The Internet of Things: Cyber Issues for AGs

Michael A. Aisenberg, Esq.
Senior Fellow, GWU Center for Cyber & Homeland Security
Chair, ABA Information Security Committee

NAAG Summer Meeting. Huntley Lodge, MT.
What’s Coming

• Posture of emerging norms for IoT
• The context of IoT: what is new? Different?
• Risks from IoT device use; stakeholders
• Legal theories of cyber liability generally
• Bases of IoT Civil Liability
• Sources of IoT Device Liability: What might go wrong?
• Federal Statutory Environment
• State level interests
• Paths forward for states
• Bedtime reading
PC Week:
Implantable medical devices can be hacked to harm patients

The way to a man's heart is through his pacemaker's security flaws, researchers say
IOT Norms in a Nutshell: Standards, Regulation & Statute

- **Basic Principles:** A crime is still a crime, even if the instrument is an implanted cardiac defibrillator…
- **Criminal use of a connected device:** no need to define a new “crime”
  - IOT is no different from the advent of Wireless or the Cloud to the “Cyber Ecosystem
  - 'Bad behavior’ is still bad behavior, irrespective of the technological nuance.
    - (DISTINGUISH CAPACITY TO DETECT AND FORENSICALLY SUPPORT PROSECUTION—THAT MAY BE “NEW”)
  - Exception: where the specific technology materially changes the risk and requires redefining an element of the offense:
    - e.g. If use of a “connected medical device” to commit a battery on a person is substantively different from other batteries using a “weapon”, because act may not be detectable; or the criminal is less detectable
- **Civil Liability for improper design, manufacture or use of a connected device**
  - As with Wireless devices and Cloud, civil liability for reckless design or use of an IOT device may add a new basis for legal liability, determined in a law suit; compensated by new insurance products
  - So far, only evidenced in sector best practices statements & industry standards, not law
- **Relation to Federal regulation**
  - Example: connected medical: FDA Conducts pre-market and post market assessment, certification for connected medical devices
  - 2015 *Wyndham Hotels* decision establishes obligation on data **custodian to use reasonable security to protect consumer** data; may become principle on broad economy-wide **duty of wired steward to customer**, enforced by FTC “unfair consumer practice” provisions of Section 5 of FTC Act.
Context

- **Not new** (Like “cloud”—which is “time sharing”); Many monikers for old wine in new bottles
  - “IoT” “ICS” “CPS” “SCADA”:
  - Hollerith card patent::”The Art of compiling Statistics”: 1884

- **What IS new are:**
  - **SCOPE** (Global)
  - **SCALE** (IP v4=4.3 billion addresses; IPv6= $3.4 \times 10^{38}$ addresses (7.9\times10^{28} times as many as IPv4) (Essentially: **inexhaustible**)
  - **VALUE** (Gartner 2010 $2$ trillion; 2015 $4-5$ trillion; 2017 est. by 2025 $10-15$ trillion)

- Thus, the “Willie Sutton” issue: IoT is where the money is, so it’s where the bad guys will go.
  - Even at $4$ trillion economic value, IoT *rounding errors and accounting mischief could be OM $10-100$ billion dollars !!!!
  - This funds a lot of crime, terrorism and illegal R&D

- **Much activity/little progress:** over 200 separate IOT standards efforts under way
Where do the risks lie?

Bases of IOT Liability include:

• **Users: Patients, Drivers, Passengers**
  – Physical Harm
  – Emotional Distress
  – Privacy (HIPPA disclosure violations)
  – Economic loss

• **Providers and Vendors**
  – Financial risk: civil liability
  – Business reputational risk/brand
    • Criminally negligent manufacturing or use
    • Medical malpractice
Legal Theories of “Cyber” Liability Generally

- **Parties in Interest (“stakeholders”) and sources of risk**
  - **Providers:** Patients, 3rd Party Care givers, Device vendor/service provider,
    - Varies by venue-Self-administered, home, clinic, in-patient facility
    - Physician: primary care, specialist, ancillary (anesthesia; consultant
  - **Technologists:** vendor, component manufacturer, 3rd party provider to venue (contract device operator)
  - **Consumables:** drugs, fluids, reagents, dyes

- **Theories of Liability**
  - Distinguish *Contractual Responsibility* from *Financial Accountability*
  - HHS Medical Device Amendments of 1976: assigning financial accountability irrespective of provable legal responsibility
Bases of IOT Civil Liability

**Device production**
- Emerging new standards of vendor due diligence for manufacture, including
  - **System design**: include consideration of scale, scope and complexity, as well as “hiding in plain sight”
    - Obligation on vendor to appreciate use environment
  - Obligation on vendor to police their own **supply chain**: complex components—microprocessors
    - Assuring security, integrity in use, rather than merely identifying defects
    - Exception: faulty firmware or other embedded software. Opacity requires extensive, **extraordinary testing**.
    - Sources of best practice/standards: Industrial Internet Consortium, and individual sectors (e.g. HL7/HIMMS for medical devices)

**Device use**
- Obligations on user entity: train and police service provider/user
- Customer obligation, via contract, to police their own supply chain
- Insiders are continuing source of risk, liability and thus require due diligence
- Burden on user/provider to qualify personnel deploying devices
  - E.g in health care, nurses, specialty therapists, and other staff engaged in direct contact/operation of connected medical devices in the course of patient care
Theories of Civil Liability for defective IoT Devices

1. **Privacy/HIPPA** -- unconsented access to PII
   i. Data Loss due to "breach"
   ii. Failure to meet test of "data stewardship"

2. **Unfair/deceptive consumer practice**: FTC/ **Wyndham** lack of cyber security as an unfair or deceptive consumer practice (§5 FTC Act)

3. Breach of contract

4. Unjust enrichment

5. **Bailment** (of valuable personal/organizational data)
Federal Statutory Environment

- **2 Preemptive Regulatory Structures**
  - Medical Devices: FDA
  - Vehicles: NHTSA

- **2015 Cybersecurity Act**
  - HHS Mandate to examine cyber requirements of health device vendors & clinical users

- Health is the sole sector identified for “remediation”
  - No provisions for “connected medical devices”
  - Pending **HHS Task Force Report on Medical Device Cybersecurity**
  - Focus likely to be on security of networks
New Theories of State level Civil Liability to Account for Connected Vehicles and Medical Devices

- **IoT Opens New Avenues of Risk** Generally
  - Federal regulatory reviews based on vehicle/device safety:
    - Reviews do not address IT integrity or vulnerability!!
  - “Big Data”: interpolation/aggregation of specific information about a patient, or a disease, or a cluster:
  - Data=Value to collector, but COLLECTION may be HIPPA crime
  - Economic Harm to Data Asset
    - Arises from Intentional Act of Defendant—a DATA “EXPLOIT”), or
    - Breach of Duty of stewardship over valuable data

- **BUT FOR VEHICLES & MEDICAL DEVICES, perhaps, a HIGHER DUTY of CARE?**
  - Even economic harm alone should be recognized: “patient data” is special data, with special value
    - Losses from: storage device failure (‘Aurora’ rotating media), second order effect physical harm to patient when data is lost/corrupted, losses by deploying entity (clinic, lab); losses by indemnifying insurers or self insurers
Why should AGs care?

- Risks falling under criminal jurisdiction:
  - Device corruption or takeover
    - Impacts commercial users, criminal justice/law enforcement
  - Privacy & other consumer/fraud abuses
  - Network Insecurity
    - Impacts CJ/LE, Government Services, Election Systems
  - Physical injury or death to citizens
- These are exacerbated by IOT’s massive scale
State Role

• **Police the state/local IoT ecosystem**
  – IT supply chain: devices, components, software
    • Inspectors General or Fraud divisions of OAG
    • IT & vehicles = # 2, 3 state/local expenditure after real estate

• **Establish clear civil jurisdiction** for vehicle, medical device failures/injuries caused by IoT IT

• **Contract vigilance**: know your vendor/supply chain
  – Don’t buy network services from known terror threat state actors
REFERENCES

• US GAO. IOT Technology Assessment. May 2017 (GAO 17-75)
• Industrial Internet Consortium. IOT Reference Architecture (2016)
• OECD: “IOT-Securing the Benefits” (2016)
• NIST: Public Private Working Group on Cyber Physical Systems: Report 2015 (draft)
# Wrapping up IoT Devices

<table>
<thead>
<tr>
<th>Harm</th>
<th>Source of remedy</th>
<th>Legal theory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy &amp; Data security Losses</td>
<td>HIPPA, State privacy statutes</td>
<td>Statutory/strict liability</td>
</tr>
<tr>
<td>Bodily injury/Physical Harm</td>
<td>Tort/Contract</td>
<td>Med Mal/Negligence/Breach</td>
</tr>
<tr>
<td>Economic harm</td>
<td>None, unless more than $ loss</td>
<td>“Data as an Asset”</td>
</tr>
</tbody>
</table>
WIRED:
Medical Devices Are the Next Security Nightmare
Inside Patent Litigation

THE SERIOUS AND IMENSE IMPACT OF A MEDICAL DEVICE HACK

• 21 FOOTNOTES !!!
BBC NEWS:
Medical devices vulnerable to hackers
USA TODAY:
– Medical-device, IoT hacks spurring security software boom

POPULAR SCIENCE HEALTH
– Hacked Medical Devices May Be The Biggest Cyber Security Threat In 2016
  • Through insulin pumps and pacemakers, hackers could hold your life ransom

abc NEWS
– FDA Issues Safety Advice for Cardiac Device Over Hacking Threat
And even more recently....

- **October 2016:**
  - Johnson & Johnson reports remote takeover of one-touch *Ping Insulin Pump*

- **January 2017**
  - St. Jude Medical releases security patch to Defense Implantable Cardiac Defibrillator (pacemaker) device
Implementing the “higher duty” argument

• We concede recovery in Negligence is difficult if vendor and provider have done “something” to meet duty of care
• Therefore, more direct route to recovery is strict liability, such as from statutory liability
  – No need to establish privity; little risk of $0 recovery
  – But, often, multiple defendants
• Liability theories to be embedded in state acts to protect patients:
  i. Design defect—unreasonably dangerous product
  Defective components, open source firmware, network failure, insufficient access security
  i. Failure of Security: exploit or attack succeeded: *res ipsa loquitor*
  Explicitly extend Wyndham “vendor” duty to Connected Medical Devices
  i. Technology Error or Omission: insurable interest