The Internet of Things: Insurance Coverage Considerations

By

Ellen M. Farrell and Rachel P. Raphael*

I. INTRODUCTION

Today, billions of different devices are connected to the Internet and the Internet-capability of everyday objects is expected to grow exponentially in the years to come. The Internet of Things (IoT) refers to the network of these devices which collect and exchange data. Connected devices may include everything from automobiles to implantable medical devices to home appliances. The large-scale use of these devices is already revolutionizing many aspects of our daily lives by increasing the availability of information and changing the ways that business and consumers interact. But at the same time, it is creating a host of new cyber-related risks, as a wealth of new information may be open for attack.

Indeed, controlled demonstrations and data breach incidents have shown that there are still improvements to be made in the techniques used to secure IoT devices. The exposure of vulnerabilities has led to lawsuits against companies involved in the production, sale, distribution and marketing of Internet-connected products. When facing potential liability, companies commonly turn to their insurance policies for coverage. But with complicated risks come complicated insurance issues. The tangible and intangible nature of data breaches involving IoT products raises interesting issues under both stand-alone cyber insurance and more traditional liability policies. After briefly discussing the background of risks associated with IoT devices, their regulation and litigation, this article discusses how courts and the Insurance Services Office (ISO) have considered coverage for other cyber-related incidents and what these court decisions might suggest for coverage issues that arise concerning IoT devices.

II. IOT RISKS, FEDERAL REGULATION AND LITIGATION

IoT is generally understood to refer to a decentralized network of physical objects that are connected to the Internet and enable communication between humans, computers, objects, applications and devices.[1] The number of connected objects in the IoT is growing at a rapid rate: In 2003, approximately 500 million devices were connected to the Internet.[2] Today, there are over 6.4 billion such devices, with approximately 5.5 million more connecting to the Internet each day.[3] By 2020, the number of devices in the IoT is predicted to exceed 20 billion[4] -- possibly reaching as much as 40 to 50 billion.[5]

---

* Ms. Farrell is a senior counsel and Ms. Raphael is an associate in Crowell & Moring's Insurance/Reinsurance Group. Ms. Farrell and Ms. Raphael thank Tom Kinney, Anupama Prasad and Sahar Sabir for their assistance with this article.

1 Nasrine Olson, *The Internet of Things*, 18 New Media & Soc'y 680 (2016) (book review); National Sec. Telecomms. Advisory Comm., NSTAC Report to the President on the Internet of Things (2014).

2 Shawn DuBravac & Carlo Ratti, The Internet of Things: Evolution or Revolution? 6 (2015).

3 H. Michael O'Brien, *The Internet of Things and its Future Impact on Product Liability* (2015).

A. Risks

The IoT presents risks to privacy, cybersecurity and safety. As to privacy, within the IoT, billions of sensors around the world are constantly acquiring information about their surroundings, and new ways of capturing and using personal information continue to emerge.[6] As a result, there are concerns regarding the unpermitted access to and misuse of personal information and consumer data,[7] for example data collected from the IoT might be used in ways its consumers did not authorize.[8] Another privacy concern is the ease with which hackers may conduct identity theft: "General data available on the internet, combined with social media information, plus data from smart watches, fitness trackers and if available smart meters, smart fridges and many more" provide hackers with "a great all-round idea" of individual identities.[9]

As to cybersecurity, the potential of cyber-attacks (and associated costs) has risen, and will continue to rise, with the growing number of smart objects in the IoT. Cybersecurity is designed to protect "information systems, their components and contents, and the networks that connect them from intrusions or attacks involving theft, disruption, damage or other unauthorized or wrongful actions."[10] Cyberattacks result not only in the theft of data, but can also cause bodily injury and property damage.[11] For example, in 2008, hackers accessed a Turkish Pipeline through surveillance camera software and caused an explosion by super-pressurizing the oil in the pipeline after shutting down its alarms.[12] In 2014, the German Federal Office of Information Security announced that hackers had gained access to a German steel factory's production networks and caused system components to fail by tampering with the controls of its blast furnace.[13] More recently, in January 2017, hackers infiltrated an Austrian hotel's electronic key system, locking guests out of their rooms and forcing the hotel to give in to

---

4 *Id.*

5 DuBravac & Ratti, *supra* note 2, at 2.

6 DuBravac & Ratti, *supra* note 2, at 15.

7 Mohana Ravindranath, *Who's in Charge of Regulating the Internet of Things?,* Nextgov (Sept. 1, 2016), http://www.nextgov.com/emerging-tech/2016/09/internet-things-regulating-charge/131208/.

8 *Id.*

9 Lea Toms, *Beware! Data and Identity Theft in the IoT*, GlobalSign Blog (Mar. 22, 2016), https://www.globalsign.com/en/blog/identity-theft-in-the-iot/.

10 Eric A. Fischer, Cong. Research Serv., R44227, The Internet of Things: Frequently Asked Questions 14 (2015).

11 *Id.*

12 Jordan Robertson & Michael Riley, *Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar,* Bloomberg Tech. (Dec. 10, 2014, 5:00 AM), https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.

13 *Hack Attack Causes 'Massive Damage' at Steel Works*, BBC (Dec. 22, 2014), http://www.bbc.com/news/technology-30575104; Andrew Roth, *Not Just the DNC: Five More Hacks the West Has Tied To Russia*, Wash. Post (June 15, 2016), https://www.washingtonpost.com/news/worldviews/wp/2016/06/15/not-just-the-dnc-five-more-hacks-the-west-has-tied-to-russia/?utm_term=.d0fd4b683b32.

the hacker's ransom demand.[14] And just eight days before President Trump's inauguration, hackers tampered with 70% of storage devices that record data from police surveillance cameras in Washington, D.C., "forcing major citywide reinstallation efforts."[15]

Finally, the most significant risk posed by IoT is the risk to our safety – by, for example, the unauthorized access to medical devices. For instance, in 2014, the Federal Bureau of Investigation (FBI) warned hospitals to discontinue use of a particular line of infusion pumps produced by Hospira due to security flaws that could allow a user to remotely change medication doses.[16] And in January 2017, the Food and Drug Administration (FDA) confirmed that St. Jude Medical's implantable cardiac devices had vulnerabilities that could allow a hacker to access them and deplete their batteries and/or administer incorrect pacing or shocks.[17]

Hackers can also endanger our safety by targeting different modes of transportation. For example, in 2008, a teenage boy hacked into a Polish train system, causing a train derailment and injuring at least 12 people.[18] In April 2015, the U.S. Government Accountability Office (GAO) published a report addressing cybersecurity issues with commercial aircraft.[19] In its report, the GAO noted that the increasing interconnectedness of modern aircraft creates the possibility of unauthorized access to aircraft avionics systems.[20] Similarly, "[w]hile there have been no known cyber-attacks against vehicles . . . most experts believe 'real-world attacks with safety implications could occur in the near future, particularly as automakers begin deploying autonomous (i.e., self-driving) vehicles and connected vehicle technologies.'"[21]

---

[14] Dan Bilefsky, *Hackers Use New Tactic at Austrian Hotel: Locking the Doors*, N.Y. Times, Jan. 30, 2017, https://www.nytimes.com/2017/01/30/world/europe/hotel-austria-bitcoin-ransom.html?_r=0.

[15] Clarence Williams, *Hackers Hit D.C. Police Closed-Circuit Camera Network, City Officials Disclose*, Wash. Post, Jan. 27, 2017, https://www.washingtonpost.com/local/public-safety/hackers-hit-dc-police-closed-circuit-camera-network-city-officials-disclose/2017/01/27/d285a4a4-e4f5-11e6-ba11-63c4b4fb5a63_story.html?utm_term=.7ccd6a0e1b23.

[16] Jessica Condit, *FDA Tells Hospitals to Ditch IV Pumps That Can be Hacked Remotely*, Engadget (July 31, 2015), https://www.engadget.com/2015/07/31/fda-security-warning-hackers/.

[17] Press Release, FDA, Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication (Jan. 9, 2017).

[18] Graeme Baker, *Schoolboy Hacks Into City's Tram System*, Telegraph (Jan. 11, 2008), http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html.

[19] U.S. Gov't Accountability Office, GAO-15-370, Air Traffic Control – FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen (2015).

[20] *Id*.

[21] *See* Paul Merrion, "House smart car caucus revs up vehicle cybersecurity issue," Congressional Quarterly Roll Call (April 28, 2016). The possibility of such intrusions was confirmed in mid-2015 when two individuals conducting a "white hat" hacking experiment were able to manipulate systems and then disable a Sport Utility Vehicle speeding on a busy highway 10 miles away. Michael E. Miller, *'Car Hacking' Just Got Real: In Experiment, Hackers Disable SUV on Busy Highway*, Wash. Post, July 22, 2015, https://www.washingtonpost.com/news/morning-mix/wp/2015/07/22/car-hacking-just-got-real-hackers-disable-suv-on-busy-highway/?utm_term=.7a30e09871f9.

B. Federal Regulation

As with any new, emerging technology, both public and private sectors are struggling to keep up with the IoT and its rapidly advancing role in everyday life. Most IoT regulation consists of guidance or non-binding principles suggested by various federal agencies (although Sates are beginning to weigh in as well).

There is no single federal agency with oversight of the IoT – instead, multiple different agencies each have sector-specific regulatory responsibility for the IoT.[22] For example, within the Department of Commerce (DOC), in 2014 the National Institute of Standards in Technology (NIST) unveiled a cybersecurity framework for identifying cybersecurity vulnerabilities, and putting practices and procedures in place to minimize them, detecting breaches and responding to them.[23] Although not specific to the IoT, the NIST framework certainly encompasses the IoT, and other federal agencies have referenced the NIST framework when suggesting best practices with respect to cybersecurity and IoT for entities that they regulate. Separately, the National Telecommunications and Information Administration (NTIA) recently issued "Fostering the Advancement of the Internet of Things," a Green Paper representing the DOC's analysis of public comments received on the current technological and policy IoT landscape in 2016.[24]

In January 2015, the Federal Trade Commission (FTC), whose mission is to prevent unfair and anticompetitive business practices,[25] issued a Staff Report specific to the IoT.[26] This report describes "best practices" for companies to consider, including a proactive approach to the security of IoT devices,[27] and minimizing the collection and retention of consumer data.[28]

The Food and Drug Administration (FDA) regulates IoT medical devices. The FDA has issued guidance as to the security of such devices, including in December 2016.[29] This guidance encourages implementing a proactive, comprehensive risk management program, and

---

22 Cong. Research Serv., *supra* note 10 at 9.

23 *Framework for Improving Critical Infrastructure Cybersecurity,* Nat'l Inst. of Standards and Tech. (Feb. 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

24 U.S. Dep't of Com., Fostering the Advancement of the Internet of Things (2017), https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf

25 https://www.ftc.gov/about-ftc.

26 U.S. Fed. Trade Comm'n, *Internet of Things – Privacy & Security in a Connected World* 3-4 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

27 *Id.* at iii; *See also* U.S. Fed. Trade Comm'n, Careful Connections – Building Security in the Internet of Things (2015) (the FTC advises companies to encourage a culture of security, implement "security by design", implement a "defense-in-depth" approach, take a risk-based approach, consider the risks of collecting consumer information and avoid using default passwords).

28 U.S. Fed. Trade Comm'n, *supra* note 26, at iv.

29 U.S. Food and Drug Administration, Postmarket Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff (2016), https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm482022.pdf. The FDA issued previous guidance in January 2005 and June 2013.

emphasizes that manufacturers should monitor, identify and address cybersecurity vulnerabilities as part of their post-market management of medical devices.[30] It also recommends that manufacturers address security weaknesses by establishing processes handling vulnerabilities, adopting coordinated vulnerability disclosure policies and deploying strategies to mitigate cybersecurity risk before a cyber-attack takes place.[31]

The National Highway Traffic Safety Administration (NHTSA) within the Department of Transportation has addressed cybersecurity in vehicles. Recently, the NHTSA issued a "Federal Automated Vehicles Policy" which addresses highly automated vehicles ("HAVs").[32] Among other things, the Policy (1) outlines best practices for the safe pre-deployment design, development and testing of HAVs prior to commercial sale or operation on public roads; (2) establishes a national framework, but leaves states with the responsibilities for vehicle licensing and registration, traffic laws and enforcement, and insurance liability regimes; discusses the NHTSA's available regulatory authority over HAVs including interpretations, exemptions, notice-and-comment rulemaking, and defects and enforcement authority; and identifies new authorities and regulatory structures that could aid deployment of new technologies in a safe and expeditious manner.[33]

Other examples of federal agencies that oversee the regulation of various aspects of the IoT include the Federal Communications Commission (FCC),[34] Department Homeland Security (DHS),[35] Department of Justice (DOJ), Department of Defense (DOD), National Science

---

30 *Id.*

31 *Id.*

32 The National Highway Traffic Safety Administration, Federal Automated Vehicles Policy – Accelerating the Next Revolution In Roadway Safety, (Sept. 2016), https://one.nhtsa.gov/nhtsa/av/av-policy.html.

33 *Id.*

34 The FCC recently published "Cybersecurity Risk Reduction," a White Paper on the IoT and reducing cyber risk. *See* U.S. Fed. Commc'n Comm'n, FCC White Paper – Cybersecurity Risk Reduction (2017), http://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0118/DOC-343096A1.pdf. In this White Paper, the FCC indicated that cybersecurity was the FCC's top priority, and that the FCC was "uniquely situated to comprehensively address this issue given its authority over the use of radio spectrum as well as the connections to, and interconnections between, commercial networks, which touch virtually every aspect of our economy[.] *Id*. at 4. Among its recommendations, the White Paper called for collaboration with Internet stakeholder groups, cooperation among federal agencies and regulatory solutions where the market fails.

Although former FCC Chairman Wheeler stated that transitioning to a new presidency should not delay the FCC's work towards achieving cybersecurity, the FCC White Paper was rescinded on February 3, 2017, shortly after President Trump was inaugurated. *See* Jenna Ebersole, FCC Claims Role in Internet of Things, Law360 (Jan. 19, 2017), https://www.law360.com/articles/882644/fcc-claims-role-in-internet-of-things-other-cybersecurity.; *see* also *In re Pub. Safety & Homeland Sec. Bureau White Paper on Cybersecurity Risk Reduction*, No. DA 17-132 (U.S. Fed. Commc'n Comm'n Feb. 3, 2017), https://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0203/DA-17-132A1.pdf. As such, the White Paper is to have "no legal or other effect or meaning going forward." *Id*. It remains to be seen whether and in what form the FCC may reinstate the White Paper.

35 On November 16, 2016, DHS released *Strategic Principles for Security the Internet of Things* (IoT) (2016), https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf. These nonbinding principles, aimed at "stakeholders" with respect to IoT including manufacturers, software developers, and consumers, recommend (inter alia) (1) the incorporation of security at the design phase of IoT devices; managing vulnerabilities in IoT devices, including through security

Foundation (NSF), National Aeronautics and Space Administration (NASA), National Institutes of Health (NIH) and Department of Veterans Affairs (VA).[36]

C. Litigation

As controlled demonstrations and cyber incidents have begun to expose vulnerabilities in Internet-connected products, courts have started to see litigation involving IoT products. These suits have been filed by various parties from individual customers to regulatory agencies, alleging that the susceptibility of these connected products put consumers at risk of bodily injury, property damage and privacy violations. Just as the different types of plaintiffs have run the gamut, so too have the types of devices in question, including over connected cars, children's toys, implantable medical devices, and home security systems.

For example, in 2015, two class action lawsuits were filed against automobile manufacturers over alleged vulnerabilities in the computer systems used in "connected" cars.[37] In *Cahen*, consumers who purchased cars in California, Oregon and Washington filed a putative class action against Toyota, Ford and General Motors alleging that the manufacturers equipped their cars with computer technology that made the vehicles susceptible to hacking and collecting private customer data.[38] According to the complaint, the poor security of the cars' computer systems could cause the driver to lose control of basic functions such as steering, accelerating and breaking and endanger the driver and his or her passengers.[39] The plaintiffs did not allege that their connected cars had been hacked but merely that these cars were *vulnerable* to hacking.[40] As a result, the problem for the plaintiffs in *Cahen* was standing: plaintiffs had to show (1) injury in fact that is "actual or imminent," (2) injury traceable to challenged actions of the car manufacturers, and (3) injury redressable by a favorable judicial decision.[41] The plaintiffs argued that they were injured as a result of the car manufacturers' misrepresentations – had they known about the security issues they would not have purchased their cars or would not have paid as much if they did purchase them.[42] The court was not convinced. The California federal district court dismissed the action for lack of standing, concluding that the alleged risk of hacking was "too speculative" to constitute actual injury.[43] The court also rejected plaintiffs' "benefit of the bargain" argument, explaining that the plaintiffs "have not . . . alleged a

---

updates; utilizing security practices and prioritizing security based on the potential impact if an IoT device were compromised.

[36] *Id.*

[37] *See Cahen v. Toyota Motor Corp.*, 147 F. Supp. 3d 955 (N.D. Cal. 2015); *Flynn v. FCA US LLC*, No. 3:15-cv-0855, 2016 U.S. Dist. LEXIS 130614 (S.D. Ill. Sept. 23, 2016).

[38] 147 F. Supp. 3d at 958.

[39] *Id.*

[40] *Id*.

[41] *Id*. at 965-66.

[42] *Id*. at 966.

[43] *Id*. at 969.

demonstrable effect on the market for their specific vehicles based on documented recalls or declining Kelley Bluebook values."[44]

A month after the class action complaint in *Cahen*, a similar class action complaint was filed against Chrysler and Harmon International seeking damages from alleged security flaws in the "uConnect" systems installed in certain vehicles.[45] Similar to the *Cahen* case, the plaintiffs in *Flynn* alleged that this computer system – which allowed for integrated control of the cars' phone, navigation and entertainment functions – contained vulnerabilities which allowed hackers to take remote control of the vehicles steering and braking functions.[46] Plaintiffs' complaint contained a number of causes of action for negligence, fraud, breach of warranty and violations of consumer protection laws.[47] In September 2016, the U.S. District Court for the Southern District of Illinois dismissed and/or trimmed down plaintiffs' claims.[48] Like the court in *Cahen*, the Illinois federal district court held that the plaintiffs "lack[ed] standing to pursue damages for a risk of harm or a fear of that risk" and dismissed plaintiffs' claims linked to non-economic damages.[49] But unlike *Cahen*, the court in *Flynn* concluded that the plaintiffs had standing to sue for damages concerning the diminished value of their cars given that "ongoing vulnerabilities have reduced the market value of their vehicles."[50]

Another subject of early litigation is connected children's toys. In December 2015, two mothers filed a putative class action lawsuit in California Superior Court against Toytalk and Mattel concerning the companies' Hello Barbie toy.[51] Hello Barbie included a smartphone app that allowed the parents to play, share, and delete the audio recordings of their children produced by the doll.[52] The doll would engage in conversation with the child, record the conversation and then store the recording on the cloud.[53] Among other things, the plaintiffs alleged that the toy was not as secure as it should be and recorded voices of children without parental consent in violation of the Children's Online Privacy Protection Act, 15 USC § 6501, *et seq.*, ("COPPA").[54] According to the complaint, consent was obtained by parents whose child owned the toy but the doll also captured the voices of other children whose parents had not provided consent.[55]

---

44 *Id*. at 971. The case is currently on appeal before the Ninth Circuit.

45 *See Flynn*, 2016 U.S. Dist. LEXIS 130614, at *2.

46 *Id*. at *2-3.

47 *Id.* at *3-4.

48 *Id.* at *35-36.

49 *Id.* at *35.

50 *Id.* at *12-13. On January 10, 2017, the judge lifted the stay on plaintiffs' remaining claims and set a new briefing schedule for the parties.

51 *See Archer-Hayes v. Toytalk, Inc*., No. BC603467 (Cal. Super. Ct. filed Dec. 5, 2015).

52 *Id.* at ¶ 13.

53 *Id.* at ¶ 12.

54 *Id.* at ¶ 20.

55 *Id.* at ¶ 40.

Around the same time, toymaker VTech Electronics North America was met with class action lawsuits filed by parents of children using VTech's electronic learning toys. VTech designs, manufactures and sells electronic learning toys for children that include software programs such as Kid Connect, which allows parents and children to interact with each other through online text messages.[56] VTech experienced a data breach in November 2015, compromising the personal information for millions of consumers, including children.[57] Shortly thereafter, consumers of VTech's products filed putative class actions in the U.S. District Court for the Northern District of Illinois.[58] According to the consolidated complaint, VTech (1) employed data security that was not as secure as it should have been, inconsistent with its representations, and far below industry standards,[59] (2) was slow to detect the unauthorized access to its database,[60] and (3) responded inadequately when it learned of the data breach.[61] Plaintiffs' allege that VTech's "acts and omissions have placed Customers at serious risk of fraud and identity theft and, in the worst case, harm to young children . . . [and that] VTech Customers may have or will become victims of identity theft due to the breadth of the" November data breach.[62]

The lawsuit involving Hello Barbie was voluntarily dismissed with prejudice in July 2016 and litigation in the consolidated action against VTech has been stayed pending mediation. But this looks like it will only be the start of litigation involving connected toys. Indeed, in December 2016, public interest organizations in the United States and the European Union submitted complaints to the FTC and EU Data Protection Authorities ("DPAs") describing various privacy and security weaknesses in connected toys produced by other manufacturers.[63]

Vulnerabilities in implantable medical devices have also started to attract attention. For example, in August 2016, a patient filed a proposed class action against St. Jude Medical in the U.S. District Court for the Central District of California.[64] The plaintiff alleged that St. Jude Medical failed to employ adequate security measures when remotely tracking its pacemakers and

---

56 *See Tittle v. VTech Electronics North America, LLC*, No. 1:15-cv-10889, at ¶¶ 10-11 (N.D. Ill. filed Dec. 3, 2015).

57 *Id.* at ¶ 2.

58 *See, e.g.*, *Giron v. VTech Electronics North America LLC*, No. 1:15-cv-11885 (N.D. Ill filed Dec. 31, 2015); *Tittle*, No. 1:15-cv-10889. In February 2016, a judge in the Northern District of Illinois consolidated five suits pending before him over VTech's toys. *See In re VTech Data Breach Litigation*, No. 1:15-cv-10889 (N.D. Ill. filed Feb. 24, 2016).

59 *Id.* at ¶¶ 30-31.

60 *Id*. at ¶ 37.

61 *Id*. at ¶¶ 38-41.

62 *Id*. at ¶¶ 46, 48.

63 *See* Complaint and Request for Investigation, Injunction, and Other Relief, *In re Genesis Toys and Nuance Commc'ns* (FTC filed Dec. 6. 2016); *Connected toys violate European consumer law*, Forbrukerradet (Dec. 6, 2016), *available at* https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/. .

64 *See Ross v. St. Jude Medical Inc.*, No. 2:206-cv-06465 (C.D. Cal. filed Aug. 26, 2016).

other heart-regulating implants.[65] According to the complaint, these medical devices are vulnerable to hackers:

> For example, by forging, altering, or replying to previously captured transmissions to or from an implanted cardiac device, a bad actor could monitor and modify the implant without necessary being close to the victim. Such attacks can put at risk the safety of the patient with the implantable device, with fatal consequences in certain cases.[66]

The plaintiff filed his complaint after a recent report by Muddy Waters Capital which claimed to find security deficiencies in St. Jude Medical's remotely-controlled medical devices.[67] As with the lawsuits involving connected cars and toys, the plaintiff alleged that St. Jude Medical's devices were susceptible to a data breach but not that these devices had in fact been hacked. Just a few months after filing his complaint, the plaintiff voluntarily dismissed the litigation without prejudice.

III. INSURANCE COVERAGE ISSUES RAISED BY THE IoT

A. Cases Dealing with the Definition of "Property Damage"

Courts have long grappled with whether cyber-related losses are covered under first and third party insurance policies. In early cases, courts addressed coverage for losses to data or functionality of electronic devices that resulted from causes such as faulty equipment, power outages or malware. Today, courts all over the country continue to address these issues.

Generally speaking, policyholders have sought coverage for the loss of use of data or functionality of electronic devices on the ground that such losses involved property damage, which has been typically defined as including injury to or the loss of use of tangible property. In contrast, insurers have argued that such losses were not covered because those losses did not involve injury to or the loss of use of such property. Although courts have reached different conclusions on these issues, their reasoning may be instructive as courts begin to deal more specifically with coverage for tangible losses relating to IoT devices.

At one end of the spectrum is *American Guarantee and Liability Insurance v. Ingram Micro, Inc.*[68] The policyholder in that case, Ingram Micro, distributed "microcomputer products" and used a network ("Impulse") to track orders and keep information on its customers and products.[69] Due to a power outage, programming information which had been stored on Ingram Micro's mainframe computers was lost and had to be reprogrammed and Ingram Micro's data center was disconnected from the Impulse network for eight hours until a system switch was

---

65 *Id*. at ¶ 32.

66 *Id*. at ¶ 17.

67 *Id.* at ¶¶ 26 – 32; *see also* "St. Jude Medical, Inc.," Muddy Waters Capital LLC (August 25, 2016).

68 No. 99-185, 2000 U.S. Dist. LEXIS 7299 (D. Ariz. Apr. 18, 2000).

69 *Id*. at *2-3.

fixed.[70] Ingram Micro sought coverage for its resulting business and service interruption losses under an All Risks policy that Ingram Micro had procured from American Guarantee and Liability Insurance Company ("AGLIC"). [71] This policy provided coverage for "'[a]ll Risks of direct physical loss or damage from any cause, howsoever or wheresoever occurring . . . ."[72]

AGLIC argued that the All Risks policy did not cover Ingram Micro's business and service interruption losses because Ingram Micro's computer systems were not physically damaged, since the "power outage did not adversely affect the equipment's inherent ability to accept and process data and configuration settings when they were subsequently reentered into the computer system."[73] By contrast, Ingram Micro argued that the computer systems had been physically damaged because they had lost their functionality.[74]

The U.S. District Court for the District of Arizona sided with Ingram Micro, concluding that loss of programming information and customer configurations did constitute physical damage to tangible property. In so doing, the court explained:

> At a time when computer technology dominates our professional as well as personal lives, the Court must side with . . . [the] broader definition of "physical damage." The Court finds that "physical damage" is not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality.[75]

America Online, Inc. v. St. Paul Mercury Insurance Company represents the other end of the spectrum in these cases.[76] There, multiple class action suits had been filed against America Online ("AOL"), alleging that AOL's access software Version 5.0 caused plaintiffs' operating systems to crash and their computers to lose stored data. AOL tendered the defense of those suits to St. Paul Mercury Insurance Company, which had issued a commercial general liability (CGL) insurance policy to AOL.[77] The policy covered property damage, which was defined as:

---

70 *Id*. at *3-5.

71 *Id.* at *3.

72 *Id.*

73 *Id.* at *5-6.

74 *Id*. at *6.

75 *Id. See also Centennial Ins. Co. v. Applied Health Care Systems*, 710 F.2d 1288, 1291 (7th Cir. 1983) (underlying complaint that alleged faulty controllers caused the loss of electronically stored data "clearly raise[d] the spectre that liability for property damage [might] ensue."); *Computer Corner, Inc. v. Fireman's Fund Ins. Co.*, 46 P.3d 1264, 266 (N.M. Ct. App. 2002) (lower court had concluded data lost when policyholder reformatted a hard drive constituted tangible property, and the parties did not appeal that conclusion); *Retail Systems, Inc. v. CNA Ins. Companies*, 469 N.W.2d 735, 737 (Minn. Ct. App. 1991) (data on a computer tape was tangible constituted tangible property).

76 347 F.3d 89 (4th Cir. 2003).

77 *Id*. at 91-92.

> physical damage to tangible property of others, including all resulting loss of use of that property; or loss of use of tangible property of others that isn't physically damaged.[78]

St. Paul denied AOL's claim on the ground that the underlying complaints did "not allege damage to 'tangible' property" under the CGL policy.[79]

In the resulting coverage litigation, the U.S. District Court for the Eastern District of Virginia, and then the Fourth Circuit Court of Appeals, agreed with St. Paul. In so doing, the Fourth Circuit analogized the loss of use of software on a computer to a lock combination and the lock itself, noting that "when the combination to a combination lock is forgotten or changed, the lock becomes useless, but the lock is not physically damaged. With the retrieval or resetting of the combination – the idea – the lock can be used again."[80] With this in mind, the court then explained that although AOL's CGL policy "cover[ed] any damage that may have been caused to circuits, switches, drives, and any other physical components of the computer," it did not cover "the loss of instructions to configure the switches or the loss of data stored magnetically." [81] Because "[t]hese instructions, data and information are abstract and intangible," the court held that damage to them "is not physical damage to tangible property."[82] Other courts have followed *American Online* and similarly concluded that damage to electronic data is not covered property damage.[83]

B. Coverage for Damages Resulting from the Unauthorized Access to Data Under "Traditional" Liability Policies

Coverage disputes relating to data breaches may also be instructive as courts begin to deal with IoT-related coverage disputes. Policyholders seeking coverage for such breaches generally argue that their resulting losses constitute property damage under Coverage Part A of their general liability policies or advertising injury under Coverage Part B of those policies.

i. Data Breaches as Covered Property Damage

As a general matter, courts which have considered whether breach-related losses constitute "damage to tangible property," as required under CGL policies, have determined that they do not. For example, in 2012, the U.S. District Court for the Western District of Wisconsin addressed whether electronic funds in an on-line bank account were "tangible property" under a

---

78 *Id*. at 94.

79 *Id*.

80 *Id.* at 96.

81 *Id.*

82 *Id.*

83 *See e.g*., *Ward General Ins. Services, Inc. v. Employers Fire Ins. Co*., 114 Cal. App. 4th 548, 556 (Cal. Ct. App. 2003) (the loss of a computer database was not a direct physical loss or damage to covered property under the first party insurance policy at issue, as the court rejected the idea that "*information, qua* information, can be said to have a material existence, be formed out of tangible matter, or be perceptible to the sense of touch.").

commercial excess liability and "Bis-Pak" policy.[84] In *Carlon*, the policyholder, Delaget, had been hired by a restaurant group to manage its finances.[85] The restaurant group's accounts were allegedly exposed to a virus on Delaget's computer and several hundred thousand dollars were stolen from the restaurant group's bank account.[86] Delaget argued that the term "tangible property" was reasonably susceptible to more than one meaning, and therefore, should be read to include electronic bank account funds.[87] The district court disagreed.[88] It concluded that the electronic funds at issue were not covered under the third party liability coverage form because there was no required loss of use of *tangible* property.[89]

More recently, a federal district court in Alabama reached a similar conclusion.[90] In that case, the policyholder, Camp's Grocery, was sued by three credit unions after a breach of its computer network.[91] In the underlying suit, the credit unions alleged that the data breach had compromised their customers' credit card, debit card and check card information.[92] Camp's Grocery sought coverage under a business owners insurance policy and when the insurer refused to provide coverage, Camp's Grocery filed suit.[93] Among other things, Camp's Grocery argued that the physical credit, debit and check cards were "tangible property" and that the losses suffered by the credit unions in replacing these cards was "covered property damage."[94] Rejecting Camp's Grocery's argument, the U.S. District Court for the Northern District of Alabama concluded that the underlying claims were based on compromised *intangible* data contained on the cards that made the cards unusable.[95]

ii. Data Breaches as Advertising Injury

The term "advertising injury" is typically defined in CGL policies as "a. Oral or written publication of material that slanders or libels a person or organization or disparages a person's or organization's goods, products or services; b. oral or written publication of material that violates a person's right of privacy; c. misappropriation or advertising ideas or style of doing business; or d. infringement of copyright, title or slogan." Unlike the recent decisions considering whether breach-related losses constitute property damage, courts have reached different results when deciding whether such losses qualify as advertising injury.

---

84 *See Carlon Co. v. DelaGet LLC*, No. 11-cv-477, 2012 U.S. Dist. LEXIS 70836 (W.D. Wis. May 21, 2012).

85 *Id.* at *3.

86 *Id.*

87 *Id.* at *14-15.

88 *Id*. at *14.

89 *Id*.

90 *See Camp's Grocery, Inc. v. State Farm Fire & Cas. Co*., No. 4:16-cv-0204, 2016 U.S. Dist. LEXIS 147361 (N.D. Ala. Oct. 25, 2016).

91 *Id.* at *2.

92 *Id*.

93 *Id*. at *1.

94 *Id.* at *21.

95 *Id.*

In April 2011, Sony Corporation suffered a massive data breach in its PlayStation video game online network, which led to the theft of millions of customers' private information. Sony faced claims following a hack and it sought coverage under its general liability policies. In *Zurich American Insurance Company v. Sony Corporation*, a New York trial court was asked to decide whether the insurance companies were obligated to provide coverage for these claims.[96] In an oral opinion issued by Judge Oing, the court held that a "publication" took place when hackers breached Sony's network even though the hackers did not actually make the stolen information public.[97] However, pursuant to the general liability policies issued by Zurich, the "publication" had to be made by Sony itself.[98] Coverage could not be triggered by the actions of third parties.[99] Thus Zurich's policies did not cover Sony's losses because the hackers rather than Sony were responsible for the "publication."[100]

On the other hand, in *Travelers Indemnity v. Portal Healthcare Solutions, L.L.C.*, the Fourth Circuit held that the insurer was obligated to defend its policyholder in a class action lawsuit alleging that the policyholder had made private medical records available on the Internet for several months.[101] In that case, confidential patient records kept by a medical records company were made available to unauthorized users.[102] The medical records company, Portal Healthcare, sought coverage under two commercial general liability policies for a class action law suit that had been filed against it.[103] The insurer argued that it was not obligated to provide coverage because Portal Healthcare's conduct did not effect a "publication" and no "publicity" occurred when Portal Healthcare posted the records online."[104] The district court disagreed, concluding that making the records publicly available on the Internet amounted to a "publication" that gave "unreasonable publicity" to and "disclose[d] information about patients' private lives" under the commercial general liability policies even though no third party was alleged to have viewed the information and Portal Healthcare took no steps to attract public attention to the information.[105]

On appeal, the Fourth Circuit affirmed the district court's decision, holding that the insurer had a duty to defend Portal Healthcare in the underlying class action because the alleged conduct at least potentially constituted a publication of a the patients' confidential information.[106]

---

96 No. 651982/2011, 2014 N.Y. Misc. LEXIS 5141 (N.Y. Sup. Ct. Feb. 21, 2014).

97 *Id.* at *70.

98 *Id*.

99 *Id.*

100 *Id.*

101 35 F. Supp. 3d 765 (E.D. Va. 2014).

102 *Id.* at 768.

103 *Id.*

104 *Id.* at 770-72.

105 *Id.*

106 644 F. App'x 245, 247-48 (4th Cir. 2016).

C. ISO Endorsements

In response to coverage disputes under traditional policies involving the loss of inability to access data and the unauthorized access to data, the Insurance Services Office ("ISO") has dealt with whether to exclude or limit coverage under tranditional policies for cyber-related losses. For example, after some courts had determined that electronic data could constitute tangible property, in 2001 the ISO issued a CGL coverage form which explicitly provided that electronic data was not tangible property.[107] In 2004, the ISO then introduced an exclusion (p) in the CGL form for "Damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."[108] But that same year, the ISO also introduced an endorsement through which policyholders could buy back limited coverage for "'property damage' because of all loss of 'electronic data' arising out of any one 'occurrence.'" That same endorsement defined the term "property damage" for purposes of the endorsement to include the "[l]oss of, loss of use of, damage to, corruption of, inability to access, or inability to properly manipulate 'electronic data', resulting from physical injury to tangible property. . . ."[109] Thus, this endorsement would apply where there has been a loss of or inability to access or manipulate electronic data only where there had otherwise been injury to tangible property.[110]

i. ISO Endorsement CG 24 13 04 13

More recently, through endorsements which went into effect in April 2013, the ISO amended the definition of "advertising injury" to which Coverage Part B applies. Recall that CGL policies typically define "advertising injury" as:

> a. Oral or written publication of material that slanders or libels a person or organization or disparages a person's or organization's goods, products or services; b. oral or written publication of material that violates a person's right of privacy; c. misappropriation or advertising ideas or style of doing business; or d. infringement of copyright, title or slogan.

Endorsement CG 24 13 04 13 removes subpart (b) of that definition – and in so doing (inasmuch as policyholders have relied on subpart (b) in seeking coverage for data breaches), this endorsement arguably defeats coverage in most cases for cyber liability claims as "personal or advertising injury."

---

[107] ISO Policy Forms, Form Number CG 00 01 10 01. That amendment defined "electronic data" as "information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment."

[108] ISO Policy Forms, Form Number CG 00 01 12 04.

[109] ISO Policy Forms, Form Number CG 04 37 12 04 at D.17.

[110] ISO Policy Forms, Form Number CG 04 37 12 04. That same year, the ISO also introduced a claims made coverage for liability due to the loss of data, where computer hardware has not also been damaged. ISO Policy Forms, Form Number CG 00 65 12 04.

ii. ISO Endorsement CG 21 06 05 14

Finally, the ISO endorsement CG 21 06 05 14 , which went into effect in May 2014, impacts both Coverage Parts A and B by seeking further to limit recovery for cyber-related losses under traditional policies. With respect to Coverage Part A (bodily injury and property damage), the endorsement replaces exclusion (p) of CGL policies with the following:

> This insurance does not apply to: . . . [d]amages arising out of: (1) Any access to or disclosure of any person's or organization's confidential or personal information, including . . . any other type of nonpublic information; or (2) The loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.

"Electronic data" means "information, facts or programs stored as or on, created or used on, or transmitted to or from computer software . . . ." This endorsement also provides that the exclusion applies even if "damages are claimed for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred by [the named insured] or others arising out of" that which is the subject of the exclusion.

Notably, there are two versions of this endorsement. Both versions have the language quoted above, but the second version also expressly excepts bodily injury from the exclusion by providing that "[u]nless Paragraph (1) above applies, this exclusion does not apply to damages because of 'bodily injury.'" This version of the endorsement thus indicates that damages due to bodily injury which arise out of "[t]he loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data" may not be excluded from coverage, as long as the bodily injury did not arise from access to or disclosure of a person or organization's nonpublic information. This variation of endorsement CG 24 13 04 13 will likely be "front and center" in future coverage disputes, where policyholders are liable for bodily injury due to the hacking or other malfunctions of IoT devices.

Finally, with respect to Coverage Part B (personal and advertising injury), CG 21 06 05 14 also states:

> This insurance does not apply to: . . . "[p]ersonal and advertising injury" arising out of any access to or disclosure of any person's or organization's confidential or personal information . . . [t]his exclusion applies even if damages are claimed for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred by you or others arising out of any access to or disclosure of any person's or organization's confidential or personal information.

An ISO executive explained the rationale for endorsement CG 21 06 05 14 at the time that it was introduced:

> At the time the ISO Commercial General Policies (CGL) were developed, certain hacking activities or data breaches were not prevalent and, therefore coverages related to the access to or disclosure of personal or confidential information and associated with such events were not necessarily contemplated under the policy.

> As the exposures to data breaches increased over time standalone policies started to become available in the marketplace to provide certain coverage with respect to data breach and access to or disclosure of confidential or personal information.[111]

Thus, the intent of the CG 21 06 05 14 seems to be to direct policyholders to standalone policies for coverage for cyber-related claims, with the notable exception of claims for bodily injury, where policyholders have purchased coverage with that version of the endorsement.

D. Coverage for Data Breaches Under Stand-Alone Cyber Policies

At the same time that courts have reached mixed results (at best) as to whether coverage is available for cyber-related incidents under traditional policies, and against the backdrop of the ISO's exclusionary endorsements, the market for stand-alone "cyber" policies has grown. Unlike traditional policies, which often have standard wording, there is no standard wording for cyber-related policies. Cyber policies typically present coverages for discrete types of cyber-related losses, such as first and third party losses arising from data breaches, network interruption, and extortion.

Although specialized policies have gained popularity in recent years, so far there have been few reported court decisions regarding the scope of coverage under these policies. Although the case law is thus less well-developed, a few key cases underscore the importance of paying attention to policy terms and understanding the scope of coverage even when purchasing a specialized policy.

One of the first litigated disputes involving a stand-alone cyber insurance policy was *Columbia Casualty Company v. Cottage Health System*.[112] In that case, Cottage Health suffered a data breach which released private health care information on approximately 32,500 patients that was stored on its servers.[113] Columbia Casualty had issued a stand-alone NetProtect360 cyber insurance policy to Cottage Health and following the data breach, Columbia Casualty sought a declaration in the U.S. District Court for the Central District of California that it was not obligated to provide coverage for Cottage Health's losses.[114] More specifically, Columbia Casualty alleged that (1) the breach occurred because Cottage Health and/or its third party vendor stored the patient information on a system that was Internet-accessible and without the proper security measures, and (2) Cottage Health violated non-delegable duties under California law to maintain the security of confidential medical records and to detect and prevent data breaches on its systems.[115]

---

[111] "ISO Comments on CGL Endorsements for Data Breach Liability Exclusions," INS. J., July 18, 2014, *available at* http://www.insurancejournal.com/news/east/2014/07/18/332655.htm.

[112] No. 2:15-cv-03432 (C.D. Cal. filed May 5, 2015).

[113] *Id.* at ¶ 16.

[114] *Id.* at ¶¶ 7-8.

[115] *Id.* at ¶¶ 17-18. Ultimately, this case was not decided on the merits. A few months later, the U.S. District Court Judge dismissed the suit to allow the parties to pursue alternative dispute resolution as provided for in the NetProtect360 cyber insurance policy.

Another early case was *Travelers Property Casualty Company of America v. Federal Recovery Services*.[116] Federal Recovery was in the business of processing, storing, transmitting and handling electronic data for other companies.[117] Federal Recovery entered into a Servicing Retail Installment Agreement with Global Fitness, pursuant to which Federal Recovery agreed to process member accounts and transfer member fees to Global Fitness.[118] A dispute erupted between the companies and Global Fitness sued Federal Recovery, alleging that Federal Recovery had retained possession of member data and interfered with Global Fitness' business dealings.[119] Federal Recovery tendered defense of the suit to Travelers, which had issued a CyberFirst Technology Errors and Omissions Liability Form Policy to Federal Recovery.[120]

Pursuant to the CyberFirst policy, Federal Recovery was entitled to coverage for losses caused by an "errors and omissions wrongful act," which was defined as "any error, omission or negligent act."[121] But in its complaint, Global Fitness alleged Federal Recovery "knowingly withheld [data from Global Fitness] and refused to turn it over until Global [Fitness] met certain demands.[122] Thus, "[i]nstead of alleging errors, omissions, or negligence, Global [Fitness] allege[d] knowledge, willfulness, and malice."[123] Accordingly, the U.S. District Court for the District of Utah concluded that Travelers did not have a duty to defend Federal Recovery in the Global Fitness suit.[124]

Additionally, just last year, in *P.F. Chang's China Bistro, Inc. v. Federal Insurance Company*, the U.S. District Court for the District of Arizona was asked to weigh in on the scope of coverage under a stand-alone cyber insurance policy. [125] P.F. Chang's, like many merchants, was unable to process credit card transactions itself.[126] As a result, it entered into an agreement with a third party, Bank of America Merchant Services (BAMS), to facilitate the processing of credit card transactions with the banks who issue credit cards.[127] Pursuant to the agreement, P.F. Chang's agreed to pay any fines, fees, or penalties imposed on BAMS by credit card associations, based on P.F. Chang's acts or omissions.[128]

---

116 103 F. Supp. 3d 1297 (D. Utah 2015)

117 *Id.* at 1298.

118 *Id.* at 1299.

119 *Id.* at 1300.

120 *Id.* at 1301.

121 *Id*. at 1302.

122 *Id*.

123 *Id*.

124 *Id*.

125 No. CV-15-01322, 2016 U.S. Dist. LEXIS 70749 (D. Ariz. May 31, 2016).

126 *Id.* at *3.

127 *Id.*

128 *Id.* at *4.

In June 2014, P.F. Chang's learned that computer hackers had obtained about 60,000 credit card numbers belonging to P.F. Chang's customers and posted these numbers to the Internet.[129] After the cyber incident, credit card associations imposed on BAMS and, in accordance with their agreement, BAMS passed along the fees to P.F. Chang's.[130] P.F. Chang's then sought coverage for cyber-related losses from Federal Insurance under a Cybersecurity by Chubb Policy.[131] Federal Insurance reimbursed P.F. Chang's for $1.7 million in costs incurred by P.F. Chang's as a result of the data breach but it refused to reimburse P.F. Chang's for the fees assessed by BAMS.[132]

P.F. Chang's filed suit against Federal Insurance and Federal Insurance moved for summary judgment.[133] In support of its motion, Federal Insurance argued that the BAMS fees did not constitute a "Loss" as it was defined under the policy and, even if it did, coverage was eliminated by two exclusions which precluded coverage for liabilities assumed by P.F. Chang's without Federal Insurance's consent.[134] The Arizona federal district court agreed with Federal Insurance, concluding that the BAMS fees did not fall under the policy's definition of "Loss" and, in any event, these fees fell within the policy's exclusions concerning assumed liabilities.[135]

IV. IoT COVERAGE ISSUES

To date, courts deciding coverage disputes following a data breach have considered whether the loss of electronic data constitutes property damage. But with IoT products, a cyber-related loss could fall under the more traditional definition of covered property damage.

For example, the 2008 hack of a Polish train system discussed above resulted in a train derailment that injured at least 12 passengers and may very well have caused damage to the passengers' personal property and the property in the vicinity of the incident. In a situation like that one, the train company might, in the first instance, seek coverage for any third party claims under traditional general liability policies. If those general liability policies exclude coverage based on the unauthorized access of the train's electronic systems, there might well not be coverage. As discussed above, ISO endorsement CG 21 06 05 14 excludes "[d]amages arising out of: . . . (2) [t]he loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data." This would arguably exclude property damage (and, unless the adopted endorsement contains the limited exception, bodily injury) resulting from the hack if the train derailment were considered as damage "arising out of . . . [the] corruption of . . . electronic data." Having said this, policyholders like the train company might argue (especially as to policies that have not incorporated the more recent ISO endorsements, or that have adopted the variant of CG 21 06 05 14 which excepts bodily injury) that the focus should be on the

---

129 *Id.*

130 *Id.* at *6.

131 *Id.*

132 *Id.* at *5-7.

133 *Id.* at *1.

134 *Id.* at *11-23.

135 *Id.* at *14-15, 24-25.

resulting injury (not the cause), and that bodily injury and/or property damage emanating from the unauthorized access to data therefore should be covered.

The train company might also look to its cyber insurance policy for coverage. But unlike general liability policies, those policies tend to focus coverage for costs of more "typical" post-breach losses such as customer notification, credit monitoring, legal fees and fines. By contrast, those policies typically do not provide coverage for bodily injury or property damage.

Recently, however, certain carriers have started to offer insurance policies that include broader coverage for the types of losses that might occur after a cyber-incident. For example, some cyber insurance policies now cover bodily injury, property damage, business interruption and product liability related to a data breach. Even still, cyber policies offering coverage for a wider array of damages are not as commonplace right now; most cyber insurance policies do not provide such coverage. As a result, even if a company, like the train company, had purchased traditional insurance coverage and a stand-alone cyber insurance policy, that company might face complex insurance-related issues when property damage and/or bodily injury occurs after a cyber-attack, as in the example just discussed.

Beyond coverage for bodily injury and property damage, the interconnectedness of a widespread number of devices presents other issues. Information stored on one IoT device is only as protected as the least secure device connected to the same network. Regardless of how secure a particular device is on its own, if it is connected to a network, the security of that device could be vulnerable due to lack of security of a completely different device connected to that network. This has the potential to compromise a policyholder's ability to seek coverage under it stand-alone cyber policy.

As mentioned above, in the case of *Columbia Casualty Company v. Cottage Health System*, Columbia Casualty sought a declaration that it was not obligated to provide coverage for its policyholder, Cottage Health, under a NetProtect360 cyber insurance policy after a data breach released tens of thousands of patient medical records stored electronically on Cottage Health's servers.[136] Columbia Casualty alleged, in part, that the cyber incident occurred because Cottage Health and/or its third party vendor had stored the patient files on a system that lacked the proper security measures contrary to the representations Cottage Health made on its insurance application.[137]

Such representations are commonly required in cyber insurance policy applications. Where the security of one connected device depends on all other devices connected to the same network (potentially including devices outside of the policyholder's control), this could complicate a policyholder's ability to make representations regarding the security measures in place and/or comply with a cyber insurance policy requirement to maintain certain security measures.

---

[136] No. 2:15-cv-03432.

[137] *Id.* at ¶¶ 17-18.

V. CONCLUSION

The explosion of the IoT brings many opportunities. But it also comes with a wealth of unique risks. Controlled demonstrations and actual cyber incidents have shown IoT products to be susceptible to attacks. The next wave of insurance coverage litigation may very well involve these products as manufacturers derive new and creative ways to connect everyday objects to the Internet. As more disastrous losses occur with the mainstream use of these products, courts will be faced with complicated insurance coverage questions regarding the interplay between various insurance policies. As a result, it will be all the more important for insurance carriers and policyholders to pay careful attention to the specific terms of their insurance policies to make sure that the available coverage satisfies both parties' expectations.