LAW360

January 3, 2014

Coverage Risks in the Age of the 'Internet of Things'

by Lon Berk and Paul Moura


The "Internet of things" is here. According to Cisco, sometime during 2008, the number of things connected to the Internet exceeded the number of people. Cows, corn, cars, fish, medical devices, appliances, power meters — practically any item imaginable has been or can be connected. Eventually, we will be able to "sync" an entire home so that its heating system is programmed to adjust to weather patterns and inhabitants' activities, its dishwasher automatically orders soap refills, its refrigerator is always stocked with milk (or beer), and maybe even its lights blink on and off when important emails are received.

These are just a few examples of what can be done with "the Internet of Things" ("IOT") — ordinary objects and devices able to process and transmit information based upon their environments that they then communicate to servers running algorithms designed to anticipate and address user needs. Businesses ranging from small startups to long-standing conglomerates are now embedding adaptive "smart" technologies into even mundane products, including window shades, light bulbs and door locks.

While IOT devices create obvious value, they also expand risk. In effect, we are creating an "infrastructure for surveillance," that constantly generates critical, sometimes exceptionally private, data transmitted for use on servers perhaps thousands of miles away. Although the benefits of this infrastructure are evident, the risks can be hidden within a technological "black box." The degree to which our well-being depends upon the integrity and security of networks, software and data will increase exponentially.

If an IOT device malfunctions, or if data or software is compromised or lost, individuals and businesses may suffer devastating losses. Dosages of critical medication might be missed, for instance, or needed medical treatments omitted. In fact, the risks posed by IOT have already attracted the attention of regulatory authorities. This past June, the U.S. Food and Drug Administration surveyed the industry and decided to update its guidance on cybersecurity for IOT medical devices and the Federal Trade Commission held a symposium addressing IOT issues on Nov. 19.

As use of these products continues to expand, such risks will be realized and manufacturers will look to their insurers for defense and indemnity protection. Coverage for products liability is typically provided under liability policies, which can be written on an occurrence or claims-made basis. Liability of the manufacturer of a malfunctioning fire alarm that fails to alert homeowners of a fire should be covered under such policies, as should bodily injuries or property damage caused by other defective products, including products that are part of the IOT. Injuries from such products may result not only from a device's failure to work but also from a network's failure to provide communications as needed. These failures, as well as the more traditional product failures, should continue to be covered if insurance is to continue to serve its function and transfer financial risk.

Coverage Risks in the Age of the 'Internet of Things'
by Lon Berk and Paul Moura | Law360, January 3, 2014

Liability policies generally define the products risk to include

All bodily injury and property damage occurring away from premises you own or rent and arising out of your product or your work except:

1. products that are still in your physical possession; or
2. work that has not yet been completed or abandoned.

The policies define "your products" to be any property (other than real property) manufactured, sold, handled, distributed or disposed of by the insured and to include warranties or representations made at any time with respect to the fitness, quality durability, performance or use of your product; and the providing of or failure to provide warnings or instructions.

Liabilities for malfunctions of IOT products appear to fit squarely within this definition. There are, however, some complications that insurers might put forward were they interested in denying coverage, and policyholders will need to examine their insurance proactively to avoid the uncertainty and cost of coverage litigation.

Coverage for IOT risk is complicated by the fact that the devices add value and efficiency by communicating with each other and distant servers on which data is stored and algorithms run. Indeed, this interoperability is the critical and promoted feature of IOT products. To see how this can complicate the coverage question, let us take a concrete example.

Let us imagine a refrigerator — the eFridge — that communicates data concerning the products it holds. When combined with complementary devices — called eShelves — it is able to keep track of all food in the kitchen. The refrigerator also keeps track of its states, including its internal temperature, and transmits its state data and food stocked to a server maintained by smartKitchens Inc., at a distant location. On this server the data is stored and analyzed by an algorithm designed by smartKitchens' software engineers. The algorithm, based upon eFridge state data and data on stocked food, generates recommended recipes for the week so that all food is used before it is spoilt. The recommendations sent from the server to the eFridge appear on a screen on the refrigerator's front door.

There are two Internet transport protocols, TCP and UDP. The latter is often used when broadcasting within a network is needed (as it is so that the eShelves can be configured) and can be cheaper to implement, but it is also less reliable because communicating devices receive no notice when UDP datagrams — the electronic containers of transmitted data — are lost or dropped. The eFridge is designed to use UDP, and the software engineers have developed their algorithm to deal with the problem of dropped datagrams as follows. Rather than generating a warning that there is incomplete information, the algorithm assumes that the refrigerator's state is consistent with the average state maintained over the prior two weeks. This is done to avoid multiple appearances of "error" messages on the eFridge door/screen and to increase customer satisfaction.

Now imagine that one week the server fails to receive datagrams regarding the state of the refrigerator on Monday, during which for some unknown reason the temperature inside the refrigerator exceeded room temperature. Unfortunately, as of Monday, the refrigerator contained a pound of mussels, which as a result of the temperature change are spoilt. Data concerning this

temperature increase were not received by the server, and therefore the algorithm, having been designed to assume that the temperature was maintained at its average, recommends a recipe for Wednesday of Mussels Provençale. As a result, the consumer sustains a very serious case of food poisoning and naturally seeks compensation from smartKitchens, which demands coverage from its insurer. Is smartKitchens covered?

The event appears to be squarely within the sort of products liability coverage that product manufacturers and distributors expect. There is a product away from the insured's premises that made a "defective" recommendation and caused bodily injury. As such, there should be coverage.

But an aggressive insurer could construct an argument to the contrary. They might contend that in fact the injury was caused by the algorithm, not the refrigerator, and that had the algorithm been designed to indicate through an error signal that data had not been received, there would have been no recommendation of Mussels Provençale on Wednesday. Insurers might contend that the algorithm constitutes "work that has not been completed or abandoned," pointing to the fact that the engineers have the ability to change the algorithm to address the possibility of spoilt mussels and that therefore the risk is not within the product's coverage.

Such an argument should ultimately fail. The fact that smartKitchens' software engineers can update the algorithm does not mean that they have not "completed or abandoned" it for purposes of the insurance policy. Moreover, liability policies generally provide that "work which requires further … correction … because of defect or deficiency, but which is otherwise complete, shall be deemed completed." In fact, here, smartKitchens let the algorithm run as it was designed to and it did so. Nonetheless, although the insured should eventually obtain the benefit of coverage, that could very well be only after protracted and expensive litigation, reducing the value of the insurance purchased.

There is another argument as well the insurer might make. Since about 2003, liability policies have generally included an exclusion — exclusion p, on the Insurance Services Office Inc. form — barring coverage 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.

As used in this exclusion, electronic data means 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-ROM[s], tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.

An insurer might contend that the problem was created, not by the eFridge, but by the loss of electronic data, when the packets were dropped. They might use this argument to contend that coverage is barred. Again, however, the insured should prevail were the insurer to make such an argument. The algorithm functioned as it was designed. It did not fail to process data, but processed data exactly as intended. It was merely responding as designed to an unfortunate consequence of the decision to implement the UDP protocol. But here too, the insured is likely to find itself in an expensive coverage dispute, depriving the insured of the value of the insurance purchased.

As always, new technologies create new risks, and new risks create the possibility of coverage disputes. These disputes should be resolved in the insured's favor, as it is the responsibility of an insurer to draft policy language to clearly and unequivocally exclude risks. This rule has especial force where, as in our example, there is an expectation that liability for products would be covered. It should, in other words, be the responsibility of underwriters to understand the products they insure and clearly state if they do not desire to cover an attendant risk. Nonetheless, as the use of IOT devices continues and expands, the past has taught that we can expect to see risks expand and insurers attempt to restrict coverage.

Lon Berk is a partner in Hunton & Williams' New York office and has experience involving commercial and insurance disputes. He has represented clients in insurance disputes in state and federal, trial and appellate courts nationwide and in international arbitrations.

Paul Moura is an associate in Hunton & Williams' Los Angeles office where he focuses on complex insurance recovery matters and related business litigation, including counseling, audits and arbitration.