The Internet of Things and its Future Impact on Product Liability

H. Michael O’Brien
Wilson Elser Moskowitz Edelman & Dicker LLP
1133 Westchester Avenue
White Plains, New York 10604
michael.obrien@wilsonelser.com
What is the Internet of Things?

IoT is *not* Y2K
What is the Internet of Things?

The Third Wave of the Internet

First wave – 1990s building the infrastructure

Second wave – 2000s dual development of internet services as well as mobile connectivity
IoT operates on embedded sensors sending environmental and activity information to Data Stores.
Data Stores, in turn, interact with Analytic Engines to provide feedback and, in turn, control to sensors.
What is the IoT?

Sensors give objects the power of perception into conditions such as temperature, voltage, motion, chemistry and usage.
What is the IoT?

Sensor driven computing (i.e. the analytics) converts these perceptions into insights that operators and systems can act on.
IoT devices already exist:

1. Cars and trucks;
2. Smart TVs, cell phones;
3. Home security and HVAC system management;
4. Industrial manufacturing;
5. Medical devices;
6. Drones, 3D manufacturing, etc.
How big is the IoT?

The 2015 Consumer Electronics Show in Las Vegas had over 900 exhibitors of IoT technologies for homes, cars, security systems and appliances.
How big will the IoT become?

According to Gartner, Inc., there are over 5 billion devices connected to the internet.

By 2020, there will be 25 billion, with revenues exceeding $300 billion.
1. wearables;
2. connected cars;
3. connected homes;
4. connected cities; and
5. industrial internet: (e.g.) transportation, oil & gas and healthcare

The Internet of Things: Making Sense of the Next Mega Trend – Goldman Sachs (Sept. 2014)
Goldman Sachs identified key sectors
The driving market forces:

1. cheap sensors;
2. cheap bandwidth;
3. cheap processing;
4. smart phones;
5. ubiquitous wireless coverage; and
6. big data
Other forces:

The value proposition of new product cycles and cost efficiencies, productivity and cost savings

New apps and software platforms
The Industrial Internet Consortium was formed in 2014.

Founding members include AT&T, Cisco, GE, IBM and Intel.

Today, there are 200 member companies.
The Industrial Internet of Things (IIoT)

...describes the integration of complex physical machinery and devices with networked sensors and software, used to predict, control and plan better business and social outcomes.
Many M2M applications have been developed and many more are being developed.

Early applications are being applied on “advanced scheduled” and “preventative maintenance” and to “anticipate critical failures” for large industrial applications.
The Industrial Internet of Things (IIoT)

- GE has estimated the Industrial Internet could add $10-$15 trillion to global GDP over the next 20 years.

- Gartner has estimated that 1 in 3 knowledge workers will be replaced by 2020.

- McKinsey Global Institute estimates an annual economic impact of $2.7 trillion to $6.5 trillion by 2025.
IoT Growth; But at what cost?

Hewlett Packard 2014 study found 70% of commonly used IoT devices contain security vulnerability.

Internet of Things Research Study – Hewlett Packard (2014)
Hypothetical IoT Threat

- Smart refrigerator communicates with store to setup delivery of groceries

- What are the potential threats?
  - That your purchase patterns are monitored?

- It could be a privacy and security threat to your personal data which could be collected and sold

- Or it could become an entry point for a hacker
Hypothetical IoT Threat

- It can also be an entry point for hackers to access the store’s payment database.

- The large scale hack against Target was through a third-party HVAC vendor whose software security was the weak link allowing for access to Target’s customer database.
Examples of Actual IoT Failures

- Wink’s wireless hub connected to a variety of devices in the home via a single app. Glitch in April 2015 disabled connected devices.

- Chamberlain and Ooma had similar failures.

- Hospira’s Symbiq insulin fusion pump. FDA issued warning to hospitals that it was vulnerable to hacking and dosing of “critical patient therapies” was possible.
Examples of Actual IoT Hacks Leading to Property Damage

- Stuxnet cyber attack of Iranian nuclear facilities at Natang in September 2010 damaging centrifuge operational capacity. The attacks forced a change in centrifuge’s rotor speed first raising then lowering them to destroy the centrifuge.
HOW STUXNET WORKED

1. Infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. Search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. Update
If the system isn’t a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. Compromise
The worm then compromises the target system’s logic controllers, exploiting “zero day” vulnerabilities—software weaknesses that haven’t been identified by security experts.

5. Control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. Deceive and Destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won’t know what’s going wrong until it’s too late to do anything about it.
Examples of Actual IoT Hacks Leading to Property Damage

- German steel foundry attacked in 2014. Hacker gained access to blast furnace controls leading to runaway condition resulting in large scale damage to the furnace.
IoT as a Threat to National Security / Emergency Preparedness

- November 2014, the National Security Telecommunications Advisory Committee (NSTAC) issued a report to the President on the Internet of Things.

- “[i]n 2008, the U.S. National Intelligence Council warned that the IoT would be a disruptive technology by 2025.”
The Council said that individuals, businesses, and governments were unprepared for a possible future when network interfaces reside in everyday things.

Almost six years later, this warning remains valid, though it now seems certain that the IoT will be disruptive far sooner than 2025 - if it is not so already.” [Emphasis added.]
The NSTAC found that the compromise or malfunction of IoT devices could have national security / emergency preparedness implications.

Compromised devices connected to different critical infrastructure systems could have the potential for major economic disruption, kinetic damage impacting public safety, or in extreme cases, catastrophic failure of national infrastructure or critical systems.
Among the more compelling and thought provoking findings reached by the committee were:

- “The line between consumer and industrial devices continues to blur, with consumer devices used—intentionally or not—in ways that affect national security/emergency preparedness.

The strong growth in interconnected, potentially adaptive devices implies a larger cybersecurity attack surface with potentially cascading adverse effects in both the cyber and physical domains.”
Among the more compelling and thought provoking findings reached by the committee were:

- “IoT represents a convergence, or perhaps a collision, of IT and OT. To this point, the two disciplines have approached cybersecurity differently.

IT security involves patches and frequent updates and the ability to take systems offline as needed, while OT security is largely based on obscurity and specialization, in large part because of the need for systems to remain online, whether compromised or not.

This disconnect creates gaps that attackers could exploit.”
Among the more compelling and thought provoking findings reached by the committee were:

- “Innovation and adoption of IoT technology are outpacing the development of IoT governance structures and related policies. This appears to be true at both the national and global levels.”
Potential Threats Identified

- Federal Trade Commission (FTC) in Jan. 2015 identified safety and security concerns
  
  Examples: Insulin pumps being accessed remotely and dosages changed; remote access to starting a car or disabling safety devices.

- Former U.S. Vice President Dick Cheney revealed in 2013 he disconnected his defibrillator and heart pump from the internet to prevent its hacking

Internet of Things: Privacy & Security in a Connected World – FTC Staff Report (Jan 2015)
Sen. Edward Markey (D-MA) issued a report addressing IoT concerns present today with automobiles and the threat of hacking to take control over vehicles or disable vehicle safety devices.

Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk
Potential Threats

- U.S. GAO April 2015 found – “modern aircraft are increasingly connected to the internet. This interconnectedness can potentially provide unauthorized remote access to aircraft avionics systems”

- “FAA has taken steps to protect its ATC (Air Traffic Control) systems from cyber based threats; however, significant security control weaknesses remain.

- Security researcher Chris Roberts of One World Labs claims to have hacked and seized control of a commercial aircraft in 2015. FBI commenced an investigation.
Potential Threats

- September 10, 2015 the Federal Bureau of Investigation (FBI) posted online a public service announcement warning the public of IoT risks for cyber crime.

In addition to threats to individuals’ and business’ personal data “compromising the IoT device to cause physical harm” was identified. Universal Plug and Play protocol (UPnP) was identified as being especially vulnerable to exploitation.
Identified the Internet of Things as having a very high risk impact potential along with:

- Deglobalization
- The great monetary experiment
- Super nat-cats
“From cyber breaches to shifting questions of property and products liability, businesses cannot afford to enter this new technological world unprepared.

For example, every object that connects with the Internet is another entry point through which the cyber-criminals can enter a business’ enterprise system.

Equally dangerous, in a world where machines replace humans as the decision-makers and sensors are continually capturing data, serious questions of liability, resulting physical damage and privacy arise.”
Privacy & Data

- AT&T reports a 458% increase in Internet of Things (IoT) vulnerability scans against devices
- 50 billion things will be sharing data by 2020
- Small sensors can be harder to secure than bigger more sophisticated devices like PCs and tablets
- Bottom line: more but less complex devices mean more potential security gaps to manage

What every CEO Needs to Know About Cybersecurity, Decoding the Adversary, AT&T Cybersecurity Insights, Volume 1, October 1, 2015
What are the Litigation Risks?

Small glitches impacting on hundreds of thousands or millions of devices is an ideal recipe for product liability no-injury class action litigation.
Theories of Liability: breach of warranty as vehicles were not free of defects: “because defendants failed to ensure basic electronic security of their vehicles, anyone can hack into them, take control of the basic functions of the vehicle, and thereby endanger the safety of the driver and others.”
Each vehicle has up to:
A) 35 separate electronic control units (ECUs)
B) Controlled area network (CAN)

“Vehicle functionality and safety depend on the functions of these small computers, the most essential of which is how they communicate with one another”

“[H]acker could take control of such basic functions of the vehicle as braking, steering and acceleration – and the driver of the vehicle would not be able to regain control”
IoT Class Action Litigation

- *Wired* magazine in July 2015 reported on a remote hack of a Chrysler Jeep where critical safety systems were taken control of remotely

- Chrysler Fiat within days announced a recall of 1.4 million affected vehicles

- Aftermath of Fiat-Chrysler Recall: Class action: *Brian Flynn, et. al., v. FCA US LLC, et. al.*, U.S. District Court for the Southern District of Illinois, Case No. 3:15-cv-855
Allegations

- Harman International manufacturer of “infotainment system” called UConnect
- The recall announced by Fiat-Chrysler did not fix the entire problem. The essential problem is “that non-secured systems are coupled with essential engine and safety controls” which is not a software problem
- Software updates are only remedial fixes for known vulnerabilities
- Breach of warranty, fraud, negligence, unjust enrichment, state consumer fraud and business practices violations
Government Intervention

- The Spy Car Act of 2015:
  - All driving data collected shall be reasonably secured to prevent unauthorized access
  - Also provides for a *cyber dashboard* which will inform consumers of … “the extent to which the motor vehicle protects the cyber security and privacy of the owners, lessees, drivers and passengers…”
  - Sec 27 addresses privacy and requires that each motor vehicle shall provide notice of the collection, transmission, retention and use of driving data collected from the vehicle
Government Intervention

- The Spy Car Act of 2015 (cont.):
  - Owners and lessees are to be given the option of terminating the collection and retention of driving data with two exceptions. First, if they do elect to terminate, there should be no loss of navigation tools or other features or capabilities. Second, driving data stored as part of the electronic data recorder system or other safety systems on-board that are required for post incident investigations, emissions history checks, crash avoidance or mitigation, or other regulatory compliance programs will remain in place.
Emerging PL Considerations

Traditional PL claim – Design or Manufacturing Defect with a sensor or software leading to property damage or bodily injury
Emerging PL Considerations

Traditional PL claim – Design or Manufacturing Defect with a sensor or software leading to property damage or bodily injury

PL claims where “hacking occurs” resulting in property damage or bodily injury
Emerging PL Considerations

Traditional PL claim – Design or Manufacturing Defect with a sensor or software leading to property damage or bodily injury

PL claims where “hacking occurs” resulting in property damage or bodily injury

PL claims where “hacking occurs” resulting in stolen data used for a variety of illegal harmful purposes
Emerging PL Considerations

- New types of experts required – software engineers & cyber security specialists
- Currently no standards governing IoT products
- Insurance coverage implications – gaps
- Cyber policies traditionally don’t cover property damage and bodily injury
- CGL, PL, E&O and D&O may cover some losses
- Differences in conditions coverage may be needed
Emerging PL Considerations

- Reporting obligations to government safety agencies (CPSC, FDA, NHSTA & FTC)
- Product recalls / Corrective actions
- What will be the remedy and at what cost?
New Issues – Security vs. Privacy

- What role / responsibility will the consumer bear if they aren’t tending to their own data security?

- Is the responsibility to update software, prevent malware – up to the individual, the business stakeholders or both?

- Who has custody, ownership and control of the data?
New Issues – Security vs. Privacy

- Manage security throughout the lifecycle of a device

- Securing the supply chain – chips, software, network – each connection point is a potential vulnerability

- Cost concerns: Cheaper IoT connected products may be less secure but more popular in the market than more secure expensive products
Security and Product Differentiation:

- Car – Expensive, used for years - vs.
- Stove, TV, Refrigerator, Washer & Dryer - vs.
- Coffeemaker, toaster oven - vs.
- Wearables

Does the cheaper the device equate with greater vulnerability and less likelihood that fixes will be made available?

- What happens when the product is out of warranty?
- What happens when the product line has been discontinued?
Security and Product Differentiation:

- With the Internet of Things and the multiple platforms of interconnected devices, the security of all of the devices may very well be established by the weakest link in the chain of interconnected devices.
Supply Chain Considerations

- What type of language will be needed in supplier agreements to address risk shifting and allocation?

- This spans the entire supply chain. The product manufacturer may source the sensors and software for IoT connectivity from a third party or it may be propriety. Does the sensor and software company have a stake in the liability equation?
Supply Chain Considerations

- Hold harmless and indemnification provisions as well as documentation of adequate insurance coverage with additional insured endorsements and provisions will be required and it needs to be the right kind of insurance.

- What will be the reporting obligations of those in the supply chain to government regulatory and safety agencies such as the CPSC, FTA, FDA and NHSTA?

- What incidents will require a corrective action or recall to be implemented? Can it be fixed by a patch or upgraded security?

- What will be the impact if an IoT failure is based on a terrorist act?
Developing Standards

- **Institute of Electrical and Electronics Engineers (IEEE):**
  - P2413 Draft Standard for an Architectural Framework for The Internet of Things Working Group

- **International Telecommunications Union (ITU):**
  - Y2060 – Overview of The Internet of Things

- **International Standards Organization (ISO):** has working group assessing ISO 27000 family of security standards insight be adopted to address IoT security needs
Industry Groups

- Online Trust Alliance – IoT Trust Framework: to develop best practices in the Internet of Things security, privacy and sustainability
Insurance and the IoT

- The traditional business model for insurance...is becoming less sustainable in the long term due largely to the rapid innovation that the Internet of Things is driving throughout the economy.
- Insurance coverage is becoming part of a broader value chain with new types of products and services.
- The IoT will impact the core of insurance, as 80 percent of insurers believe it will radically change the nature of risks covered.
- This change will occur in two ways. First, new technologies (drones, for example) will present new risks to be insured.
Insurance and the IoT

- Second, assessment of existing risks will need to consider new parameters (for instance, self-driving cars controlled by autonomous systems)

- 75% of insurers believe that industry boundaries will dramatically blur as the IoT and other platforms reshape industries into interconnected ecosystems
Insurance and the IoT

- Insurers...will no longer compete just with other insurance companies, but also with players from a variety of traditional and innovative industries... Digital innovators...such as Google, Apple and Facebook – are particularly threatening as they may define the new competitive rules for the IoT economy

- The risk for insurance is becoming a mere commodity

Are You Ready to be an Insurer of Things? How the Internet of Things is Changing the Rules of the Game for Insurers, Accenture Strategy - 2015
Terms of service agreement (ToS) effectively allows Google, Facebook, LinkedIn and other internet companies to monetize all of your personal data for any purpose they choose.

Free technology makes the consumer the product.

The real customers of the tech companies are the businesses that buy the data from internet companies.

It’s a multi-billion dollar business that will get bigger as IoT expands.
KANAMITS OFFER PEACE AND PROSPERITY
We all are the Product!
Suggested Reading

- The Internet of Things - Samuel Greengard
- Future Crimes - Marc Goodman
Thank you

Comments & Questions?