In 1990, Internet pioneer John Romkey connected a Sunbeam toaster to the Internet for a demonstration at the Interop Internet networking trade fair. The toaster could be turned on and off by sending commands over the Internet. Romkey’s demonstration is an early example of the “Internet of Things,” or “IoT.” Experts now predict that IoT-related sensors and devices will reach 50 billion by 2020. The explosion of IoT products, software and services creates interdependent and rapidly evolving IoT “ecosystems” that include exciting benefits and potential risks.

Devices have been connecting to each other for quite some time. The surge of consumer IoT Ecosystems, however, has resulted in a greater focus on IoT’s benefits and risks, including interoperability, security, privacy, and data management. This article explores four common IoT “use cases” to demonstrate some of the benefits and risks in our homes and in the retail, healthcare and auto industries. We then distill current government, industry and legal analysis into principles and recommendations for businesses to consider when selling, buying or otherwise using IoT Ecosystems.

Understanding The IoT Ecosystem

The Internet of Things has been defined as a ubiquitous network of connected sensors embedded in everyday objects for the purpose of collecting and sharing data via the Internet. The graphic below is an example of a generic IoT Ecosystem. It is based on the graphic created by the GSMA, a leading mobile technology industry group, and illustrates a generic IoT Ecosystem.
The Service Ecosystem is comprised of software and database clusters that filter and qualify the data collected by the devices and sensors that form the Endpoint Ecosystem. The Endpoint Ecosystem is typically the technology that originates and collects data. The Service Ecosystem will ultimately use data collected by the Endpoint Ecosystem to improve user experience, enhance product performance, create new products, schedule maintenance for products, and accomplish a number of other strategic goals.

Some examples of Service and Endpoint Ecosystems given by the GSMA include:

<table>
<thead>
<tr>
<th>IoT Service Ecosystem</th>
<th>Endpoint Ecosystem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Infrastructure-based solutions</td>
<td>Wearables</td>
</tr>
<tr>
<td>Container-based application deployments</td>
<td>Home security sensor endpoints</td>
</tr>
<tr>
<td>Traditional datacenter server environments</td>
<td>Proximity beacons</td>
</tr>
<tr>
<td></td>
<td>IoT connected lighting systems</td>
</tr>
<tr>
<td></td>
<td>Appliances (such as refrigerators or washing machines)</td>
</tr>
<tr>
<td></td>
<td>Gateways (which are technically not endpoints, but may be managed by a service provider or network operator).</td>
</tr>
</tbody>
</table>

Depending on the use case, there could be a substantially greater number of networked devices and sensors in the IoT Ecosystem that collect and share data. Every point in an IoT Ecosystem (often referred to as the "Attack Surface") represents a corresponding vulnerable point(s) of contact, thus expanding the footprint of privacy and security risks.

**What Makes IoT Different From Less Connected Ecosystems?**

Domestic and international regulators and industry groups are diligently working to understand the benefits and risks associated with IoT. The Office of Privacy Commissioner of Canada ("OPC") issued a report in February 2016 that identifies some reasons why IoT Ecosystems are different relative to potential risks:

- **Interoperable communication** - electronic devices and everyday objects, especially consumer products, are increasingly being built to facilitate interoperable communication through sensors and Internet connectivity;
- **Increased sophistication** - sensors are becoming more sophisticated;
- **Seamless connectivity** - objects and devices have the ability to seamlessly connect and communicate a wide range of online and offline information (including location, biometrics, purchases, and online browsing history);
- **Affordability** - IoT computing devices are becoming affordable and accessible for individuals and organizations of all sizes, including small- and medium-sized enterprises; and
- **Cloud computing and Big Data analytics** - are available for all organizations to store information, share it, and make inferences about their clientele.
In order to identify and anticipate the various risks associated with IoT, regulatory agencies in Europe and the U.S. have invited open dialogue with industry representatives and other public interest groups through forums, workshops, and public consultations. The FTC held its initial IoT workshop in 2013 and published an updated staff report concerning IoT best practices and policies in 2015. Similarly, the European Commission’s Article 29 Working Party published its own formal opinion of IoT benefits and risks in 2014. In addition, numerous industry associations such as GSMA, NHTSA, NIST, IPSO, and many others have also issued guidance to, and solicited opinions from, the various industry interests they represent, and have created industry-specific IoT practice recommendations in the process.

In its 2015 Staff Report, the FTC identified numerous IoT use cases which are already in the market, such as RFID tags used to monitor inventory in retail environments, connected healthcare devices that improve diagnosis, treatment and disease prevention, smart meter devices that promote and regulate efficient energy use in the home, and smart cars that alert first responders when airbags are deployed.

Below are use cases that demonstrate the current and potential impact of IoT on the following four industries: (1) the Retail Industry; (2) the Residential and Home Goods Industry; (3) the Automotive Industry; and (4) the Healthcare Industry.

I. **IoT USE CASES: BENEFITS**

1. **Retail Industry Use Cases**

   The OPC’s privacy report provides an in-depth look at IoT’s potential impact on the retail industry. Retail use cases include in-store tracking, interactive mannequins, and targeted ads that offer discounts on in-store items to consumers that pass within a wireless boundary surrounding the store. As noted by the Retail Council of Canada, “[t]he store is no longer just a store, but instead a space where opinions, reviews, social media, mobile, expectations, experience, technology and attitude combine to create connections.”

   **1.1 Consumer Benefits**

   Home replenishment technologies, the ability to “test” products virtually prior to purchase, and “connected” fabrics and garments may transform the customer experience. More specifically:

   - IoT may change the consumer shopping experience by eliminating trips to retail establishments altogether, through “home replenishment” technologies that notify or automatically purchase replacement products when needed.
   - Amazon introduced small electronic devices called “Dash Buttons” in 2015 which allow consumers to place orders for frequently used domestic products such as detergent or dishwashing liquid with the touch of a button.
   - Egg Minder is a smart egg tray that keeps track of how many eggs are in the refrigerator and alerts its owner to approaching expiration dates.
• Smart phone applications allow consumers to experiment with beauty products before making a purchase.21
• Sensors inside smart fabrics offer consumers clothing which can change color based on mood, monitor vital signs, or provide exact measurements so consumers know exactly what size to order for every article of clothing.22
• Google and Levi, for example, recently teamed-up “to launch a “connected” smart jacket aimed at urban cyclists that will allow wearers to do things like control their music, answer phone calls, access navigation and more, all by tapping and swiping on the jacket’s sleeve.”23

Consumers will also benefit from enhanced in-store experiences as IoT-enabled devices provide consumers with notifications of on-sale products and services based on a consumer’s browsing history.24 Virtual reality mirrors may allow consumers to “try on” clothing without ever setting foot in a changing room.25 Interested shoppers may interact with smart mannequins to ask about the clothes they are wearing.26 And, smart beacons will automatically alert a shopper to discounts and products they are interested in as soon as they walk through the doors.27

1.2 Retail Industry Benefits

The OPC demonstrated how retailers might benefit from tracking both current customers and prospective customers – whether inside or outside the store – through “passive” and “interactive” tracking technologies.28 As the chart below demonstrates, interactive and passive tracking methods incorporate the use of cellular, wi-fi, Bluetooth, Near Field Communications (“NFC”), and Radio Frequency Identification (“RFID”) technologies. Combining these technologies, retailers can track prospective customers and present targeted advertising and convince a customer “walking by a store, to walk through it, to browse products on a shelf or on a smart phone, and eventually to make purchases.”29

<table>
<thead>
<tr>
<th>In-store</th>
<th>Outside of Store</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passive Observation</td>
<td>Location tracking via short-range radio.</td>
</tr>
<tr>
<td></td>
<td>Short-term behavior analysis.</td>
</tr>
<tr>
<td></td>
<td>Video cameras used to analyze customer traffic flows.</td>
</tr>
<tr>
<td></td>
<td>Facial detection and analysis to customize digital signs and ads.</td>
</tr>
<tr>
<td></td>
<td>Downloading an app to receive coupons when in store.</td>
</tr>
<tr>
<td></td>
<td>Connecting to a “free” Wi-Fi service.</td>
</tr>
<tr>
<td></td>
<td>Completing a NFC-enabled transaction (for example, a mobile payment on a smart phone).</td>
</tr>
</tbody>
</table>
Of course, as with other use cases, there are additional benefits of advanced inventory management loss prevention using connected sensors and GPS capabilities.

2. Residential and Home Goods Industry Use Cases

IoT is already integrated with home life in subtle and practical ways through smart TVs, streaming content services like Netflix or Hulu, Internet radio such as Pandora, and many other daily use products and services. In the coming years the focus will shift from siloed smart devices within the home to the numerous smart appliances, devices and sensors that compose an IoT-Ecosystem referred to as the “smart home.”

2.1 Consumer Benefits

The potential convenience and comfort benefits of the home IoT Ecosystems are tremendous. Examples include:

- Smart energy meters reduce inefficient energy use and cut costs for consumers.
- Smart TVs and entertainment systems allow consumers on-demand frictionless access to their favorite content.
- Security systems allow consumers to remotely monitor security camera video feed from their homes or open the front door for a dog-sitter all through their smart phones.
- Traditional main-stay appliances will be able to communicate with consumers and each other to maximize convenience, increase efficiencies and cut costs.
- Smart refrigerators tell consumers when the milk has gone bad. Smart ovens allow consumers to begin the preheat process before they leave the grocery store with a frozen pizza.
- The smart backsplash will transition from a mere accent piece to an entertainment hub in the kitchen, allowing the consumer to display photos or stream movies while at the stove.

In 2015, CNET, a technology and consumer electronics media outlet, acquired a 5,800 sq. ft house for the sole purpose of integrating, testing and reviewing IoT smart home technology. As of May 2016 they have incorporated the following smart home devices:

- Wi-Fi enabled smart speakers
- Wireless smart switches to control lights
- Wi-Fi enabled DIY security cameras
- Wi-Fi enabled smart home security system
- Wi-Fi enabled smart frying pans
- Wi-Fi enabled smart range and...
stovetop
- Smart cooking thermometer
- Smart ceiling fans
- Smart garage door opener
- Smart thermostat

- Smart slow cooker
- Smart remote and entertainment management devices
- Smart washer and dryer

2.2 Industry Benefits

Smart home goods and appliances will also communicate with their manufacturers providing an unending supply of data and valuable insight into product improvement, regular maintenance requirements, energy consumption, and consumer satisfaction. Smart home goods and appliances may also provide manufacturers with the opportunity to assess emerging consumer needs and to create new products and services that address such consumer needs. Some industry experts claim that, where manufacturers are concerned, IoT opportunities have less to do with selling smart products and more to do with leveraging the smart products they do sell to create new service offerings for consumers. Following this model, manufacturers may be able to convert products formerly confined to a single sale into future recurring revenue streams.

Information collected by manufacturers can also help (or hurt) in connection with product liability cases. Examples include when relevant information, such as when appliances are left “on” or when a product is used in a way not intended, is collected. This type of information is already used, for example, in airplane disasters with the “black box” recording relevant data. Use data in IoT Ecosystems will likely become more relevant and expansive.

3. Automotive Industry Use Cases

Regulatory agencies, car manufacturers, technology providers and industry interest groups have been working on the auto IoT Ecosystem for quite some time. Industry groups like GSMA have estimated that every car will be connected in some way by 2025, and the market for connected vehicle technology will reach $54 billion by 2017.

The average American car has between 60 and 100 onboard sensors each of which has IoT connectivity potential that could enhance vehicle maintenance and performance as well as driver and passenger safety. These sensors include the following:

<table>
<thead>
<tr>
<th>Air Pressure Sensor</th>
<th>Airbag</th>
<th>Blind Spot Monitoring Camera</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collision Detection Sensor</td>
<td>Drive Recorder</td>
<td>Driver Monitoring Sensor</td>
</tr>
<tr>
<td>Electronic Control Brake</td>
<td>Electronic Control Steering</td>
<td>Electronic Control Throttle</td>
</tr>
<tr>
<td>Fire Detector Sensor</td>
<td>Forward Obstacle Sensor</td>
<td>GPS Sensor</td>
</tr>
</tbody>
</table>
The who’s who of the tech and automotive industries are teaming up to invest in everything from self-driving cars to mapping technology for autonomous vehicles. And, put simply, car companies are moving towards becoming technology companies and vice versa. Elon Musk, CEO of Tesla Motors, recently mused that Apple will eventually be a direct competitor and make its own vehicles as soon as 2020. Amazon has teamed up with Ford to create self-driving cars that can communicate with consumers’ in-home devices, and it was recently rumored that Microsoft and Amazon would each invest in mapping systems for autonomous vehicles. Google, Uber, and Ford announced the launch of a coalition to further self-driving cars. Ford recently invested over $182M dollars in Pivotal Software, Inc., a cloud-computing joint venture of EMC Corp. and VMware Inc., and created a new unit, Ford Smart Mobility, to expand its presence and partnerships in the tech-focused region.

And, as with any technology, start-ups are entering the fray, including a company called Otto, which is comprised of former Googlers intent on creating safe self-driving technology to big-rig trucking.

### 3.1 Consumer Benefits: Vehicle Sensors, Performance and Safety, Autonomous Cars

Industry professionals tout potential consumer safety, performance and infotainment benefits among consumer experience benefits for the automotive industry. For example, some assert that consumer safety may increase significantly once a majority of passengers are transported by vehicles equipped with numerous IoT devices which allow them to make critical and timely safety decisions. As the GSMA noted, “the goal is to leverage the intelligence of as many sensors as possible to [allow the vehicles to] make critical decisions in very small windows of time . . . [and] automatic breaking, tire blow-out broadcast alerts, temporarily disabled operator warnings, and other critical scenarios can potentially be resolved through the use of sensors and well-designed computer systems.” In addition, many automotive use cases aim to promote entertainment features which drivers will be able to enjoy while their self-driving car takes them from A to B. Some industry experts have even predicted that when many people purchase their next car they “will not need to look under the hood [because] what will be valuable to [them] is the screen size of the console, or the ease of connection to [their] devices or the interface in which [they] can power these devices in [their] car.” As discussed above, IoT-enabled cars are expected to feature a large number of on-board sensors that will
communicate their presence (in what would formerly have been regarded as a blind spot) to other cars and observe their immediate environments while warning other cars of poor road conditions.

Currently, autonomous and self-driving vehicle technologies are quickly moving from prototype vehicles to reality. Numerous reputable auto manufacturers are exploring the technology alongside tech industry representatives like Google and Uber.\textsuperscript{55} Carlos Ghosn, the CEO of Renault-Nissan, indicated that Nissan will have 10 vehicles on sale by 2020 with "significant autonomous functionality."\textsuperscript{56} Many "high-end" cars have much of the technology required for autonomous vehicles, including sensors and technology for GPS, automatic breaking, lane departure protection, Lidar, Radar, Sonar for accident avoidance, active cruise control, and others. Though it may be some years before all of us enjoy reading a book while our car navigates rush hour traffic, there are immediate and practical use applications, such as the ability to control and monitor cars remotely. In the future, consumers may be able to send their cars to the grocery store to pick up groceries they order online.\textsuperscript{57} All of these possibilities and more could be appealing and beneficial to consumers.

\textbf{3.2 Industry Benefits: Auto Manufacturers, Car Insurance, Rental Companies, Automotive Lenders}

The potential benefits to the automobile industry are fairly obvious and range from enhancing customer experience to potentially increasing safety. Data collected can range from creating loyalty to particular brands, to learning driving habits, to helping understand the future of vehicle use and consumption by consumers and industry. Apps, for example, can help show where the next electric recharge station is located for future reference based on driving habits to assist drivers in planning. Further, sensors and information can be used to help determine if and when parts are in the process of failing before they do so, having potential impacts on increasing vehicle safety impacting product liability law suits.

In addition to diagnosing their own maintenance and performance issues, IoT-enabled cars are capable of providing information about our driving habits to insurance companies that can affect our premiums.\textsuperscript{58} Car insurance companies have been using GPS systems to monitor and reward safe driving behaviors for years by monitoring whether their insured drives less than a certain number of hours each year, drives after midnight, or frequently slams on the brakes.\textsuperscript{59} Other carriers have implemented more sophisticated sensors that measure and report speeding violations, seat belt use, and provide geographical location data. Insurance companies now provide drivers with apps that monitor their driving habits in exchange for better rates and to presumably improve driver safety because there is a knowledge that the driver is being monitored. Some have noted that the “use of data for insurance decisions could bring benefits – e.g., enabling safer drivers to reduce their rates for car insurance or expanding consumers’ access to credit – but such uses could be problematic if they occurred without consumers’ knowledge or consent, or without ensuring accuracy of the data.”\textsuperscript{60}

Similarly, the car rental industry has also experimented with such sensors to promote safe driving among its renters.\textsuperscript{61} Lenders that finance subprime car loans have equipped their
debtors’ vehicles with GPS to track vehicle location and kill switches or starter interrupt devices that allow lenders to remotely disable a vehicle’s ignition when a creditor falls behind on his or her car payments.\textsuperscript{62} These technologies are already being incorporated into IoT and one lender reported that he was able to disable a vehicle from his smart phone while shopping at Wal-Mart.\textsuperscript{63} Using these technologies some lenders have reduced instances of late payment from 29\% down to 7\%.\textsuperscript{64} These technologies also have applicability for companies requiring fleet management and in the trucking industry.

4. Healthcare Industry Use Cases

Various studies have already demonstrated the numerous healthcare benefits that can be derived from connected and IoT-enabled devices\textsuperscript{65} and industry groups have predicted that the healthcare IoT market is poised to hit $117 billion by 2020.\textsuperscript{66} Like other use cases the benefits flow both to individual consumers as well as the industry concerned.

4.1 Consumer Benefits

Healthcare professionals have long touted the ability of connected and IoT-enabled devices to better engage patients in their own care rather than leaving it entirely in the hands of physicians.\textsuperscript{67} For example, glucose monitors worn by diabetics have allowed physicians to remotely and continually monitor their patients’ blood sugar levels and adjust medications accordingly resulting in improved disease management and cost efficiency for patients.\textsuperscript{68} Edible technology is being inserted in the form of IoT “smart” pills that can monitor patients’ medication regiments and identify outstanding health issues.\textsuperscript{69}

Just as they have in the automotive industry, tech titans are teaming up with healthcare providers and medical device makers to harness the full potential of the IoT in the healthcare space.\textsuperscript{70} In a 2014 industry report, Intel and Dell discussed the profound impact of IoT on the burgeoning telemedicine space citing increased accessibility of healthcare services for patients with limited mobility such as those in assisted living or palliative care and other hard-to-reach patients such as those living in rural or remote locations in underserved countries like Africa, India, or Central America.\textsuperscript{71} Big Data analytics may enable medical professionals to identify critical cause and effect relationships and improve patient outcomes using data collected by smart medical devices.\textsuperscript{72}

Consumers with health concerns are not the only ones that benefit. Numerous wearable devices and fitness trackers aim to enable healthy consumers to improve their existing health.\textsuperscript{73} Fitness wearables such as the FitBit, iWatch, Garmin, Vivosmart, and TomTom have enabled individual consumers to monitor and record their exercise activities, heart rate, sleeping habits, and steps taken per day.\textsuperscript{74} Telemedicine allows patients to stay “in-home” for treatment rather than costly (or sometimes impossible) visits with doctors many miles away, ranging from using a mobile device or phone to communicate with doctors to more complex and integrated telemedicine mobile “stations” that can help take and transmit glucose levels to doctors, take temperatures and blood pressure, and include other monitoring devices.
4.2 Healthcare Provider Benefits

IoT-enabled devices are already helping the healthcare industry address operational issues related to everything from equipment and inventory management to patient tracking.\(^7^5\) RFID technologies and mobile scanners, connected with cloud technology, are helping organizations control and manage their inventories to help ensure that physicians and patients have the medications and equipment they need to provide continuity of service.\(^7^6\) Cloud-based hygiene systems may help healthcare organizations significantly reduce hospital-acquired infections that have a tremendous impact on rising healthcare costs.\(^7^7\) Physician consultations provided over the Internet through telemedicine are already saving healthcare providers significant overhead costs in addition to opening up significant new revenue streams for healthcare providers.\(^7^8\)

4.3 Healthcare Insurance Industry Benefits

In the same way that IoT vehicle sensors have allowed ancillary industries outside of the automotive industry to advance their own agendas, so have IoT medical devices become a key part of the healthcare insurance industry’s strategy. Even where collected data is not sensitive personal health information, the continuous collection of non-sensitive data through numerous sensors may ultimately allow third parties to compile an unprecedented amount of data about an individual and draw ‘sensitive’ health inferences about that individual. For example, non-sensitive data collected from existing smartphone sensors has allowed third parties to make specific inferences about an individual’s mental, physical and financial health.\(^7^9\) This information could be used to impact premiums for health coverage.

II. IoT USE CASES: THE RISKS

1. Retail Industry: IoT Risks

The retail industry is replete with consumer privacy and security and management concerns. Other than tracking a device, a primary purpose is to study the behavior of the consumer who owns or uses the device and, as such, even anonymized, de-identified data may ultimately provide enough data to make personal inferences about device owners, with or without consent.\(^8^0\) The Supreme Court of Canada recently held that there is a reasonable expectation of privacy in subscriber information linked to Internet activity, since such information may reveal sensitive information about a subscriber.\(^8^1\) Also, the Advocate General (“AG”) of the Court of Justice of the European Union issued an opinion stating that Internet Protocol (“IP”) addresses are personal data to the extent they can be combined with other data allowing for the identification of the user (and thus become subject to the EU data protection laws and requirements).\(^8^2\) Compliance with laws may become more difficult, and notice and consent requirements often provide a challenge to industry. The additional increased number of collection/attack points increase the potential for hacking like any other IoT Ecosystem, but notice and consent consistent with required regulations is also an issue in retail.

2. Residential and Home Goods Industry: IoT Risks
Consumer privacy and security concerns are even more acute and “personal” in the home. Smart devices may collect data that is used to improve consumer experience or their own performance; however, what else will smart devices be allowed to monitor within our homes and who will they be allowed to share it with?

IoT of the home may offer a technological and convenience-oriented paradise while at the same time creating a “privacy hell.” Unless proper controls and procedures are implemented, IoT will invariably support the continuous and indiscriminate collection of tremendous amounts of personal data. For example, one study indicated that a group of less than 10,000 homes, each containing an IoT device, produced in excess of 150 million discrete data points per day.

Of course, IoT will not merely collect performance data from smart kitchen appliances but may also collect sensitive data concerning an individual’s financial information, healthcare information, and physical location from a myriad of other sensors. Companies must work to define the degree of control that consumers will be allowed to exert over connected environments and determine whether consumers will be able to control the types of information that may or may not be collected. Depending on the particular IoT Ecosystem, Consumers may need to be informed as to whether connected devices are primarily passive and reactionary or whether manufacturers or other third parties will be allowed to actively collect data through connected devices. Defining a consumer’s right to control and limit connected devices and environments presents a threshold challenge for IoT’s privacy concerns.

A consistent theme in many "use cases" involves product liability analysis. What if, for example, a sensor fails to detect a fire? What if the signal to turn an appliance "off" fails, leading to that fire? Another interesting question is whether reliance on a sensor creates "reliance" as a legal risk? These and other product liability issues are consistent risks in most uses cases and worthy of exploration.

3. Automotive Industry: IoT Risks

Potential risks related to IoT of the Automotive Industry are many, including from hacking a vehicle for nuisance issues, to scraping personal data contained in the auto IoT Ecoystyem, to product liability and safety, including the manipulation of critical components such as a car’s brakes or even turning a car off. In 2015, two hackers conducted an experiment to determine whether they could remotely hack a 2014 Jeep Cherokee loaded with onboard sensors. When they succeeded in breaching the vehicle the hackers worked their way around the car turning on the air conditioning, the radio, and the windshield wipers before toying with more critical systems like the transmission and ultimately the cars brakes.

Government and industry groups such as the National Highway Transportation Safety Administration (“NHSTA”), the National Institute of Standards and Technology (“NIST”), and the GSMA have all provided helpful guidelines and industry practices for those developing IoT products and services related to the automotive industry. Automotive cyber security is premised on the assumption that all entry points on the vehicle are potentially vulnerable. Such assumption assumes, for example, that Wi-Fi, infotainment, and the On-Board
Diagnostics-II ports are vulnerable so that each system may be identified and programmed to take appropriate measures to protect itself even when an attack on another system is successful. 

### 4. Healthcare Industry: IoT Risks

IoT-enabled medical devices may pose significant risks to the patient health and data. For example, Vice President Dick Cheney’s cardiologist, fearing a malicious attack delivered over the Internet, famously disabled Wi-Fi capability of the Vice President’s pacemaker during his time in office. Security researchers have also researched the vulnerabilities of IoT-enabled drug infusion pumps and found that such devices were susceptible to attacks that would allow a hacker to remotely control the dosage of medication delivered by the pump. In a 2015 article Wired magazine listed the following medical devices as being vulnerable to a life-threatening hack:

- Drug Infusion Pumps;
- Insulin Pumps;
- Implantable Cardioverter Defibrillators;
- X-Ray Systems;
- Blood Refrigeration Units;
- CT Scans; and
- Medical Simulators.

In addition, there has been an increasing attack of ransomware as more points of vulnerability are created in the IoT Ecosystem. Ransomware is malicious code that, once downloaded, allows bad actors to freeze a system’s functionality and hold the system hostage until demands for payment are met. Ransomware presents a current threat to healthcare providers particularly where critical systems are affected. In May 2016, the HHS Office for Civil Rights revealed that it is developing guidance on how health-care organizations should prepare for and respond to ransomware attacks.

The FDA is also concerned about the security of medical devices. In January 2016, the FDA issued guidance and the Agency’s recommendations for managing post-market cybersecurity vulnerabilities for marketed medical devices.

Manufacturers are encouraged to address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment and maintenance of the device. A growing number of medical devices are designed to be networked to facilitate patient care. Networked medical devices, like other networked computer systems, incorporate software that may be vulnerable to cybersecurity threats. The exploitation of vulnerabilities may represent a risk to the safety and effectiveness of medical devices and typically requires continual maintenance throughout the product life cycle to assure an adequate degree of protection.
against such exploits. Proactively addressing cybersecurity risks in medical devices reduces the patient safety impact and the overall risk to public health.

In 2015 the Atlantic Council partnered with Intel Corporation and Intel Security Group to publish a healthcare industry white paper entitled “The Healthcare Internet of Things: Rewards and Risks.” This paper discusses the impact of IoT on the healthcare industry and the challenges that bring security risks to the fore of IoT of healthcare.

- **Lack of Overarching Security Standards and Best Practices**: Firmware and Software underlying IoT-enabled medical devices lack consistency amongst versions, standards and approaches to implementation.

- **Lack of an Infrastructural Standard**: IoT-enabled medical devices have no network standard operating environments, architectures, communications methods or networking backends.

- **Security Measures Counter to Legitimate Business Needs**: Stringent security measures implemented in a local health network may improve security but hinder access to information and interrupt service delivery in critical care scenarios.

- **Software Disparities**: Device and application software disparities are commonplace due to a lack of standard programming language across a given industry. The costs of updating or switching code prohibit most companies from moving beyond a device’s “legacy code.”

### III. FTC REGULATORY ENFORCEMENT

Two recent FTC regulatory actions resulting in Consent Orders help illustrate some of the risks of the IoT Ecosystem for Internet Protocol (“IP”) cameras and routers.

1. **TRENDnet Enforcement Action: The Facts**

   In 2013 the FTC initiated regulatory action against TRENDnet (“TREND”) in a seminal case that is likely the first regulatory enforcement action against a manufacturer of IoT devices. TREND is a retailer of various networking devices including routers, modems and IP cameras. TREND’s IP cameras allowed users to remotely monitor their homes and business over the Internet.

   However, the IP cameras contained two fatal design flaws. One design flaw allowed users to waive the requirement for login credentials and the other design flaw allowed for a user’s live feed to be accessed publicly even when set to private. In addition to these design flaws, TREND regularly transmitted user login credentials in clear text over the Internet. After discovering these design flaws, a hacker posted the live feeds from various IP cameras online. The live feeds posted by the hacker featured footage of babies asleep in their cribs and young children at play. TREND was apprised of the breach in early 2012 and provided new software to
eliminate the vulnerability. Thereafter the FTC began its investigation resulting in the entry of a Consent Order.\textsuperscript{101}

2. \textit{ASUSTeK Enforcement Action: The Facts}

In 2016, Taiwan-based computer hardware manufacturer ASUSTeK Computers, Inc. (“ASUS”) agreed to a 20-year consent order, resolving claims that it engaged in unfair and deceptive practices in connection with routers it sold to U.S. consumers. In its original complaint the FTC alleged that ASUS failed to take reasonable steps to secure the software for its routers, which were advertised and sold to U.S. consumers specifically for the purpose of providing security and protection for consumers’ personal networks.

The FTC further alleged that the ASUS routers were susceptible to a number of commonplace “well-known and reasonably forseeable vulnerabilities” that allowed hackers to gain easy, unauthorized access to consumers’ files and router login credentials. As a result, the FTC concluded that ASUS had subjected its customers to significant risks with respect to their personal and private information. Again, as in TREND, the FTC’s investigation resulted in the entry of a Consent Order.\textsuperscript{102}

3. \textit{Lessons From TRENDnet and ASUSTeK Consent Orders}

Ultimately, the FTC issued Consent Orders to both TREND and ASUS listing the steps required for each company to establish and maintain a security program sufficient to protect its devices in the future.\textsuperscript{103} These steps included action items such as the appointment of a security officer, the design and implementation of safeguards and controls for hardware and software, and the development of a vendor management program. Using the FTC’s action items TREND and ASUS are required to establish internal governance programs that will integrate security into their organizations. Many of the action items represent core governance principles that have been reaffirmed by other regulators and industry focus groups throughout the world.

IV. \textbf{EMERGING IoT RECOMMENDATIONS}

Below is a compilation of recommendations from various sources identified in this article, including from governmental agencies, industry, legal commentary and the two recent FTC Consent Orders. Some language is modified, while other language is provided verbatim. The recommendations are presented in three phases: (1) Identify; (2) Implement; and (3) Improve.

For purposes of the list, the following definitions apply, modified from the FTC Consent Orders:

“Covered Device and Network” means: (a) an applicable device used in an IoT Ecosystem; (b) the network over which an applicable device may communicate; (c) the software used to access, operate, manage, or configure the device, including, but not limited to, the
firmware, web or mobile applications, and any related online services used with or compatible with the device; and (d) the network over which an applicable device may communicate.

“Covered Information” means any individually-identifiable information from or about an individual or any information that, when used in combination with other information, could identify an individual, collected by or through a Covered Device or input into, stored on, captured with, accessed, or transmitted through or in connection with a Covered Device.

A. IDENTIFY.

• **Identify Your Team for a Security Program.** Identify key stakeholders and internal business units throughout the organization and designate an employee or a group of employees to coordinate and manage a security program specific to IoT products and services with the help of these key stakeholders and business units (“Security Program”).

• **Identify an Emergency Response Team and Process.** The same team (or a subset of the team) leading the Security Program should be in place for emergency response and a process should be in place for incidence. Contingency plans should be in place and there should be training and simulated response drills on some regular basis (example: annually).

• **Identify the Risks to Covered Devices and Networks.** Company management should work with the Security Program personnel to identify material internal and external risks to the security of Covered Devices and Networks that could result in unauthorized access to or unauthorized modification of a Covered Device and Network, and assessment of the sufficiency of any safeguards in place to control these risks. It is often helpful to create a graphic of the specific IoT Ecosystem to help identify all possible devices and networks.

• **Identify the Risks to Covered Information.** Company management should work with the Security Program personnel to identify material internal and external risks to the privacy, security, confidentiality, and integrity of Covered Information that could result in the unintentional exposure of such information by consumers or the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. It is often helpful to overlay data transfers to the graphic created for the specific IoT Ecosystem.

• **Identify the Covered Information For Data Minimization.** As a ubiquitous network of connected smart sensors, IoT has the potential to create an unscrupulous data dragnet with each sensor indiscriminately collecting data that has no correlation to the device’s purpose or the manufacturer’s needs. Carefully consider the business needs and data collection practices in order to develop tailored data collection and retention limitations that are reasonable and limited in light of such needs.
• **Identify Privacy and Security Regulations.** The Security Program should be designed to regularly identify and implement the requirements of new regulations affecting the applicable Covered Device and Network.

• **Identify Applicable Standards for the Covered Device and Network.** The Security Program should be designed to regularly identify and understand the growing number of standards for the applicable Covered Device and Network. Many standards organizations are working on the creation of generally applicable standards to help with interoperability and help provide greater data privacy and security.

• **Identify Product Liability Issues.** While privacy and security are key, the Security Program should meet regularly to identify potential product liability issues, ranging from the ability to manipulate "nuisance systems" (like air conditioning in a car) to critical systems (like smart meters that may be hacked to gain access to the smart grid or whether home owners are likely to be at home based on energy usage). In addition, identify that a consumer may rely on certain features of Covered Devices for purposes greater than intended; accordingly, the purpose and limitations of the same should be considered.

**B. IMPLEMENT.**

• **Implement Operational Controls and Safeguards.** Implement practices to address covered Devices and Networks and Covered Information Risks, including considering the following: (1) employee training and management, including in secure engineering and defensive programming; (2) product design, development, and research; (3) secure software design, development, and testing, including for default settings; (4) review, assessment, and response to third-party security vulnerability reports, and (5) prevention, detection, and response to attacks, intrusions, or systems failures.

• **Implement Personnel Risk Management Controls.** Companies, through management and Security Program personnel, should develop personnel practices and procedures that promote good security and promote a pervasive culture of security. Companies must accept that data privacy and security is now an enterprise-wide risk, and is no longer a risk to be relegated to its IT Department.

• **Implement Software Controls and Safeguards.** Company management should work with the Security Program personnel to design and implement reasonable safeguards to control the risks identified above through reasonable and appropriate software security testing techniques, such as (1) vulnerability and penetration testing; (2) security architecture reviews; (3) code reviews; and (4) other reasonable and appropriate assessments, audits, reviews, or other tests to identify potential security failures and verify that access to Covered Devices and Covered Information is restricted consistent with a user’s security settings.
• **Implement Reasonable Access Controls.** Companies should implement reasonable access control measures to prevent unauthorized access to connected devices.

• **Implement Security By Design Principles.** Companies should implement “security by design” during product development by intentionally designing robust security into their products at every stage of development. In addition, companies should regularly pressure test their designed security measures with risk assessments and security tests prior to launch. It is important to note that there may be practical difficulty with securing these systems for embedded/hardware devices. These systems are not always easily updatable (less so for software, but much more for "firmware" embedded in the hardware).

• **Implement Defense-In-Depth To Account for Interoperability Risks.** Companies should implement a defense-in-depth approach at several levels to secure systems with significant risk. The defense-in-depth approach addresses potential vulnerabilities created by interoperability. According, companies should work to ensure data security in each individual device and within the communication lines between such devices.

• **Implement Notice and Choice.** Companies should provide consumers with notice of IoT products and services and the opportunity to choose whether he or she will accept such products and services, and also consent to the data collection and use. Consumer protection principles of “notice and choice” have grown out of the Internet era, however, these principles may present new challenges in IoT where complex networks of devices may prevent consumers from receiving meaningful notice and choice. Nevertheless, providing consumers with the opportunity to make informed decisions concerning the use of their data remains critical, particularly where sensitive personal data is implicated.

• **Implement a Comprehensive Vendor Contracting and Management Program to Engage and Manage Vendors with Appropriate Security Standards.** Management in connection with the Security Program personnel should develop a comprehensive vendor management program to address (a) vendor negotiations; (b) vendor security assessments; (c) vendor contracts; (d) vendor on-boarding processes; (d) vendor audits; and (e) any continual vendor monitoring practices.

C. **IMPROVE.**

• **Pressure Test Controls and Safeguards.** Regularly test and monitor the effectiveness of the safeguards’ key controls, systems, and procedures.

• **Review and Assess.** Management, in connection with the Security Team, should schedule and implement privacy and security risk assessments at regular intervals and should implement and review the results of same to execute any improvements.
• **Continually Evaluate and Revise the Security Program.** Evaluate and adjust the Security Program in light of the results of the testing and monitoring, any material changes to a company’s operations or business arrangements, or any other circumstances that the company knows or has reason to know may have a material impact on the effectiveness of the Security Program.

• **Device Lifecycle Management.** Companies should examine the potential lifecycle of their IoT product and service offerings and clearly communicate to consumers any scheduled updates. Many IoT devices may have a relatively short lifecycle and, as a result, consumers may be faced with out-of-date and unsecure devices interacting with their connected environments.

• **Accountability.** Companies should proactively demonstrate a willingness to be held accountable for their data collection and usage practices and should inform consumers how they have used, are using, and will use consumer data.

• **Transparency.** IoT Ecosystems will likely include numerous devices that are designed to operate without a consumer’s knowledge and, as a result, consumers may find it increasingly difficult to answer “what, when, where, why and how” questions regarding IoT devices hiding in plain sight. Depending on the IoT Ecosystem, consider clearly notifying consumers of the presence and purpose of certain IoT devices and sensors. There are, however, differing opinions as to how such notice is best provided. One option may be to provide consumers with a SMS notification of such IoT devices but such notifications could lead to an endless barrage of SMS messages.

**Conclusion**

We live in dynamic and exciting times. IoT Ecosystems are transforming our individual and business experiences, disrupting how we historically viewed consumer-provider relationships and creating new, intelligent connections and possibilities.

In addition to propelling us forward on a broad range of fronts, IoT Ecosystems also introduce and perhaps compound risks associated with data management, interoperability, security and privacy. More consistent sets of best practice recommendations and themes are beginning to take shape, directly addressing the management of these risks.

Undoubtedly, regulations and industry standards will continue to develop over time, including regulations applicable to specific industry and the development of IoT standardization. With respect to regulations, while many agencies are looking at the topic, some have resisted the temptation. The FTC, for example, recently reaffirmed its stance that regulating privacy and security for IOT would be premature.\(^{104}\) Notwithstanding, maintaining a knowledge of the regulatory landscape remains important, as regulation is only a matter of time, and "guidance" issued (including the FDA guidance, for example) may foreshadow compliance expectations.
With respect to standards, government and other organizations have been working on industry-specific standards for IoT Ecosystems. In 2015, the Institute of Electrical Engineers (“IEEE”), for example, published its “IEEE-SA Internet of Things Ecosystem Study” noting that there is almost universal consensus that global standardization is necessary. The study states that most of the existing standardization challenges are not unique to any region, and most companies want to produce products and services for a global market. IoT standardization will enable and promote such global markets. Related issues include wireless and security and privacy regulations, which vary by region. As a result of such regional variance, the development of generally acceptable and applicable standards will present a significant ongoing challenge to companies incorporating IoT into their business plans.

By the time this article is distributed, there will be even more discussion concerning the treatment of the various benefits and risks that originate from or are associated with IoT Ecosystems. Proper internal controls, policies and programs, along with an interest and willingness to stay abreast of IoT’s ever-changing terrain, can help position companies to strike the right risk-reward balance and leverage the possibilities of the Internet (of Everything).

Jason Epstein is the Co-Chair of the Technology and Procurement Industry Group for the Firm. He and the technology team provide legal services to buyers and sellers of technology both domestically and internationally. Mr. Epstein’s experience includes outsourcing, cloud computing, licensing, Healthcare IT, FinTech, Internet of Things (IoT), joint ventures, mergers and acquisitions, technology transfer, privacy and security, and open source code. He also acts as outside general counsel to various companies. You can contact Mr. Epstein at: Jason.Epstein@nelsonmullins.com.

Will Gibbs is an associate in the Technology and Procurement Industry Practice Group. He assists the technology team in providing legal services to buyers and sellers of various technology solutions. Mr. Gibbs’ experience includes representing companies in connection with technology licensing and IT outsourcing agreements, buying and selling of financial services technologies, healthcare services companies, data management and security matters, and general corporate governance and transactional matters. You can contact Mr. Gibbs at: Will.Gibbs@nelsonmullins.com.

---

2 Id.
4 Recent technological developments have allowed the scope of IoT to expand far beyond standalone smart appliances and consumer experience enhancement. In fact, some predict that as IoT is deployed across numerous industries such as healthcare, transportation, energy, manufacturing and distribution operations, retail, and agriculture, such a broad application may result in enterprise use of IoT outpacing consumer use. While IoT’s broad applicability in enterprise certainly merits its own focused discussion, this article is focused on the issues implicated by consumer adoption of IoT.
See The Internet of Things, Office of the Privacy Commissioner of Canada (February 2016), http://www.priv.gc.ca/information/research-recherche/2016/iot_201602_e.asp.


See The Internet of Things, supra note 9.


See Hawkins, supra note 45.


See Michael Corkery and Jessica Silver-Greenberg, supra note 57.


See Jill Duffy and Alex Colon, The Best Fitness Trackers for 2016, PC Mag (May 16, 2016), http://www.pcmag.com/article2/0,2817,2404445,00.asp.


See Transforming Healthcare with Telemedicine Solutions Based on the Internet of Things, supra note 68.

See The Internet of Things, supra note 9.

Id.


Id.

Id.


Id.

Id.


Id.


Id.

See Kim Zetter, Medical Devices That are Vulnerable to Life-Threatening Hacks, Wired (November 24, 2015, 7:00 AM), http://www.wired.com/2015/11/medical-devices-that-are-vulnerable-to-life-threatening-hacks.


Id.

Id.


Id.


Id., see Consent Order, supra note 99.

http://www.bna.com/web-things-security-n57982073787/