

Insurance Implications Of 'The Internet Of Things'

Law360, New York (October 3, 2016, 3:30 PM EDT) --

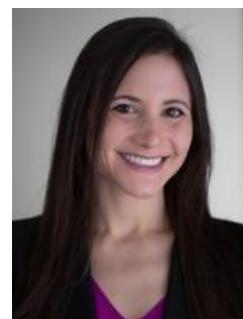
We live in a constantly changing and increasingly interconnected world. The internet of things refers to the network of connected devices that can collect and exchange data. Do you want to make sure that you shut your garage door? Do you want to make sure that the thermostat in your office is set to a cool 66 degrees Fahrenheit? Today, you can remotely monitor these devices from many miles away. In 2015, there were approximately 10 billion IOT devices, ranging from automobiles to fitness GPS devices to washers and dryers.[1] And researchers estimate that by 2020, the number of connected devices will reach 34 billion.[2]



Ellen MacDonald Farrell

This ever-changing landscape presents new and exciting opportunities for policyholders and insurers alike. But at the same time, the interconnectedness of these products opens up a whole new realm of vulnerabilities.

The tangible and intangible nature of IOT products can present complex issues concerning coverage under both traditional insurance policies and stand-alone cyberinsurance policies. For example, if a fire erupts at a hotel and the guests of the hotel file suit over the damage to their belongings, the hotel would typically look to its general liability policy for coverage of those third party claims. But in today's environment, that fire could have started because a computer hacker accessed the hotel's security system — and that computer hacker could have gained access due to a lapse in security in a completely different device that was connected to the same network.



Rachel Raphael

On the one hand, the hotel's general liability policy may provide coverage for the claims brought by the hotel guests. On the other hand, the hotel's policy may exclude such coverage. Indeed, many general liability policies have started to incorporate the exclusion endorsement introduced by the Insurance Services Office (ISO) and effective May 2014. With that endorsement, the policy excludes "[d]amages arising out of: (1) Any access to or disclosure of any person's or organization's confidential or personal information ... ; or (2) The loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data." The endorsement also provides that this 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. The endorsement specifies that "electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software" In the hotel example, damage resulting from access to the security system may

have arguably been excluded if the hotel's policy incorporated this ISO endorsement and this was considered damage arising out of corruption of electronic data.

In contrast to general liability policies, stand-alone cyberpolicies tend to focus on data loss and coverage for breach notification as opposed to physical damage. Indeed, many cyberinsurance policies expressly exclude coverage for claims alleging bodily injury and property damage.

More recently, some carriers have started to broaden coverage to include the physical loss that may arise from a cyber-attack. For example, there are certain cyberpolicies that now offer coverage for bodily injury, property damage, business interruption and product liability related to cyberincidents. Despite these more recent developments, most cyberpolicies do not provide such coverage. Thus, even if the company has a traditional general liability policy and a stand-alone cyber policy, coverage issues may arise when property damage occurs because an organization's systems have been compromised, as in the example above.

Additionally, the interconnected nature of IOT devices adds an additional layer of complexity. Information stored on one connected device is at risk not just based on the security of that device, but on the security of all other devices connected to the same network. This aspect creates a host of new cyber-related risks: a wealth of new information may be open for attack, and this new information may be even more vulnerable than before. This can potentially compromise a company's right to coverage under a stand-alone policy. For example, in the case of *Columbia Casualty Company v. Cottage Health System*, the insurer sought a declaration that it was not obligated to provide coverage to the policyholder under a NetProtect360 cyberinsurance policy for a data breach that disclosed tens of thousands of patient medical records stored electronically on the policyholder's servers.[3] The insurer alleged, in part, that the data breach took place because the policyholder and/or its third party vendor had stored the patient files on a system that lacked the proper security measures. According to the insurer's complaint, the policyholder had made representations regarding its cybersecurity measures in its application for the NetProtect360 policy.

Although *Columbia Casualty* was dismissed so that the parties could pursue alternative dispute resolution, the case raises an important issue for policyholders with IOT devices. The security of a connected device depends on all other devices connected to the same network and some of those other devices may be outside of the policyholder's control. As a result, this may complicate a policyholder's ability to (1) make representations regarding the security measures in place, and (2) comply with a cyberinsurance policy requirement to maintain certain security measures.

The next wave of coverage litigation may very well involve these IOT products as they become more mainstream. And as losses continue to arise in connection with these products, it may highlight the ambiguities in current insurance offerings and generate more complicated coverage disputes. It is important for policyholders and insurance carriers alike to pay close attention to the specific language of and interplay between the insurance policies at issue to make sure that coverage matches both parties' expectations.

—By Ellen MacDonald Farrell and Rachel Raphael, Crowell & Moring LLP

Ellen Farrell is a senior counsel in Crowell & Moring's Washington, D.C. office and a member of the firm's insurance/reinsurance group. Rachel Raphael is an associate at Crowell & Moring's Washington, D.C. office and also a member of its insurance/reinsurance group.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] "BI intelligence projects 34 billion devices will be connected by 2020," Business Insider (Nov. 6, 2015), available at <http://www.businessinsider.com/bi-intelligence-34-billion-connected-devices-2020-2015-11>.

[2] *Id.*

[3] See *Columbia Cas. Co. v. Cottage Health Sys*, No. 2:15-cv-03432 (C.D. Cal.) (filed May 7, 2015).

All Content © 2003-2016, Portfolio Media, Inc.