THE UNIVERSITY OF CHICAGO
THE LAW SCHOOL

Internet of Things (IoT)

Risk Manager Checklist, U.S.

Salen Churi, Assistant Clinical Professor of Law
Bluhm-Helfand Director of the Innovation Clinic
The University of Chicago Law School

Harrison Hawkes and **Noah Driggs**, Students
The University of Chicago Law School Innovation Clinic

Foreword by:
Lex Baugh, Chief Executive Officer
North America General Insurance, AIG

Research made possible
through a generous grant from

AIG

RISK + INNOVATION | PART 4 IN A SERIES
www.aig.com/innovativetech

What's Inside

The Innovation Clinic at the University of Chicago Law School would like to thank the following, among others, during the creation of this checklist: Philip Kibler, Head of Cyber Risk Consulting at AIG; Cinthia Granados Motley, Partner at Sedgwick LLP; Lori S. Nugent, Shareholder – Cybersecurity and Crisis Management at Greenberg Traurig; Kingshuk K. Roy, Partner at Purcell & Wardrope, Chtd.; and Prashanthi Sudhakar, Innovation Manager at Schneider Electric.

Foreword

Lex Baugh
Chief Executive Officer
North America General Insurance, AIG

Something profound happened to the profession of Risk Management in only the last three years. New technology, and our readiness to embrace it, has made the vocation of underwriting far more complicated … and more exciting. The predictive power of so many sensors, analytics made possible by faster processing, and cloud connectivity – among other advances – are challenging the tools we underwriters have historically relied on. 33 years ago in my first week as an underwriter, I remember being issued a "triangle" that was supposed to help me calculate loss costs. It guided my best guess at what the future holds, based on what happened in the past. Checking the rear-view mirror will remain a fundamental check in the underwriting process. But, in order to focus on the unmapped road ahead, we need new tools and updated methods.

That is where this "checklist," and the partnership we have developed with Professor Churi and the University of Chicago Law School Innovation Clinic, comes in. **This whitepaper is the start of a new, practical guide to underwriting the future**. With collaborators like Professor Churi and his students, we can offer more conviction to institutions and inventors that rely on our counsel. No whitepaper will give us all the answers. But this one aims to assist readers in asking the right questions, in the right sequence, to analyze connected technology risk in the future.

I wish we had a crystal "triangle" that would tell us precisely where risks will shift, the magnitude, and how quickly in the hyper-connected, Internet of Things world we live in today. We don't. Truth is this will take several years, good and bad regulations, favorable and unfavorable court decisions, and private negotiations to fully sort out. But that doesn't mean we can't train ourselves to recognize the signals. There has never been a more complex time to be in Risk Management. That's what makes it so exciting. We are delighted to have the Innovation Clinic along as co-pilots for the journey – and hope you benefit from their insight as much as we have.

Introduction

Salen Churi
Assistant Clinical Professor of Law
Bluhm-Helfand Director of the Innovation Clinic
The University of Chicago Law School

With people, assets, and services becoming increasingly connected by software and hardware, physical risks are now directly intertwined with digital risks. In other words, every risk now or will soon contain some kind of technology risk. Whether we consider this a self-contained category or "peril" in itself, or a growing component of each risk category that already exists today, it is a phenomenon we cannot ignore.

IoT is injecting software into previously unconnected hardware, connecting everything from autonomous vehicles to smart thermostats, gathering data and generating insights in the cloud. Will autonomous vehicles become smart enough that we stop thinking of driver error as human error? Will errors made by artificial intelligence be treated more like products liability or vicarious liability? The law offers no clear answers to these questions…yet. Since IoT is so new, there is no definitive legal reference or concise volume of regulation on this topic. That's what makes this a perfect project for the University of Chicago Innovation Clinic: the Clinic strives to illuminate the shifting fault lines caused by new technologies and business models colliding with existing regulations and legal regimes. The mission of this checklist is not to provide theoretical research, but to generate practical, actionable insights for the executive who will confront the ambiguities of a changing technological paradigm.

This unique and untested challenge required us to reach outside our own walls, get onto the battle field, and partner with an insurance company that has a leading point of view, from the middle of it – AIG. Their support was invaluable in granting us access to perspective from the leaders who are on the front lines of these new innovations across multiple industries and different types of products, services, and business processes. I hope this document will enable risk managers to better navigate the challenges of integrating IoT related enhancements into products, services, operations and overall governance models. As with any cutting-edge legal or regulatory environment, there are no easy answers, but this checklist is meant to help the risk managers ask the right questions as IoT becomes increasingly pervasive in his or her business and products.

As the risk landscape continues to evolve from IoT's impact, so does the risk management model and how it operates. New applications applied to existing technologies and tools can enhance how old products are used and monitored. This phenomenon could allow the risk management community to bolster their core competencies, apply their findings and results for more precise pricing – and ultimately reduce risk. Along with these opportunities, there are obviously broader challenges – data usage and retention, cybersecurity, asset performance management, and how this can provide economic value for servicing clients.

This checklist is meant as an enabler to accelerate our digital future, allowing empowered readers to say "yes" with confidence that they have literally checked the relevant boxes. It is not meant to be a list of reasons to say, "no." AIG have been excellent partners for students in the Innovation Clinic and myself in this endeavor. In suggesting the idea of this practical guide and partnership, they are helping readers like you to empower the future in a safe and secure way.

This checklist offers a broad overview of the questions a risk manager should be asking. It focuses on generalized issues that risk managers across industries will face, but offers some particularized hypotheticals illustrating issues in some common IoT applications. These hypotheticals are not meant to be exhaustive, but by cross-referencing sections of the checklist, offer an example of ways risk managers might apply the insights of the checklist to their particular business.

Clearly, IoT's rapid rise and disruption has sparked important discussions around technology, operations and security. While the forthcoming innovation doesn't have a defined roadmap or set of solutions, guidance frameworks can help companies balance meeting business goals with uncertainty. As the IoT ecosystem becomes increasingly connected and companies implement complex technologies, collaboration and partnership is key.

Human vs. Machine Error: Industries Faced with the Challenge of Allocating Liability When Both Are Involved

I. Autonomous Vehicles

A driver was driving an autonomous vehicle that was in autonomous mode. The vehicle crashed into an oncoming semi as the latter turned left into the vehicle's path. The vehicle was in autonomous mode and the driver did not have his hands on the steering wheel despite being contractually obligated to do so, even when the vehicle is in autonomous mode. Both drivers were injured and both vehicles received substantial damage. Assume that the semi made a proper left-hand turn and that all fault rested with the driver and his autonomous vehicle.

Issues to consider:

a. What procedures are taken to determine whether the driver, vehicle manufacturer, autonomous system creator, or any other party is liable?
   i. See: Tort Liability VII

b. How is the liability allocated?
   i. See: Tort Liability I; Contract Liability I, II; Risk Transfer 3

c. What testing is completed after the accident?
   i. See: Tort Liability IV.2

d. What testing was previously completed?
   i. See: Tort Liability II, IV.1

e. What continuous testing and maintenance are completed?
   i. See: Tort Liability III, IV.2

f. Are any parties indemnified from liability?
   i. See: Risk Transfer 3

g. Was the driver properly informed of the risks of driving an autonomous vehicle?
   i. See: Tort Liability I; Contract Liability I, II

h. How enforceable is the driver's contractual obligation to keep his hands on the steering wheel when the vehicle is in autonomous mode?
   i. See: Contractual Liability I.3

i. Is that level of autonomous vehicle permitted in that jurisdiction?
   i. See: Jurisdictional Considerations; Regulatory Considerations

j. Is it known by third parties that autonomous vehicles operate in that jurisdiction?
   i. Tort Liability V

II. Home Automation

Your company sells an IoT thermostat that allows consumers to adjust the temperature of their home from their electronic devices. The thermostat is perpetually collecting data and sending it to your company, including the temperature in the home. One day, the thermostat registers a dramatic spike in room temperature due to a fire. Your thermostat is not a smoke detector.

Issues to consider:

a. Has your company incurred a duty to warn the consumers of the fire despite not being a smoke detector?
   i. See: Tort Liability I; Contracts Liability I
b. If your company has incurred a duty to warn, how do you give sufficient notice?
   i. See: Tort Liability I
c. What do your IoT device's terms of use state are the capabilities of your IoT device and are consumers aware that it is not a smoke detector?
   i. See: Contracts Liability I, II
d. Can your company contract out of such a duty to warn or is it inherent and unavoidable?
   i. See: Contracts Liability I, II

III. Industrial Control Systems[1]

A malicious third party hacks into your company's ICS and takes control of a robotic arm on an assembly line. The third party causes the robotic arm to swing erratically. The employee responsible for controlling the arm fails to enact safety protocols in order to properly shut down the arm, and the erratic robotic arm severely injures another employee.

Issues to consider:

a. What steps are being taken in the investigation of this incident?
   i. See: Tort Liability VII
b. How is liability allocated between the company, the negligent employee, and the malicious third party?
   i. See: Tort Liability I; Contract Liability I, II; Risk Transfer 3
c. Was this a foreseeable risk? If yes, why was it not prevented?
   i. See: Tort Liability II, III, IV
d. Have any peer organizations suffered similar breaches?
   i. See: Tort Liability IV.3
e. Was the injured employee aware of such a risk?
   i. See: Tort Liability V, VI
f. Was the injured employee given the opportunity to opt into such a risk?
   i. See: Tort Liability II.4; Contract Liability I, II (as they pertain to employees)

IV. Pharmaceuticals and Healthcare Devices

Your company manufactures and sells IoT pacemakers. The CEO of a Fortune 100 company secretly has pacemaker surgery that uses one of your pacemakers. A malicious third party hacks into the pacemaker to retrieve data on the CEO's health, which is poor, and releases these data to the public. The company's stock price subsequently falls, costing investors millions of dollars.

Issues to consider:

a. What steps are being taken in the investigation of this incident?
    i. See: Tort Liability VII
b. How liable is your company for both the release of the data and the drop in stock price, especially if the CEO and her company knew the pacemaker was an IoT device?
    i. See: Tort Liability I; Privacy and Data Security; Interoperability
c. How will the data from your IoT device be used in any subsequent lawsuits, either including or excluding your company?
    i. IoT Data in Litigation

V. Smart City

In a major metropolitan area, a malicious third party hacks into a commuter train's system and causes the train to crash into the next station at an accelerated speed, causing many injuries and property damage. It is later determined that the breach would not have occurred had the train's system been properly updated.

Issues to consider:

a. What steps are being taken in the investigation of this incident?
    i. See: Tort Liability VII
b. Who is liable for steps not being taken to properly update the train's system?
    i. See: Tort Liability III
c. When is the train system tested and updated?
    i. See: Tort Liability III, IV
d. Did the commuters know that the train on which they were riding was IoT? Did the train's owner incur a duty to warn the commuters?
    i. See: Tort Liability I, V, VI; Contract Liability II

VI. Unmanned Aerial Vehicles (a.k.a. UAV or drone)

Your company's drone flies near a fire in a business park while delivering a package to a consumer's office. The presence of the drone prevents firefighting helicopters from successfully extinguishing the fire. The fire subsequently spreads to other office buildings, resulting in millions of dollars in damage.

Issues to consider:

a. What further damage was caused due to our company's drone presence?
    i. See: Environmental Risks
b. How is the liability allocated for the additional property damage?
    i. See: Tort Liability I; Contract Liability I, II; Risk Transfer 3
c. What legal considerations are there, including from the Federal Aviation Administration, surrounding the operation of a drone, especially around first responders and their vehicles/equipment?
    i. See: Regulatory Considerations; Jurisdictional Considerations

The IoT Checklist

Tort Liability: Physical Harm and Product Liability[2]

I. Notice and Duty to Warn

1. How are consumers, employees, and/or independent contractors using our IoT device?
    a. Do consumers, employees, and/or independent contractors understand that our device is an IoT device?
2. What types of data from consumers, employees, and/or independent contractors is our IoT device collecting?[3]
    a. What notice do we give consumers, employees, and/or independent contractors of that data collection?
        i. Is that notice sufficient?
3. Have we incurred a legal duty to warn of potential risks of physical harm to consumers, employees, and/or independent contractors from whose IoT devices we have collected personally identifiable information (PII)?
    a. Have we incurred a legal duty to take steps to protect those individuals and their property through mitigation or elimination of those potential risks?
        i. If yes, what are those required steps?

II. IoT Device Design and Manufacturing Issues[4]

1. Was the IoT device always intended to be IoT?[5]
    a. If no, can we ensure that all steps were taken to properly transition the device to being IoT in nature?
2. When the IoT device was envisioned and put on the drawing board, was cybersecurity considered?[6]
    a. If so, how?
3. Do we meet best industry practices in the design and manufacturing processes of our IoT device?
4. Does the IoT device's design create a risk for physical harm to people, personal property, or real property?
    a. If yes, can we design out such risk with reasonable modification?
        i. If no, can we design out some of the risk with reasonable modification?
    b. If yes, are consumers required to opt into such a risk?
5. If we improve the design of our IoT device in order to reduce the risk of physical harm, how will consumers receive reasonable notice of the improvement?[7]
6. If we improve the design of our IoT device in order to reduce the risk of physical harm, how will consumers benefit from the improvement?[8]

III. Duty to Maintain[9]

1. Is our IoT device updateable?[10]
    a. If yes, how often is it updated in order to mitigate the risk of malicious attacks or involuntary release of PII?
    b. Can the updates be made automatically?
    c. If the updates cannot be made automatically, can they be made remotely?
        i. If yes, how are we providing notice to our consumers, employees, and/or independent contractors of the available updates?
        ii. How soon after the updates are available are we providing notice to our consumers, employees, and/or independent contractors?
        iii. How are we providing notice and are those methods sufficient?

2. Does our company incur a duty to maintain the IoT device after consumers purchase the device?
    a. If yes, what is that duty to maintain?
    b. If yes, for how long is that duty to maintain?
    c. If yes, how often is that duty to maintain?
3. Have our consumers incurred a duty to maintain the IoT device, especially with regard to third-party consumers?
    a. If yes, have we properly given our consumers notice of that duty to maintain?
4. For our in-house IoT devices, how long should each IoT device be in use before it is updated or even replaced?
    a. What in-house IoT devices are vulnerable to malicious attacks?

IV. IoT Device Testing Issues[11] [12]

1. **[Pre-launch testing]** What testing procedures, including cybersecurity testing, are completed before the IoT device goes to market?[13]
    a. What expert input is required before the IoT device goes to market?
        i. What other individuals and teams are required to provide input before the IoT device goes to market?
    b. Are we hiring computer security experts, such as "white hat" hackers, to try to hack into our IoT device?
        i. If yes, what has been the result of their efforts to hack into our IoT device?
            a. If they have successfully hacked into our IoT device, have we identified and eliminated the vulnerabilities?
    c. Is it possible for our device to not be an IoT device?
2. **[Ongoing testing]** What ongoing testing procedures are completed after the release of the IoT device?[14]
    a. What expert input is required during ongoing testing of the IoT device?
        i. What other individuals and teams are required to provide input during ongoing testing of the IoT device?
    b. Is the testing regular and scheduled?
        i. If yes, how often? (Recommendation: Regular testing completed every 6-12 months)
    c. Are tests carried out after known risks are identified through, for example, information sharing associations such as the Information Technology-Information Sharing and Analysis Center (IT-ISAC)?[15]
    d. How are the testing results used to create updates for the IoT device?
3. Have any IoT devices from other companies that are similar to ours been hacked?
    a. If so, under what circumstances (i.e., controlled environment or malicious) and with what result?
    b. How are we using the knowledge of these breaches to secure our own IoT devices?

V. Premises Liability[16]

1. Do our IoT device consumers incur a duty to warn third-party consumers or others on their property of the risks associated with our IoT device, including the collection of PII by the IoT device?
    a. If yes, have we given proper notice to our consumers of their incurrence of a duty to warn?
    b. If yes, could we also incur any liability for any harm that befalls a third-party consumer due to our consumer's failure to properly warn the third-party consumer?
        i. If yes, are we able to completely or partially absolve our company from such liability?
    c. If yes, what other parties within the stream of commerce could incur any liability for any harm that befalls a third-party consumer due to our consumer's failure to properly warn the third-party consumer?

VI. Products Liability

1. Does connecting our IoT device to consumers' networks increase the risk of their networks being accessed by malicious third parties?[17]
    a. If yes, can PII be accessed?[18]
    b. If yes, can we mitigate or eliminate that risk?
    c. If yes, do consumers understand that risk?
2. What physical harms to people, personal property, or real property could our IoT device potentially cause?
    a. Do we give proper notice to consumers about the physical risks?
    b. If possible, do we give instructions on how the consumer can mitigate this risk?[19]
3. For each type of physical harm to people, personal property, or real property that our IoT device could reasonably cause when reasonably used, have we determined which party or parties within the stream of commerce would be held fully or partially liable, i.e., how is the liability allocated?[20]

VII. Incident of Physical Harm[21]

1. For each type of physical harm that could reasonably occur when a consumer reasonably uses our IoT device, what are our investigation procedures of that incident?
    a. How is the scene documented and what data is collected?
    b. What experts are needed during the investigation procedures for each type of incident?
    c. What experts are needed during the litigation procedures?
2. What procedures are in place to determine whether the cause of the physical harm was a defect or due to misuse?
3. What documentation procedures are in place for the recording of all incidents of physical harm and near misses?
4. What kind of and how much liability do we incur if someone working under our company's direction is injured by one of our IoT devices?[22]

Contract Liability

I. Breach of Contract[23]

1. What duties have we incurred with regard to consumers because of the terms of the consumer contracts of our IoT devices?
2. What duties have we incurred given the IoT nature of our devices?
    a. Have we incurred any unintended duties to consumers?
3. Is it a reasonable expectation for consumers to follow all contractual requirements concerning the IoT device?
    a. If not, which requirements do we reasonable expect consumers to not follow?

II. Breach of Implied Warranty of Merchantability[24]

1. From our consumers' perspective, what are our IoT device's intended capabilities?
    a. Does our IoT device properly possess those capabilities?
    b. Do our consumers expect our IoT device to perform other capabilities?
        i. If yes, are these reasonable expectations based on our actions or the actions of others in the stream of commerce?
            a) If yes, can we properly disclaim responsibility to provide such capabilities?
2. Does our IoT device have other capabilities that our consumers do not desire or that might cause them to bring forth litigation?

IoT Data in Litigation[25]

1. What consumer data collected by our IoT device might be used in litigation?
    a. How could our IoT devices potentially affect consumers in litigation?
    b. Do we give consumers proper notice of the potential for our IoT devices to be used in litigation?
2. Do we have a process for finding and accessing data that might be discoverable?
3. What data retention requirements do we face with ongoing litigation?
4. What data retention requirements do we face without ongoing litigation?

Intellectual Property (IP)

1. What IP does our IoT device or software implicate?
2. What open-source IP do we use?
    a. What are the terms of these open-source licenses?
    b. What non-disclosure agreements (NDAs) have we made with third parties and how enforceable are they?[26]
        i. What potential legal liabilities or risks to IP are not protected by the NDAs?
3. What IP might we need to license in order to make our IoT device interoperable?
4. How do recent IP-related court decisions apply to our company and IoT devices?

Risk Transfer and Contracting Between Multiple Parties

1. Does our organization have expertise in all of the types of licenses that we now utilize (i.e., software as well as traditional supplier contracts)?
2. How do our contracts allocate ownership of data and embedded software?
3. How do our contracts allocate risk between counterparties and insurers?
    a. What indemnity provisions do our contracts include that indemnify our company for any liability, such as privacy violations or physical harm?[27]
        i. How does that risk pass from our company onto a third party, such as a vendor, distributor or manufacturer?
        ii. Is the indemnity language enforceable in the jurisdiction in which litigation is pending?
        iii. What insurance coverage will apply?
    b. What is covered in our insurance contracts?
4. Does the consumer contract for our IoT device contain a general release or limitation on liability?
5. How do our contracts with employees and independent contractors address privacy and ownership issues?

Privacy and Data Security

1. What types of data are being collected by and stored on consumers' IoT devices?[28] Is it PII? (Examples include precise geolocation, financial account numbers, credit history, health information, demographics, personality types, sleep patterns, driving habits, general habits, moods, levels of exercise, physical activities, consumer preferences, and daily routines and schedules.)[29]
    a. What types of consumer data are we inadvertently collecting?
    b. How much data are we collecting from consumers' IoT devices?[30]
        i. Do we need to collect all of that consumer data? Do our business needs require all of that consumer data?
        ii. Are we developing "policies and practices that impose reasonable limits on the collection and retention of consumer data"?
        iii. Are consumers required to opt in for data to be collected from them?
            1. Can consumers choose what information and data to release?
    c. What would happen if a malicious third party accesses that data?
        i. How can a malicious third party use that data, either directly or indirectly?
            1. What interpretations can they make from the data collected?[31]
        ii. What steps are we taking to prevent such data breaches?
    d. What vulnerabilities exist in our privacy and data security processes?
2. **[In-house considerations]** What types of data are being collected from our employees and independent contractors and stored on our in-house IoT devices?
    a. Do we give our employees and independent contractors proper notice of this data collection?
    b. Are our employees and independent contractors required to opt into this data collection?
    c. How do the data collection procedures and notifications differ between employees and independent contractors?

3. **[In-house considerations]** To what networks are our in-house IoT devices connected?[32]
    a. What data are stored on those networks?
        i. What would happen if a malicious third party accessed those data?
    b. What vulnerabilities currently exist in those networks?
        i. What potential vulnerabilities are there that do not currently exist?
4. **[In-house considerations]** Have the IoT devices or networks of any of our peer organizations been accessed by malicious third parties?[33]
    a. If yes, to what extent?
    b. If no, what steps are they taking to prevent such breaches?
5. Do our IoT devices come with privacy notices for consumers?[34]
    a. When should consumers receive notice of our IoT device's privacy policy?
        i. Where should we place the privacy policy, e.g., in the device's package, on the app, on the website?
    b. Does our privacy policy read more like an Internet website privacy policy or an IoT device privacy policy? I.e., does the privacy policy "seem to have been shaped by the needs and expectations relevant to the normal Internet, not the Internet of Things"?[35]
6. Are we being transparent with consumers about the amount and types of data that we are collecting from their IoT devices?[36]
    a. Are we being transparent with consumers about who will view the data?
    b. Will the collection of data alter consumers' practices in a negative way?[37]
7. Federal-level considerations: Best practices as determined by the Federal Trade Commission (FTC) and other federal guidance:[38]
    a. Overall:
        i. Do we have a comprehensive security program that is reasonably designed to (1) address security risks related to the development and management of new and existing IoT devices, and (2) protect the privacy, security, confidentiality, and integrity of PII?
            1. Does the program contain administrative, technical, and physical safeguards appropriate for:
                a. Our company's size and complexity,
                b. The nature and scope of our company's activities, and
                c. The sensitivity of the IoT device's function or the PII?
    b. Data security:
        i. Do we use an intrusion detection system or file integrity monitoring?
        ii. Do we monitor traffic coming across our firewalls?
        iii. Do we provide data security training to our employees?
            1. If yes, does it meet best industry practices?
        iv. Do we delete collected consumer data when they are no longer needed?
            1. If yes, how soon after the data become unnecessary are they deleted?[39]
        v. Do we know whenever there has been an attempt, either successful or unsuccessful, to steal data or maliciously attack our consumers or us?
        vi. When there is an intrusion or malicious attack, what investigative procedures have we implemented to identify the source?
            1. What procedures have we implemented to ensure such an intrusion or malicious attack is not repeated?

c. Process documentation:
    i. Is the content and implementation of our comprehensive security program fully documented in writing?
        1. If yes, are written copies of our comprehensive security program sufficiently disseminated throughout our organization?
d. Consumer notice and choice:
    i. Does the consumer data collected by the IoT device align with the consumers' reasonable expectations of data collection, and are the "data uses, by both [us] and third parties, generally consistent with consumers' reasonable expectations"?[40]
        1. Note: If yes, then the Commission states that "companies should not be compelled to provide choice before collecting and using consumer data."[41]
        2. If no, then are we allowing consumers to choose whether or not they want their data collected?
        3. Are we being transparent as to what data we collect and who can view said data?
    ii. Do we *clearly* and *conspicuously* notify consumers when a software update is available or when we are aware of reasonable steps that consumers could take to mitigate a security flaw?
        1. Does the notice explain how to install the software update or otherwise mitigate the security flaw?
        2. Does the notice explain the risks to the consumers' IoT devices or PII if the consumers choose not to install the available software update or take the recommended steps to mitigate the security flaw?
        3. Is notice provided through at least one of the following means?
            a. Posting of a clear and conspicuous notice on at least the primary, consumer-facing website of ours, and, to the extent feasible, on the user interface of any IoT device that is affected.
            b. Directly informing consumers who register, or who have registered, an IoT device with us, by email, text message, push notification, or another similar method of providing notifications directly to consumers.
            c. Informing consumers who contact us to complain or inquire about any aspect of the IoT device they have purchased.
        4. In the case of a security flaw that can pose a risk to a consumer's safety or finances, is there a centralized security measure to mitigate this?[42]
    iii. Do we provide consumers with an opportunity to register an email address, phone number, device, or other information during the initial steps or configuration of an IoT device in order to receive the security notifications required?
e. Collecting data from children:
    i. Are we adhering to the Children's Online Privacy Protection Act of 1998 (COPPA) in our collection of data from children?
f. Are there any other agency-specific considerations by industry, e.g., HIPAA or FCRA?

8. State-level considerations:
    a. Are we aware of the data breach notification laws in the states in which we operate?
    b. Do our states have additional privacy laws?
    c. What lesser-known privacy statutes exist that might apply to our IoT devices?
9. Do we have a process to keep abreast of new agency guidance?

Cybersecurity[43]

1. How attractive to hackers are the data that we collect from consumers' IoT devices?
    a. Are the data directly attractive to hackers, e.g., financial accounts numbers or other PII?
    b. Are the data indirectly attractive to hackers, e.g., the lack of use of home appliances for a few days signaling that the consumers are out of town?
2. **[Pre-breach considerations]** When compared to our peer organizations, are we acting reasonably and prudently in keeping up-to-date with the known best industry practices concerning the privacy and data security of our IoT devices?
    a. Are we a member of an information sharing association, such as the Information Technology-Information Sharing and Analysis Center (IT-ISAC)? (Note: The purpose of such associations is for peer organizations to share information.)[44]
    b. At least annually, are we conducting a review of our practices to ensure proper privacy and data security?
        i. Do we have a cross-functional group from within the company whose purpose is to identify and assess the vulnerabilities in our privacy and data security?
    c. Per best industry practices, are our employees properly trained to prevent or recognize breaches?
    d. Are we consulting independent experts, such as legal counsel and forensic experts, to determine if our practices are sufficient per current regulatory requirements and best industry practices?
    e. What testing is being conducted on our privacy and data security practices?
    f. Are we designing privacy and data security into our IoT device?
3. **[Post-breach considerations]** After a breach of one of our IoT devices occurs, what is our incident response plan?
    a. How quickly are we identifying the vulnerabilities in our privacy and data security practices?
        i. How quickly are we eliminating, or at least sufficiently mitigating, those vulnerabilities?
        ii. What other similar vulnerabilities do we have that may pose material risks?
    b. How transparent are we being with regulators about the steps we are taking to rectify the issue?

Contracting with Third Parties[45]

1. Are we working in collaboration with third parties? Do we have a good working relationship with these entities?
    a. If yes, in what capacity are we collaborating?
    b. If yes, are we sharing our consumers' data with those third parties?
        i. If yes, what agreements have we made with those third parties concerning data sharing?
        ii. If yes, what data are being shared and for what purposes?
        iii. If yes, how are we ensuring that those third parties are protecting our consumers' data?
        iv. If yes, how are we ensuring that we are only sharing our consumers' data that those third parties require?
2. How do we know when third parties with whom our IoT devices are connected have been maliciously attacked?

Jurisdictional Considerations[46]

1. What jurisdictions are we targeting to implement our innovation?
    a. What jurisdictions are progressive and willing to accept the application of such innovation?
    b. For each jurisdiction in which we operate or wish to operate, what legislative or public pushback has there been against the implementation of our IoT device(s)?
2. What IoT-specific jurisdictional requirements exist?

Regulatory Considerations[47]

1. How are we keeping abreast of any new regulations or policy changes? (Note: Keeping up-to-date with new regulations is especially important if our industry is heavily regulated.)
2. Are we adhering to the current industry regulations?

Environmental Risks[48]

1. Are there any potential environmental risks because of the use of our IoT device?
    a. If yes, what are they and can we eliminate or mitigate those environmental risks?
2. Do consumers need to dispose of our IoT device in a specific manner to avoid any environmental risks, such as improper disposal of hazardous material?
    a. If yes, what is the proper disposal method and is it reasonable for consumers to adhere to that disposal method?
3. Have we given our consumers proper notice of any environmental risks and proper disposal methods so as to absolve our company from any potential liability?

Health Risks[49]

1. Are there any health risks associated with our IoT device, especially risks that do not correspond with overt physical harm?
    a. If yes, have we given our consumers proper notice of those health risks so as to absolve our company from any potential liability?
2. Have we properly notified consumers of all safety features of our IoT device?

Interoperability

1. When does our device become an IoT device that is connected to the Internet?
2. Have we properly allocated all liability associated with the interoperability of our IoT device?

Business Continuity

1. Does our company's business continuity plan include IoT considerations?
2. What IoT processes are used to support business operations? (Examples include IoT management, priority responses, labs and data centers, and go live/patch management.)
3. How is our company currently using IoT devices?
    a. What IoT devices are used within the company?
    b. What IoT devices are sold to consumers?
4. What other IoT devices is our company planning on using or selling in the near future?
5. What are the IoT-related considerations included in our business continuity plan?
    a. Are they sufficiently comprehensive?
6. What kind of analysis do we perform to determine all of the possible outcomes of IoT-related risks and the probability that each outcome will take place?
    a. What are the most material IoT-related outcomes that we must prevent?
        i. How are we allocating resources to prevent these IoT-related outcomes from occurring?
        ii. If each these IoT-related outcomes were to occur, what steps would we take to mitigate the damage?
7. Do the third-party companies that are connected to our IoT devices have business continuity plans?
    a. How much do we rely on the continuity of each of those companies?

Citations

1 Strong recommendation: Speak with an expert who has sufficient engineering knowledge and experience to speak to the specific legal risks surrounding cybersecurity and ICSs.

2 Overall concepts derived from comments by Mark Geistfeld, Sheila Lubetsky Birnbaum Professor of Civil Litigation at NYU School of Law, at a panel at the Eighth Law and Information Society Symposium, Fordham University School of Law on March 14, 2014. Link: https://www.youtube.com/watch?v=ZF9EOon3H90.

3 Overall concepts derived from p. 29 of FTC Staff Report, "Internet of Things: Privacy & Security in a Connected World," January, 2015.

4 Overall concepts derived from comments by Mark Geistfeld, Sheila Lubetsky Birnbaum Professor of Civil Litigation at NYU School of Law, at a panel at the Eighth Law and Information Society Symposium, Fordham University School of Law on March 14, 2014. Link: https://www.youtube.com/watch?v=ZF9EOon3H90.

5 Based on comments from Philip Kibler, Head of Cyber Risk Consulting at AIG.

6 Based on comments from Philip Kibler, Head of Cyber Risk Consulting at AIG.

7 Overall concepts derived from p. 29 of FTC Staff Report, "Internet of Things: Privacy & Security in a Connected World," January, 2015.

8 Overall concepts derived from p. 29 of FTC Staff Report, "Internet of Things: Privacy & Security in a Connected World," January, 2015.

9 Based on conversations with Kingshuk Roy, Partner at Purcell & Wardrope, Chtd.

10 Based on comments from Philip Kibler, Head of Cyber Risk Consulting at AIG.

11 Based on conversations with Kingshuk Roy, Partner at Purcell & Wardrope, Chtd.

12 Based on comments from Cindy Motley, Partner at Sedgwick LLP, during a conversation on September 1, 2016.

13 Based on comments from Philip Kibler, Head of Cyber Risk Consulting at AIG.

14 Based on comments from Philip Kibler, Head of Cyber Risk Consulting at AIG.

15 Based on comments from Cindy Motley, a partner at Sedgwick LLP, during a conversation on September 1, 2016.

16 Based on conversations with Kingshuk Roy, Partner at Purcell & Wardrope, Chtd.

17 Overall concepts derived from pp. 27-28 of FTC Staff Report, "Internet of Things: Privacy & Security in a Connected World," January, 2015.

18 Overall concepts derived from Product Liability Advocate article "The Internet of Things: The Inevitable Collision with Product Liability" written by Michael O'Brien, Partner at Wilson Elser Moskowitz Edelman & Dicker LLP, July 2015.

19 Overall concepts derived from Product Liability Advocate article "The Internet of Things and the Inevitable Collision with Products Liability PART 2: One Step Closer" written by Michael O'Brien, Partner at Wilson Elser Moskowitz Edelman & Dicker LLP, July 2015.

20 Based on conversations with Kingshuk Roy, Partner at Purcell & Wardrope, Chtd.

21 Based on conversations with Kingshuk Roy, Partner at Purcell & Wardrope, Chtd.

22 Overall concepts derived from The Legal Intelligencer article "Workers' Comp Case Could Deal Blow to Franchise Model" written by Ben Seal, Reporter, May 2016.

23 Based on conversations with Kingshuk Roy, Partner at Purcell & Wardrope, Chtd.

24 Based on conversations with Kingshuk Roy, Partner at Purcell & Wardrope, Chtd.

25 Overall concepts derived from American Bar Association article titled "The 'Internet of Everything': What It Means for Lawyers," written by Sharon D. Nelson, Attorney and President of Sensei Enterprises Inc., and John W. Simek, Vice President of Sensei Enterprises Inc.

26 Overall concepts derived from comments made by Prashanthi Sudhakar, Innovation Manager at Schneider Electric, during a conversation on August 30, 2016.

27 Based on conversations with Kingshuk Roy, Partner at Purcell & Wardrope, Chtd.

28 Overall concepts derived from p. 26 of FTC Staff Report, "Internet of Things: Privacy & Security in a Connected World," January, 2015.

29 Overall concepts derived from pp. 30-31 of FTC Staff Report, "Internet of Things: Privacy & Security in a Connected World," January, 2015.

30 Overall concepts derived from p. 49 of FTC Staff Report, "Internet of Things: Privacy & Security in a Connected World," January, 2015.

31 Overall concepts derived from comments made by Prashanthi Sudhakar, Innovation Manager at Schneider Electric, during a conversation on August 30, 2016.

32 Overall concepts derived from pp. 26-27 of FTC Staff Report, "Internet of Things: Privacy & Security in a Connected World," January, 2015.

33 Overall concepts derived from pp. 26-27 of FTC Staff Report, "Internet of Things: Privacy & Security in a Connected World," January, 2015.

34 Overall concepts derived from pp. 146, 163 of Texas Law Review article titled "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent," written by Professor Scott Peppet, Professor of Law at University of Colorado Law School.

35 Quote and overall concepts from pp. 146, 163 of Texas Law Review article titled "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent," written by Professor Scott Peppet, Professor of Law at University of Colorado Law School.

36 Overall concepts derived from p. 68 of FTC Staff Report, "Internet of Things: Privacy & Security in a Connected World," January, 2015.

37 Overall concepts derived from Law 360 article "The Internet Of Things: Liability Risks For Tech Cos." written by Michael O'Brien, Partner at Wilson Elser Moskowitz Edelman & Dicker LLP, July 2015.

38 Analogized from non-IoT, Internet cases: *In the Matter of LabMD, Inc.*, Docket No. 9357, opinion issued on July 28, 2016; In the Matter of ASUSTeK Computer Inc., Docket No. C-4587, opinion issued on July 18, 2016.

39 Overall concepts derived from p. 61 of FTC Staff Report, "Internet of Things: Privacy & Security in a Connected World," January, 2015.

40 Quote and overall concepts from p. 56 of FTC Staff Report, "Internet of Things: Privacy & Security in a Connected World," January, 2015.

41 Quote and overall concepts from p. 56 of FTC Staff Report, "Internet of Things: Privacy & Security in a Connected World," January, 2015.

42 Overall concepts derived from Law 360 article "The Internet Of Things: Liability Risks For Tech Cos." written by Michael O'Brien, Partner at Wilson Elser Moskowitz Edelman & Dicker LLP, July 2015.

43 Based on conversation with Lori Nugent, Shareholder - Cybersecurity and Crisis Management at Greenberg Traurig, during a conversation on September 13, 2016.

44 Based on comments from Cindy Motley, Partner at Sedgwick LLP, during a conversation on September 1, 2016.

45 Overall concepts derived from comments made by Prashanthi Sudhakar, Innovation Manager at Schneider Electric, during a conversation on August 30, 2016.

46 Overall concepts derived from comments made by Prashanthi Sudhakar, Innovation Manager at Schneider Electric, during a conversation on August 30, 2016.

47 Based on conversations with Kingshuk Roy, Partner at Purcell & Wardrope, Chtd.

48 Based on conversations with Kingshuk Roy, Partner at Purcell & Wardrope, Chtd.

49 Based on conversations with Kingshuk Roy, Partner at Purcell & Wardrope, Chtd.