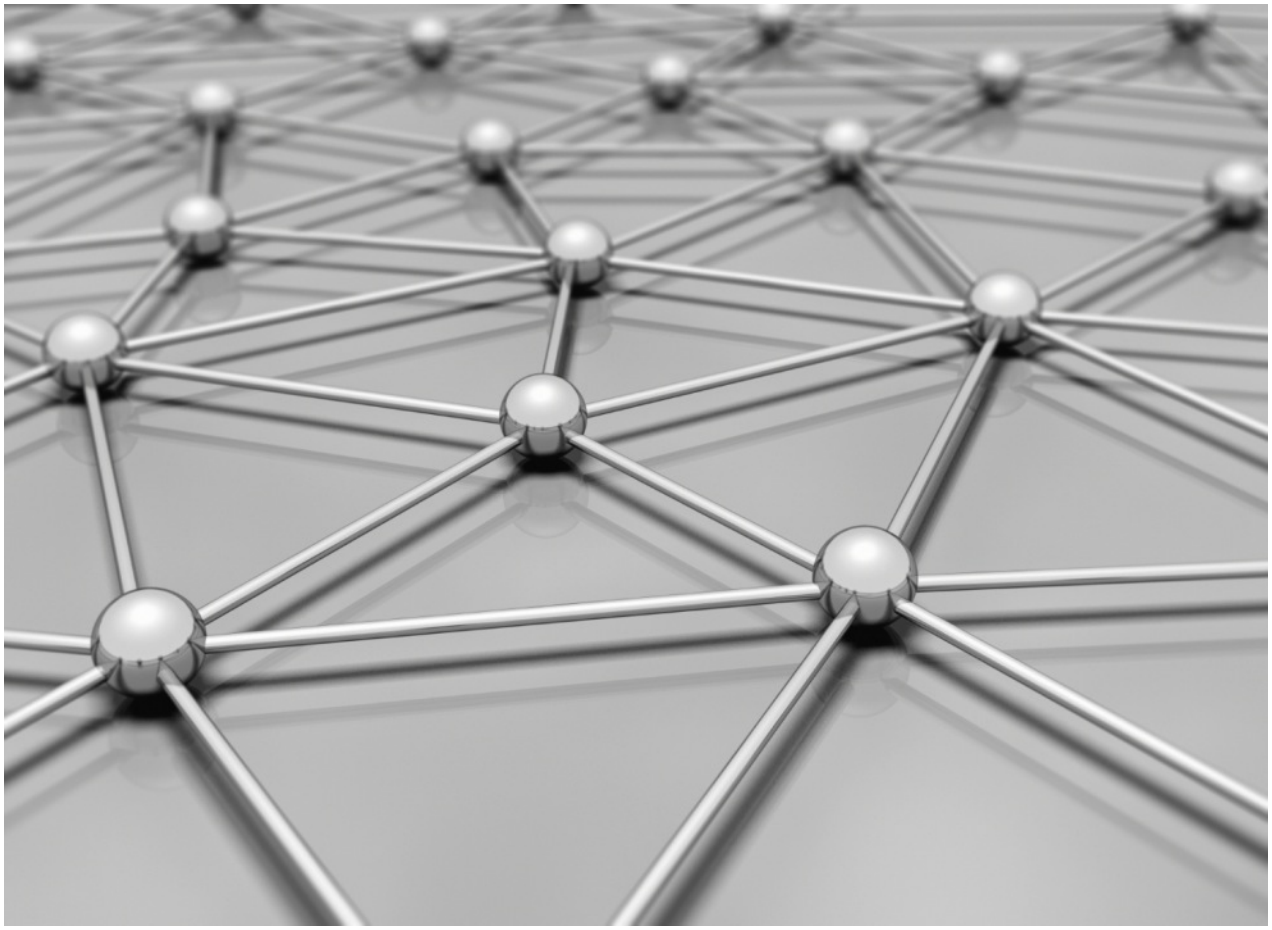
SEIGER GFELLER LAURIE LLP
ATTORNEYS AT LAW

THE INTERNET OF THINGS: A NEW ERA OF CYBER LIABILITY AND INSURANCE

VINCENT J. VITKOWSKY



New York Connecticut New Jersey

THE INTERNET OF THINGS:
A NEW ERA OF CYBER LIABILITY AND INSURANCE

By

Vincent J. Vitkowsky

Introduction

Over the course of my lifetime, the fanciful visions of cartoonists and science fiction writers have come to exist. We have entered the era of the Internet of Things ("IoT") – an era in which devices with sensors connected to the Internet collect, store, and analyze massive amounts of data, and play an increasingly prominent role in the physical world.

The IoT encompasses devices used in businesses, health care institutions, and homes. They include, for example, medical devices, cars, baby monitors, printers, smart TVs, thermostats, refrigerators and kitchen appliances, routers, home alarms, fitness trackers, and other wearable technologies. The IoT also includes some of the world's largest assets, such as trains, gas and wind turbines, oil refineries, factories, harbors, and smart grids.

It is commonly estimated that there are 10 billion devices connected to the Internet now, with projections that the number will double or triple by 2020.

Special Challenges and Issues

The IoT presents special cybersecurity challenges. Many devices were designed for convenience, not security, and as a result can often easily be hacked. In most cases, the devices were not designed with robust protections against malicious code or the capability to be easily patched. A leading technologist has stated that "the result is hundreds of millions of devices that have been sitting on the Internet, unpatched and insecure for the last five to ten years." [1] The legal, product liability and insurance coverage issues coming from these devices will emerge fully over the next decade.

The IoT presents three broad sets of issues. The first relates to privacy and data security concerns. How is the data in these devices stored and accessed, and with whom is it shared? If the data is compromised or lost, what first- and third-party liabilities arise?

The next set relates to bodily injury and physical damage. Who is liable when a device malfunctions because of defects in its software design? What about when its network is hacked and the devices are manipulated?

Finally, what forms of insurance will respond?

---

[1] Bruce Schneier, *The Internet of Things Is Wildly Insecure – And Often Unpatchable*, www.schneier.com/essays/archives/2014/01/the_internet_of_thin.html

Privacy and Data Security

IoT devices often store personally identifiable information or personal health information in unencrypted form, which can be improperly accessed or inadvertently transmitted.

The focus of cyber liability in recent years has been on data breaches resulting in the loss of personally identifiable information and private health information. Most of the litigation concerns whether consumers, or banks issuing debit or credit cards, have causes of action against retailers or other organizations that are hacked. There is virtually no definitive law. So far, plaintiffs have not had much success seeking recovery in claims for breach of contract, invasion of privacy, unjust enrichment and bailment. They have had more success, at least avoiding motions to dismiss, in claims based on common law negligence and under consumer protection statutes.

The Federal Trade Commission ("FTC") has conducted enforcement proceedings based on the position that the lack of reasonable security measures to protect consumer data may constitute an unfair or deceptive trade practice under Section 5 of the FTC Act. It has moved against companies who lose personally identifiable information through "inadequate" data security practices. In 2014, it extended its oversight to IoT consumer products, commencing a proceeding against and ultimately reaching a settlement with TRENDNet, Inc., which sells Internet-enabled surveillance cameras used for home security and baby monitors. The FTC alleged that because of software defects, hackers were able to easily access and post hundreds of live feeds, and that the feeds constituted private information.[2] The FTC has subsequently conducted workshops on the IoT and is expected to continue to play a leading role in enforcement of privacy-related issues. In January 2015, it released a staff report making non-binding recommendations for best practices, including building security into the devices at the outset.[3]

Another key dynamic of the IoT raises the stakes. As enormous volumes of data are collected, the information can be consolidated, shared and analyzed for marketing purposes. Under this variant of "Big Data," the information can be used to make sensitive predictions about consumers' medical conditions, sexual orientation, religion and race. There is uncertainty about what rights to ownership and use of such consumer data exist, what steps companies may take to exploit that data, and what steps they should take to protect its exploitation. This is further complicated when a company contracts with vendors to process and manage the data.

---

[2] Lesley Fair, *You're on Candid Camera,* www.business.ftc.gov/blog/2013/08/youre-candid-camera

[3] The Internet of Things: Privacy and Security in a Connected World, http://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices

Bodily Injury and Property Damage

IoT devices will add much convenience to our lives. But some will inevitably malfunction and cause damage in the physical world, opening the door to new cyber liabilities.[4]

Thus far, most cyber claims have involved data breach remediation costs or financial losses from network disruption. Under tort law, the economic loss doctrine typically prevents recovery for purely financial losses. With the advent of the IoT, however, recovery based on tort theories will become more likely, as malfunctions result in bodily injury or property damage.

It is fairly well settled that software can be considered a product. IoT devices comprised of integrated hardware and software systems will almost surely be treated as products. This means that theories of negligence and strict liability may be available, with no need for privity of contract.

A few observations are in order. First, negligence claims may be difficult to establish. The collective, collaborative, iterative process of developing team-designed software in a breathtakingly fluid technological environment will make it hard to establish a commonly accepted duty of care. It also may be difficult to establish proximate causation.

Given these hurdles, claimants will undoubtedly push for the application of strict product liability theories. Under those, claimants generally only need to demonstrate that there is a design defect that is unreasonably dangerous to users. For IoT devices, this will not be a clean fit. All software is "buggy." That is, the possibility of defects in software design are always present. This is widely known, so there will be substantial arguments that it would be unfair to hold manufacturers to strict liability standards. There will also be arguments that this would discourage innovation and growth. Yet there will be catastrophic incidents that cry out for relief.

As a result of these tensions, courts will be urged to adopt tests based on gradations of bugginess. How flawed must software be for a product to be found to have a design defect? How serious must the risks be for the product to be unreasonably dangerous? What importance will be assigned to the extent to which IoT devices are tested? Under negligence theories, testing can be direct evidence of the application of a standard of care. But evidence of testing is not always admissible in strict products liability cases.

Beyond cases in which the device malfunctions with no outside intervention, there will be those in which the injury or damage results from the deliberate acts of a third-party hacker. Here, the extent to which the seller or manufacturer has taken reasonable precautions to protect against hackers will become important.

---

[4] Background on cyber events with physical effects can be found at Vincent J. Vitkowsky, *The Cyber Threat Matrix To Energy and Utility Companies,* **Advisen Cyber Liability Journal,** Vol. 3, August 2012 (including discussion of SCADA industrial control systems) and Vincent J. Vitkowsky, *Industrial Cyber Attacks Generate Wide Range of Coverage Concerns,* **Business Insurance,** March 19, 2012.]

The U.S. government has started to address some IoT devices, most notably medical devices. These include devices such as pacemakers, insulin pumps, computers generating warning labels for prescription drugs, and hospital equipment. Prominent White Hat hackers have made very public yet harmless demonstrations of their vulnerabilities. Black Hat hackers will not be so benevolent.

In the fall of 2014, the Food and Drug Administration issued cybersecurity guidelines for medical device manufacturers, entitled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices." [5] The guidelines encourage manufacturers to create a set of cybersecurity controls to maintain security as part of the design and development process. Second, they recommend that manufacturers document their consideration of cybersecurity risks, and their implementation of controls to safeguard the software. The guidelines are not mandatory, but they will likely be put forth as evidence of a standard of care that manufacturers should follow.

Also in late 2014, the Department of Homeland Security was investigating and working with about two dozen manufacturers of medical devices and hospital equipment to identify and repair software bugs that could permit hackers to expose confidential data or otherwise attack people or organizations.[6]

Insurance for IoT Losses

The last five years have seen an expansion in cyber insurance as a distinct line of business. The main focus so far has been to indemnify against first- and third-party losses resulting from data breaches of personally identifiable information, disruption of a company's own network, cyber extortion, and media liability. But the industry has an evolving understanding of what risks are within the cyber domain. In 2014, a few companies introduced policies that would indemnify against claims for bodily injury and property damage related to cyber incidents. And throughout, insureds have also sought to recover cyber losses under traditional liability insurance policies.

IoT losses can consist of the compromise of data, malfunctions within the physical device itself, or malfunctions of the remote computer programs or algorithms. The results may be financial losses, bodily injury or physical damage to tangible property. These losses will implicate various types of policies. First-part property policies are often silent on whether they respond to cyber-related damage. In the third-party context, losses involving bodily injury or physical damage to tangible property will lead to product liability claims. Unless the policy is tailored to the unique qualities of IoT devices, coverage questions will arise.

---

[5] https://www.federalregister.gov/articles/2014/10/02/2014-23457/content-of-premarket-submissions-for-management-of-cybersecurity-in-medical-devices-guidance-for

[6] http://www.reuters.com/article/2014/10/22/us-cybersecurity-medicaldevices-insight-idUSKCN0IB0DQ20141022

For example, many traditional liability policies contain broad electronic data exclusions. Other common exceptions to the product liability coverage grant might also apply. The controlling algorithm, which is always a work in progress, might be found to be "work that has not been completed or abandoned," or the work of software engineers could fall within the professional services exclusion.

Moreover, the impaired property exclusion precludes coverage for property damage to impaired property that results from the insured's faulty or dangerous products or completed work. Coding errors and other software defects may fall within this exclusion. And many courts find there is no coverage where the loss is only to the electronic data or operating systems, either because they are not tangible property, or the losses are only financial.[7]

IoT malfunctions that result only in financial loss may be insured by a professional liability product that has come to be known as "Tech E&O" insurance. These policies often afford cover not just for errors and omissions, but for liability assumed by contract, which is an important consideration for software developers. They need to be carefully drafted, customized, and often specifically tailored.

Finally, various types of losses may be insured by new products developed by the cyber insurance market.

Only a few insurers have developed sophisticated, nuanced policies to address the difficult issues that may arise in IoT claims. Even those policies will be subject to varying interpretations by insurers, insureds, and courts, as events unfold in countless variations.

Conclusion

This article presents a framework for understanding the IoT, but it has only scratched the surface of the complexities and issues that arise. They present novel and fascinating challenges for both underwriting and claims teams. The future is here.

February 2015

About the Author: Vince Vitkowsky is a partner at Seiger Gfeller Laurie LLP, resident in New York. He represents insurance and reinsurance companies in complex coverage and claims matters, and on cybersecurity and cyber insurance issues. He has been identified in many leading lawyer directories, including Chambers America's Leading Lawyers for Business, The International Who's Who of Business Lawyers, and Euromoney's Best of the Best.

[7] *See, e.g., America Online Inc. v. St Paul Mercury Ins. Co.,* 347 F.3d 89 (4th Cir. 2003); *Rockport Pharmacy, Inc. v. Digital Simplistics, Inc.,* 53 F.3d 195 (8th Cir. 1995)