Legal Issues Surrounding the Internet of Things and Other Emerging Technology

ACC Houston Chapter Meeting
September 12, 2017

Jonathan Ishee
Vorys Sater Seymour and Pease, LLP

Dean Fisher
RigNet
Overview

• Internet of Things (“IOT”)
  — What is IOT
  — Privacy and Security Concerns
  — Mitigation Strategies
• Other Emerging Technology
  — Blockchain
• Questions
What is IOT

• Internet of Things revolves around increased machine-to-machine communication; it’s built on cloud computing and networks of data-gathering sensors; it’s mobile, virtual, and instantaneous connection.*

• In a general sense connecting any device with an on and off switch to the Internet (and/or to each other).*

— Most people think of consumer appliances that are “smart”

*A Simple Explanation Of 'The Internet Of Things‘ Forbes, May 13, 2014*
What is IOT – Why Should I Care?
What is IOT – Why Should I Care?

• Increased Use of Sensors for Data Collection
• Data Analytics
• Network Connectivity for Software/Equipment Updates
• Increase Use of Cloud Based Storage
• Connectivity Without Incorporating Privacy or Security
• Patchwork of Regulatory Oversight
Privacy and Security Concerns

Hackers target DOT road signs in Charlotte with vulgar messages, Jul 17, 2017
Privacy and Security Concerns (cont’d)

465,000 Pacemakers Recalled on Hacking Fears, ABC Radio
September 3, 2017

Was Russian hacking of Ukraine's power grid a test run for U.S. attack?
CBS News June 23, 2017
Privacy and Security Concerns (cont’d)

Wellness Apps Evade the FDA, Only to Land in Court, Wired April 03, 2017
ISSUES RAISED BY INCREASED PRIVACY RISK

• Ensuring users have sufficient control, as they often cannot review the data before its “collection” or “publication”

• Automatic or default communication without the user being aware. The difficulty of controlling the flow of data in these situations

• Lack of awareness by individuals of a device’s enhanced capabilities, and the quality of their consent
ISSUES RAISED BY INCREASED PRIVACY RISK

• Insufficiency of classical consent mechanisms and the need for new methods of consent

• Risk of stakeholders using the data beyond the original specified purposes, particularly with the rise of Artificial Intelligence applications

• IoT’s ability to determine habits, behaviors and daily activities of individuals
ISSUES RAISED BY INCREASED PRIVACY RISK

• Limits on the ability to remain anonymous while using IoT devices or services

• Vulnerability of devices to “re-identification” attacks where users can be identified by unauthorized users

• Risk of turning everyday object into a privacy and security target

• Battle between battery efficiency and the security of communications resulting in a lack of encrypted data flows
LAW AND REGULATIONS ALWAYS LAGS BEHIND TECHNOLOGY

No uniform regulatory approach, so providers of IoT devices will have to comply with differing regulations in each state, province, or country. However:

Senators Mark Warner (D-VA) and Cory Garner (R-CO), co-chairs of the Senate Cybersecurity Caucus, introduced legislation last month under “The Internet of Things Cybersecurity Improvement Act of 2017” (S. 1691) to require all devices purchased by the U.S. Government to meet certain minimum requirements.
Mitigation Strategies

• Risk Assessments

• Contractual Agreements with Outside Vendors

• Cyber Liability Insurance
Mitigation Strategies – Risk Assessments

• Testing of Product Before Implementation

• Exercise Should Include Assessments of the Following
  – Strategic Risks
  – Tactical Risks
  – Security Risks
    • Information Technology
    • Human Engineering
  – Safety Risks
Risk Assessments – Strategic and Tactical Risk

Figure 4-1: Tiered Risk Management Approach (NIST SP 800-37)

- Multitier Organization-Wide Risk Management
- Implemented by the Risk Executive (Function)
- Tightly coupled to Enterprise Architecture and Information Security Architecture
- System Development Life Cycle Focus
- Disciplined and Structured Process
- Flexible and Agile Implementation

TIER 1
ORGANIZATION (Governance)

TIER 2
MISSION / BUSINESS PROCESS (Information and Information Flows)

TIER 3
INFORMATION SYSTEM (Environment of Operation)

STRATEGIC RISK

TACTICAL RISK
Risk Assessments – Security and Safety

Security risk (includes breach of data and systems security and reduction of effectiveness)

Security risk with safety impact

Safety related risk (ISO 14971)
Mitigation Strategies – Contractual Agreements

Sample Language in Purchase Agreements:

• Product does not contain components with any known security vulnerabilities or defects listed in the National Institute of Standards and Technology’s (“NIST”) National Vulnerability Database or a similar database identified by the purchaser;

• Include components that are capable of receiving “properly authenticated and trusted” patches from vendors;

• Utilize industry-standard technology and components for communication, encryption, and interconnection with peripherals; and

• Do not include “fixed or hard-coded passwords” to receive updates or enable remote access.
Mitigation Strategies – Contractual Agreements (cont’d)

• A requirement to notify the purchaser of any “known security vulnerabilities or defects subsequently disclosed to the vendor by a security researcher” or when a vendor becomes aware of such a vulnerability during the term of the Agreement.

• Update, replace, or remove, in a timely manner, vulnerabilities in software and firmware components in a properly authenticated and secure manner. This includes a requirement to provide information to the purchaser regarding the manner for such updates, as well as a timeline and formal notice when ending security support.
Contracting Recommendations—
Industry Perspective

• Consents and Opt Outs.
• Insist on Data Minimization and De-
  identification.
• Health Care Data – an example of where special
care is needed for areas of sensitive data
• Location Data. Limit device fingerprinting by
disabling wireless devices when not in use or
using random identifiers to prevent a persistent
identifier being used for location tracking.
• Transparency and Fair Processing. Disclosing the purposes for processing information from the individual.

• Security. Many devices lack encryption because of device design and cost control. Insist on encryption and immediate notification of any security vulnerability.

• Standardization and data portability. Restrict sharing of your data without your consent.
Contracting - Industry Perspective

• Most of us are risk managers when it comes to contracting. An IoT agreement brings increased risks to data privacy and security.

• Involve your security people to evaluate any new network devices that may have access to your systems.

• Foster a culture of security, adopt a defense-in-depth approach that incorporates security measures at several levels.
Contracting- Industry Perspective

• Train your people about network security issues, phishing scams, etc. as people are the weakest link in any security system. Rotate your passwords frequently.

• Take a risk-based approach – use greater security protocols where your more sensitive data is at risk. Ask about your Provider’s plans to address a security flaw or breach.
Mitigation Strategies – Cyber Insurance

• Generally Two Types
  — Cyber Liability Insurance
  — Technology Errors and Omissions

• Cost Varies Greatly Based on Industry and Insurer’s Underwriting Experience

Important to Know What is Covered and What is Not
Mitigation Strategies – Cyber Liability Insurance

• Covers Breaches of Sensitive Customer Information and Associated Costs
  — Credit Reporting
  — Notification Costs
  — Penalties imposed by state regulators

• Note: Does not cover property loss sustained by the business
Mitigation Strategies – Technology E&O Coverage

• Covers **Providers** of Technology Services or Products
  — Liability and property loss coverage
OTHER EMERGING TECHNOLOGY – BLOCKCHAIN
Blockchain – What is It?

A Shared Ledger Technology Allowing Participants in the Network to View the Record

• Components
  — Participants
  — Ledger
  — “Smart” Contract
Blockchain – What is It? (cont’d)

• Historically Used in Digital Currency
Example of Blockchain Ledger

<table>
<thead>
<tr>
<th>Number</th>
<th>Hash</th>
<th>Time</th>
<th>Transactions</th>
<th>Total BTC</th>
<th>Size (kB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>356987</td>
<td>141a6f95b2...</td>
<td>2015-05-18 13:28:14</td>
<td>1714</td>
<td>17353.00313324</td>
<td>749.227</td>
</tr>
<tr>
<td>356986</td>
<td>13cfe723ec...</td>
<td>2015-05-18 13:11:53</td>
<td>2114</td>
<td>23805.24520712</td>
<td>749.204</td>
</tr>
<tr>
<td>356985</td>
<td>1128aa2601...</td>
<td>2015-05-18 12:27:49</td>
<td>594</td>
<td>6119.90095486</td>
<td>392.306</td>
</tr>
<tr>
<td>356984</td>
<td>140b0f27b9...</td>
<td>2015-05-18 12:20:14</td>
<td>1087</td>
<td>7849.33374079</td>
<td>544.102</td>
</tr>
<tr>
<td>356983</td>
<td>d1ea5bc1c7...</td>
<td>2015-05-18 12:08:01</td>
<td>830</td>
<td>7799.27270534</td>
<td>455.006</td>
</tr>
<tr>
<td>356982</td>
<td>76634b52be...</td>
<td>2015-05-18 11:58:42</td>
<td>221</td>
<td>1706.08443753</td>
<td>152.745</td>
</tr>
<tr>
<td>356981</td>
<td>ab5a634167...</td>
<td>2015-05-18 11:57:28</td>
<td>756</td>
<td>7245.57902445</td>
<td>372.38</td>
</tr>
<tr>
<td>356980</td>
<td>b780d34ab0...</td>
<td>2015-05-18 11:46:36</td>
<td>383</td>
<td>4623.1382688</td>
<td>430.319</td>
</tr>
<tr>
<td>356979</td>
<td>110a166e82...</td>
<td>2015-05-18 11:41:08</td>
<td>2276</td>
<td>19539.64880577</td>
<td>999.931</td>
</tr>
<tr>
<td>356978</td>
<td>4591865561...</td>
<td>2015-05-18 11:01:41</td>
<td>1259</td>
<td>12186.20279942</td>
<td>722.931</td>
</tr>
</tbody>
</table>
Blockchain Benefits

• Benefits

  — Every Transaction becomes part of the record and can be reviewed by individuals with the appropriate permissions

  — Relevant information can be shared with others based on role based access

  — Distributed ledgers are shared and updated in real-time across a group of participants
Blockchain is Not

• A Messaging Solution

• Suited for transactions Involving One Participant

• For High Value or Milestone Transactions

• A Place to Store Confidential Information
Blockchain – Non Financial Use Cases

• Health Information/Data Exchange

• Supply Chain Provenance and Traceability

• Payment/Claims Processing
  — Situations in which there is a third party payor

• Food Safety
Blockchain Use Case – Food Safety

• More than 1,000 foodborne outbreaks investigated by state and local health departments are reported each year, according to the CDC

• Roughly 48 million people are afflicted annually, with 128,000 hospitalized and 3,000 dying.
Blockchain Use Case– Fact Pattern

You are a grocery store that has just been informed that a pork product that you sell has been recalled due to contamination issues at a particular plant with a particular batch.

What Do You Do?
Blockchain Use Case– Food Safety
Questions

Please Contact:

Jonathan Ishee, JD, MPH, MS, LLM
jishee@vorys.com
713-588-7037