IoT) describes everyday devices embedded with sensors and capable of communicating with you and each other.
- ***A regulatory gulf.*** There are currently no standards or communication protocols governing how IoT devices from different manufacturers would interact, although these have begun to be formalized.
- ***A laissez-faire approach.*** Currently, most regulators have adopted a hands-off attitude to IoT devices, but privacy and security concerns are paramount.
- ***Get a head start.*** Our checklist details crucial legal steps for counsel whose companies are expanding into IoT.

If, two years ago, the term *Internet of Things* was a part of your lexicon as an in-house lawyer, you were ahead of the game. Today, general news and industry publications report daily on some aspect of the Internet of Things (IoT). Predictions are that the IoT market will explode, with 25 billion devices to be connected to the Internet by the end of 2015 and 50 billion by 2020. Because an IoT market is virtually certain to emerge, in-house lawyers may find themselves confronting new territory. Privacy and security issues will dominate, but they are not the only legal risks to consider. Analysis of the legal risks for an IoT device depend on device functionality, the type of data collected, and the territory where the device will be sold. While there is no one-size-fits-all checklist of legal issues for the IoT, this article serves as a primer to understand the IoT ecosystem.

History

The IoT includes varied domains such as manufacturing (the “industrial Internet”), transportation, energy, healthcare, consumer products (like wearables) and the smart home. The IoT is not new. In the 1970s, Vint Cerf, Google’s chief Internet evangelist (his actual title), was experimenting with mobile radio and “packetized voice.” Scientist Kevin Ashton is believed to have first used the term “Internet of Things” in a 1999 presentation. But many terms are used to describe this ubiquitous ecosystem of sensors and connected devices. For example, the National Institute of Science and Technology (NIST) uses the term *Cyber Physical Systems*, defined as “a system of systems” which are “smart systems that include co-engineered interacting networks of physical and computational components.” For non-scientists, IoT devices are everyday objects (other than typical computers) embedded with sensors and computing power capable of communicating with each other; IoT devices are “always on, always sensing, always collecting, and always communicating.”

Why now?

The IoT is the result of the convergence of key Internet technologies including IPv65, “big data” analytics, proliferating smartphones, increased bandwidth, cloud computing, lower cost and smaller sized wireless radios, and improved battery technology. For many IoT consumer devices, apps installed on smartphones will interface with the consumer and may provide the platform from which the device is controlled. In the IoT, everyday “things” with embedded sensors communicate with

other sensored things through wireless technology, and ultimately send the data to a server. The data on that server may be accessed by a consumer through another device, such as a smartphone or tablet or, a PC. This creates what can be viewed as a data collection ecosystem that raises privacy and security concerns.

Challenges to adoption

The predicted expansion of the IoT will happen only after confronting significant challenges. Exciting and innovative developments include in-utero baby monitors, contact lens glucometers, smart clothes smart TVs and, of course, connected cars and refrigerators. Some devices are sure to be over-hyped and unsustainable: At the 2015 SXSW Festival, one industry member reportedly joked that his company developed a smart egg tray that needed new batteries more often than most people needed eggs.

The IoT depends on data transfer and interoperability of devices, but there is uncertainty on how IoT devices will communicate with each other. There are currently no open technical standards or open communication protocols. That could mean the predicted growth will be stymied because products from one manufacturer may not be able to communicate with products from another.

To confront the connectivity problem, industry consortia have been formed with members such as Cisco, GE Software and Intel, among many others, to work together to define communications frameworks so that wireless devices can connect and exchange information regardless of operating system or service provider. Consortia with differing, but related foci include the Open Internet Consortium (OIC), the Industrial Internet Consortium and EEEbus (primarily in the EU). The OIC sponsors the IoTivity Project, an open source software framework enabling connectivity. Industrial Internet Consortium works at defining architecture and platforms for the industrial Internet. And EEEbus focuses on interconnectivity solutions for smart home projects. As issues evolve, ne2w consortia are being formed and other consortia have created partnerships to attempt to set international standards on connectivity, communication frameworks and architecture — all to accelerate the growth of the IoT.

Bandwidth consumption is another issue. Researchers and commentators are concerned that there may not be enough public airwave space for all the billions of predicted IoT devices to communicate with each other. This issue creates business opportunity and at companies are already producing low power WiFi products that could reduce the strain in existing cellular networks.

The regulatory landscape

In-house counsel should be aware that multiple federal and state agencies and regulators may affect IoT development. Regulation of privacy and security concerns originate with the Federal Trade Commission (FTC), the Federal Communications Commission (FCC), the Food and Drug Administration (FDA), the US Department of Health and Human Services, the Department of Transportation, the National Highway Transportation Safety Administration (NHTSA) and the Department of Energy. Highlighted below is an overview, beginning with the most active and influential agency in the area to date, the FTC.

The current policy position appears to be a “wait and see” approach, or “regulatory humility” in light of concerns that innovation in the nascent IoT market could be stymied if regulation is premature. In August 2014, the Article 29 Working Party of the EU released its Opinion 8/2014 on “Recent

Developments on the Internet of Things" (discussed in EU inset). In January 2015, the FTC released the report "The Internet of Things: Privacy and Security in a Connected World" (the "FTC report"). The US Senate Committee on Commerce, Science and Transportation held a hearing on the IoT in February 2015 and the House Subcommittee on Commerce, Manufacturing and Trade hosted a "showcase" and hearing in March 2015, and the House Judiciary Committee held a hearing in July, 2015.

FTC

Emerging are some themes, with privacy and security concerns being the most prominent. The FTC report is a good study of themes discussed worldwide. The FTC report recommends the following as best practices in the IoT:

- **Implement reasonable security** in light of the sensitivity of the data to be collected and device functionality. Security considerations will likely differ for each IoT device brought to market. Implement "security by design," engage in privacy and security risks assessments and test security measures before launch.
- **Personnel practices** should promote good security. Management should take the lead in establishing a culture of security and employees should be trained on good security practices. Be aware that not all IT professionals have an understanding of privacy and security: "Technological expertise does not necessarily equate to security practices."
- **Third party vendors.** Vendors should be vetted for good security practices and contractually required to maintain those good security practices.
- **Device security.** Device security is paramount. Especially when sensitive data is collected (such as health or financial information), marketers should take steps to encrypt the IoT device and should consider the impact of the security (or lack thereof) of the consumer's network.
- **Access control** measures should be implemented so that unauthorized persons cannot access data on the device or collected from the device.
- **Device lifecycle management.** The device should be monitored throughout its lifecycle. Patches for known vulnerabilities should be provided to the user.
- **Data minimization.** This concept is somewhat controversial in the United States (but note that in the EU it is an accepted requirement — see sidebar on EU). FTC Commissioner Olhausen dissented from the FTC report's proposition that data minimization is a necessary best practice. The majority took the position that "data not collected cannot be misused." However, Commissioner Olhausen remarked that data minimization would not allow for the many positive uses of data, if collected and aggregated. The data minimization issue makes clear that privacy and security issues in the IoT cannot be separated from big data issues, which have also been explored by the both FTC and the White House.

TRENDnet

The FTC's September 2013 TrendNet case is the FTC's first true IoT regulatory action. It is a must-know case for any marketer of an IoT product. TRENDnet is a marketer of IP video cameras that allow users to monitor homes and business remotely over the Internet. The design feature that got TRENDnet in trouble was the camera's user interface, which included a setting that allowed users to turn off the requirement that login credentials be entered before the settings could be adjusted to allow feeds to be publicly broadcast over the Internet. The settings also included a flaw that allowed all user's live feeds to be publicly accessible even when they were meant to be private. A hacker

discovered this flaw after visiting TRENDnet's website and identified and obtained customer's IP addresses of TRENDnet IP cameras, and posted live feeds from the cameras online. The posted feeds famously allowed "surveillance of infants sleeping in their cribs, young children playing and adults engaging in typical daily activities." The breach was widely reported; news articles featured photos taken of the compromised feeds and depicted the city and state of many of the hacked IP cameras. TRENDnet learned of the breach from a customer in January 2012 and the FTC investigated.

In the subsequent Consent Order, the FTC outlined steps that TRENDnet had to take to secure its products against similar problems. Marketers of consumer IoT devices should know the facts of the TRENDnet case and consider whether the FTC's security requirements are appropriate for an IoT device.

FDA

Depending on the use and functionality of a device, or of software or a mobile app that interacts with a device, premarket submissions to the FDA may be required. In recent guidance, the FDA announced that it will exercise enforcement *discretion* over mobile apps that are *not* "medical devices" as defined by the Food, Drug and Cosmetic Act. Examples of such exempted apps would be popular wearables like the FitBit, which tracks health information.

"Mobile medical apps," however, are extensions of medical devices, and pose a risk to patient safety if the apps malfunction. An example would be a mobile app that controls the delivery of insulin through an insulin pump. In any event, any device that connects to or directly monitors the human body (an ingestible smart pill, for example), could be considered a medical device that requires pre-market review and approval by the FDA. The security of medical devices is also a concern. In October 2014, the FDA published final guidance and recommendations to consider when making FDA medical device pre-market submissions for effective cybersecurity management. Among other things, the FDA recommended security-by-design in medical devices and highlighted the need for manufacturers to consider risks to patients from device malfunctions.

FCC

One of the most controversial changes to regulating the Internet's privacy and security is the FCC's Open Internet Order, which went into effect on June 12, 2015. If the order survives pending challenges brought by internet services providers (ISPs), the FCC will potentially become co-regulator, with the FTC, of privacy and security in the United States. As this area develops, lawyers who advise IoT device companies may wish to stay aware of developments to maintain awareness of the entire IoT ecosystem, which the ISPs are a part.

US state law

As the US IoT market develops, states may begin to enact laws regarding collection of data from connected things. As of the date of this writing, 14 states have enacted laws regulating the use of information collected through a cars event data recorder (i.e., the car's EDR or "black box"). New Jersey's "connected car law" provides that no person, except the vehicle owner, may "retrieve, obtain, or use data recorded, stored, or transmitted from the recording device" unless the owner provides consent or pursuant to an order by competent authorities, or unless the recorded data is used for improving safety or performance, compliance with laws, or for vehicle repair — provided the

identity of the owner is not disclosed. As part of the proposed California Privacy & Consumer Protection Act, a bill introduced in February 2015 in California, AB 1116, would prevent the sale of "smart televisions" that record conversations when voice-recognition features are not in use.

Self-regulatory frameworks

Self-regulation is a way to potentially avoid regulation that industry stakeholders fear could curb industry growth. The FTC report supports self-regulation as a means to adopt privacy and security practices. The auto industry was the first to publicly commit to self-regulatory best practices in the IoT for connected cars. In November 2014, 19 US automakers made a commitment to comply, starting in 2017, with the "Consumer Privacy Protection Principles for Vehicle Services." This did little to stem legislation. After reports in July 2015 that researchers were able to wirelessly hack a Jeep Cherokee, federal lawmakers introduced the "Your Car (SPY) Act". This bill would direct the NHTSA and the FTC to create federal standards to secure connected cars and protect privacy. A few days after the hack was reported, Fiat Chyrsler announced a voluntary recall of 1.4 million cars.

Litigation risks

Products liability claims

An IoT device manufacturer will face the same litigation risks as any consumer products manufacturer. As car manufacturers find themselves operating in the technology space by offering connected cars, technology companies providing IoT platforms or applications may find themselves facing product liability claims. Legal scholars have written that "[l]iability norms may change because of the level of knowledge and control manufacturers have of their systems; and that [l]iability for developers could expand and the technology company could be considered the "least cost avoider," — the party in the best position to minimize the risk.

Product liability claims may arise from allegations that an IoT device manufacturer failed to sufficiently prevent a hacker from interfering with software in a device, and the "hack" caused physical harm. For example, thieves could hack a smart home, override the system, disable alarms, open smart locks and gain entry to a house. A hacked medical device, like a smart pacemaker, could be disabled and cause death. As noted, connected cars can be hacked and disabled remotely. The Jeep Cherokee used a "zero day" exploit to wirelessly control the Jeep via the Internet. While the car was being operated, the researcher-hackers were able to disable the transmission and the brakes.

It is unclear whether hackability alone, or even actual hacking, would result in liability. Past judgments in data breach cases that involved stolen payment cards show that standing is an obstacle for plaintiffs. It suggests that a pacemaker wearer, even if hacked, may find herself unable to recover funds from a manufacturer, at least until some physical harm occurs. After the US Supreme Court's holding in *Clapper v. Amnesty International USA,* 133S. Ct. 1138 (2013), a number of data breach cases involving payment cards were dismissed for lack of standing because the risk of harm was too attenuated from a hack. Under Clapper, standing does not lie unless harm is "certainly impending" or there is a substantial risk of future harm.

Since Clapper, a case brought by hotel chains against manufacturers of electronic key card door locks was dismissed because the plaintiffs could not show actual harm, even though security defects in the locks could certainly be breached (the hacking method was widely publicized on the internet). In July, 2015, the U.S. Court of Appeals for the 7th Circuit held that the plaintiffs suing after the

Neiman Marcus credit card breach established standing after alleging possible future harm. The Court found that it was reasonable that identity theft or credit card fraud would occur.

Patent claims

Patent litigation cases have commenced in the wearables industry. In February 2014, Adidas sued UnderArmour in a patent case over technologies in UnderArmour's products incorporating MapMyFitness. And in January 2015, Sarvint Technologies filed a patent claim against Athos, Carre and others over intelligent shirt technology. Patent claims are not surprising in the tech industry, but these are notable as they involve wearable technology.

The checklist

Hopefully, this primer provides a baseline reference to legal issues in the IoT industry. What follows is a the following is suggested checklist to help organize an in-house legal department's counsel of the IoT company-client.

- **Assemble a cross-functional team early in product development.** At a minimum, include the company's privacy officer (if there is one!), IT security personnel, software and app developers, hardware designers and engineers, marketing and the legal department. In this way, privacy and security by design principles can be effectively addressed. At this stage, IT personnel and engineers will likely identify potential third-party vendors whose products or services will be incorporated. Make sure the application development function includes those with expertise in software security.
    - *Determine the potential geography for the sale of the IoT product.* If the product will be marketed overseas at any point in its life cycle (even if not initially), it is prudent to determine the applicable regulatory requirements of all jurisdictions in which the device will be sold. Refer to the insert on EU considerations as a starting point. For products that may monitor health data, be sure not to neglect a review of medical device regulations to determine whether those apply.
    - *Determine the full range of privacy and security regulations that apply.* For example, if marketing a wearable, consider what personal data will be collected and whether any of that data triggers FDA, HIPAA or other regulations. Do not ignore research of state law, such as the New Jersey connected car law, on collection of data from devices. Again, if the product will be sold in the European Union, make sure EU laws and regulations are considered.
    - *Review applicable self-regulatory frameworks.* If the company operates in an industry that is not yet directly regulated (such as connected autos), become familiar with the applicable self-regulatory practices and apply them. Consider whether it is necessary for the device to collect any personal information at all. For example, some machine-to-machine IoT functions, such as in shipping, supply chain and cargo monitoring, may not collect any personal information, but are still considered IoT devices. (But keep an eye on the impact of developments in big data algorithms, which may allow for re-identification in ways previously considered impossible).
    - *Review your company's privacy and security practices.* If your company has not previously had to consider the privacy and security of consumer information, an IoT product should not be marketed without reviewing the company's current practices and expanding them with respect to applicable privacy rules. If your general counsel has not already been counseling management on the need to have good privacy and security practices developed or in place, these discussions must begin.

    - *As an in-house lawyer* — continually educate yourself on IoT platforms and keep informed of developments. As the IT and security departments assess platforms and cloud vendors, it would be beneficial for in-house counsel to understand basic concepts about IoT platforms. Current examples include, HealthKit (wearables), Homekit (for smart homes) and IBM's IoT Foundation. Legal and privacy functions will need to be involved in vetting platform providers.
- **Conduct privacy and security risk assessment for products and product functions.** This step is ongoing from the first meetings through product end-of-life. The assessments should consider risks of collection and retention and disposal of personally identifiable information throughout the product lifecycle. Where is information on the device going once the device is obsolete and the consumer wants to discard it?
- **Confirm or adopt an appropriate privacy framework.** A framework establishes a common set of standards or best practices. Privacy by Design, as developed by former information and privacy commissioner of Ontario, Dr. Anne Cavoukian, is a framework developed on seven foundation principles, which has set the stage for privacy by design concepts throughout the world. For consumer devices, consider a framework addressing concerns set forth in the FTC report, and relevant FTC enforcement actions. If the device will collect personal health information or operate as a medical device, HIPAA and FDA regulations may dictate the framework. State laws may have additional requirements. Consider consulting commentary on best practices such as "A Practical Privacy Paradigm for Wearables" (2015) by the Future of Privacy Forum.
- **Focus on security!**
    - Security frameworks may be sector-specific such as for processing protected health information under the HIPAA Security Rule. The FTC requires companies that collect consumer personal data to employ "reasonable" security practices. The company's IT security function will need to understand and classify data that is collected, understand where each point of personal data "sits" in the IoT device ecosystem and understand to where, and how, the data is transmitted. Security must consider the security of IoT device itself, the mobile app that may control the device, user interfaces on the web or on an app for mobile devices, cloud hosting of data, software developed specifically by the marketer of the device and incorporated third party software. Examples of security frameworks for the IoT include the FTC's companion document to the IoT report: "Careful Connections: Building Security in the Internet of Things." The NIST Public Working Group on CyberPhysical Systems has issued a draft framework expected to be finalized in 2016 and there are other standards bodies working on frameworks.
    - Security measures should be tested before product launch to make sure that there are no "backdoors" that could allow hackers easy entry. According to the IoT Report, encryption of data at rest and in transit should be implemented by companies (although it is unclear whether this is feasible, see below). Product design should not assume security of the consumer's home network. Strong authentication should be required for users and manufacturers should advise users to change default passwords, or even include a design element whereby the device would require the default password to be changed. The problem is that the low cost, low margin, low quality IoT devices that will appear on the market will make it difficult for companies to financially justify the cost of embedding security, like encryption, into the device or to justify costly patches and updates.
    - Consider how discovered vulnerabilities will be patched. According to the FTC report (and the Article 29 Working Party Opinion), the company must determine a process to patch known vulnerabilities throughout the product lifecycle. After the remote Jeep

Cherokee hack, consumers who wanted software updates to patch the vulnerability could receive a USB device to upgrade the vehicle's software. This solution to patches raises a dilemma: It could be difficult to get the upgrade in the hands of consumers and, even if accomplished, many consumers may not implement the upgrade. On the other hand, a patch that is available online is itself more vulnerable to malware.

- **Vet third party processors, data storage providers, and software and application providers.** It is unlikely that the entire ecosystem for even a simple IoT device will be produced in-house, especially for a small company or new market entrant. All of the data privacy and security due diligence for third party vendors must be applied to each stakeholder contributing to the IoT device ecosystem.
- **Consider data minimization.** Companies are beginning to include data minimization as part of the design process. For example, Apple's new forthcoming operating system, iOS9, has been designed with data minimization in mind. While there are many legitimate concerns with over-collection and surveillance, big data also may provide positive and unforeseen uses of data. So, while data minimization is a positive marking development and is likely to engender consumer trust, minimization can limit uses to be made for public health benefits, such as, for example, using aggregated data from health tracking devices for public health purposes such as tracking the spread of disease.

Pre-distribution

- **The mobile app.** All the considerations for a non-IoT mobile app will apply to a mobile app developed to control the IoT device. Do not overlook privacy and security in the mobile app itself. Refer to guidance from the FTC and State of California on best practices for security and privacy by design for the mobile app that connect to the IoT device.
- **The privacy notice.** The privacy notice should be transparent and accurate. This is when marketing is key to the cross-functional team. An IoT company could potentially distinguish itself in the market with transparent, trust-creating and educational privacy notices. Consider including in the privacy notice information on how security patches will be delivered to consumers. Educate consumers on changing device default passwords.

Post distribution — ongoing considerations

Privacy by design always consider the full-product lifecycle. The suggestion above should be reviewed continually after product launch to address new issues. The following two issues are specific post-launch considerations for the legal department:

- **Product end-of-life issues.** Do not fail to consider privacy and security throughout the lifecycle of the product. The company may be able to manage ongoing security risks by reasonably limiting the time during which it will provide updates and patches — but also clearly communicating those limits in the privacy notice so that consumers understand the safe "expiration dates" for the security of the IoT device being used. If the company does promise to provide ongoing support, it must comply with its own promise or risk regulatory action for engaging in a deceptive practice.
- **Third-party discovery and subpoenas for data collected by the device.** Create a response plan and include in the company's overall information governance policies the plan to address IoT data. There are unique issues in a connected world that did not exist before the IoT. While it may once have been both ideal and feasible to reduce risks by deleting data according to a records retention plan, big data — made possible by collection through IoT

devices — may offer value in data sets that once were considered worthless and hence destroyed. Now, the risks of retaining volumes of data will need to be balanced against the potential future value of using that data in new and previously unknown ways.

Further Reading

Cisco (IBSG), White Paper, The Internet of Things: How the Next Evolutions of the Internet is Changing Everything (2011).

NIST, Framework for Cyber-Physical Systems, Preliminary Discussion Draft, Release 0.7m March 3, 2015, NIST Cyber-Physical Systems Public Working Group.

Adam Thierer, “The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation,” Mercatus Working Paper, George Mason University, November, 2014, p. 47.

IPv6 is the most recent version of the internet protocol developed to address exhaustion of the number of internet address available under IPv4. About 4.3 billion addresses are available under IPv4, but 340 trillion, trillion, trillion internet addresses are available under IPv6 (enough IP addresses for any device that is made).

The FTC’s ability to bring actions alleging unreasonable data security practices has been challenged in two recent actions, LabMD v. Federal Trade Commission and and FTC v. Wyndham Worldwide Corp.

The FTC held a workshop in September, 2014, entitled “Big Data: A Tool for Inclusion or Exclusion?” and The Executive Office of the President published a report: “Big Data: Seizing Opportunities; Preserving Values.”

FTC v. TrendNet Consent and Order.

Webinar slides from FDA Webinar dated October 29, 2014.

Note that the House Appropriations Subcommittee included a provision in the 2016 appropriations bill that requires the FCC to settle all pending litigation with respect to the rule before it could take effect.

N.J. P.L 2015, Ch. 60, approved May 11, 2015, Assembly, NO. 3579.

Thierer quoting Bryan Walker Smith, Proximity Driven Liability, 102 Geo. L.J. 1777 (2014).

A zero day exploit is a hack that takes advantage of a software vulnerability unknown to the manufacturer and exploits the vulnerability before the manufacturer is aware of it and has time to patch it.

US Hotel and Resort Management, Inc., et al. v. Onity, Inc., Case No. 13-CV-1499 (D. Minn.).

Remijas v. Neiman Marcus, LLC, No. 14-3122 (7th Circuit, July 20, 2015).

Adidas AG vs Under Armour Inc and MapMyFitness Inc, Case No. 14-00130, U.S. District

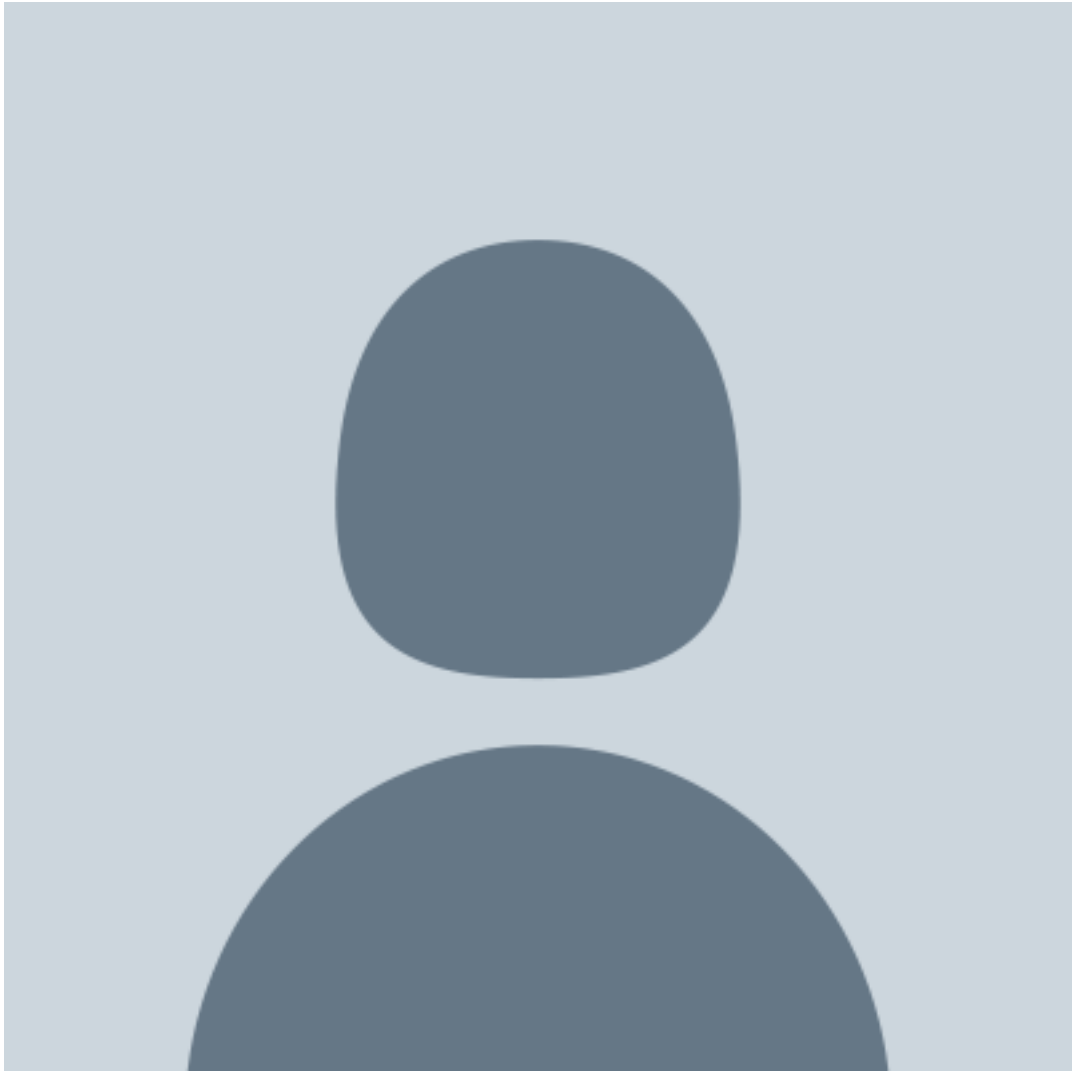
Court, District of Delaware.

Sarvint Technologies, Inc. v. Athos Works, Inc., et. al., Case No.1:2015 CV00068, N.D. Georgia.

IoT Report p. 30.

FTC Report, page 31.

Kathleen Aguilar



Corporate Counsel

Kathleen Aguilar, CIPP/US, is a seasoned corporate counsel and serves as in-house counsel on a seconded basis to companies in the Philadelphia metropolitan area. She is a trusted advisor on data privacy and security, commercial contracts and IT matters in the financial services, hospitality, insurance and nonprofit sectors.