Hogan Lovells

What product manufacturers need to know about how the Internet of Things is changing the way that the U.S. Consumer Product Safety Commission views product safety

10 December 2018

The Internet of Things (IoT) has opened doors to enormous innovative opportunities for consumer product manufacturers. But it has also introduced a new twist in the way that innovation, product safety, and the U.S. government's regulatory framework coexist. Today, many refrigerators, coffee makers, and other common consumer products can send and receive data and communicate with other IoT devices. And these connected capabilities can also generate new risks to product-related safety.

The U.S. Consumer Product Safety Commission (CPSC) is one government agency with regulatory authority over IoT-connected devices. Tasked with protecting the public from risks of injury or death from the use of consumer products, the agency conducts research into product-related illness and injury, oversees product recalls, and issues regulations and standards for the manufacture of consumer products. The Commission also enforces a statute that mandates reporting of potentially unsafe products and imposes substantial civil penalties when a firm fails to do so.

In this hoganlovells.com interview, Steven Steinborn, a partner at Hogan Lovells in Washington, D.C., discusses the role of the CPSC in ensuring product safety for IoT-connected devices, and what companies must now consider when integrating products with capabilities that have never been available in those products before.

With the CPSC now an active player as part of the federal regulatory scheme that covers the IoT products, can you give us a quick overview of what companies need to know?

Steven Steinborn: The CPSC takes a very broad view of its jurisdiction, so anything being used by the consumer inside or outside the home that creates the risk of a hazard concerns them.

When the CPSC held a public hearing in May 2018, all the commissioners were in attendance, which shows a high level of interest at the Commission. My perception is that there are a number of companies that have done a lot of good thinking about the IoT, but aren't necessarily familiar with the CPSC and how it works. It would behoove them to understand more about the agency's mission and how it looks at health and safety risks, because when the CPSC holds a public meeting, companies are well-served to build-in the CPSC perspective in how it approaches product design, manufacturing, and handling of consumer complaints among other factors that have a bearing on safety.

For example, when you talk about interconnected elements of the home, the CPSC looks at the different types of risks that could be introduced. It's also important to note that the CPSC's legal authority is very broadly written, so while their regulations are not likely to mention the IoT, they have broad regulations that give them the jurisdiction to regulate many aspects of connected devices in use in and around the home. At the risk of over-simplifying CPSC's mandate, companies should focus on two types of hazards: (1) traditional hazards that could result from any type of product due to a new technology or application of an existing technology that triggers a safety concern; and (2) potential hazards that are unique to IoT devices because of the technology they incorporate and the manner in which the products play alone and in interaction with other devices within the home.

What types of potential hazards are on the CPSC's radar in terms of IoT-connected consumer products? And what hazards are associated with the IoT-enabled "smart" home?

Steinborn: Remote connectivity of household appliances via the internet offers many conveniences and features that could dominate a given type of product. For example, imagine a stove that can be turned on remotely by the consumer. Of concern is if the stove is unexpectedly turned on without the consumer's knowledge, creating a potential hazard. The risk profile of many in-home products is arguably different if they are powered on when the consumer is present versus if the unit is powered on without the knowledge or supervision of someone present.

When smart homes link multiple functions to a single source, the risk of a malfunction in one feature of a complex system raises the risk that another element of the home control system may fail. Consider a routine software download that contains an undetected "bug." It is conceivable that the software upgrade does not go as planned, that a smoke detector system linked to the smart home system may become inoperable. Moreover, the software-caused failure may go undetected, exacerbating the potential safety problem.

If the CPSC doesn't write regulations specifically for IoT devices, how do consumer product companies know how to comply?

Steinborn: A company focused on CPSC compliance is concerned about either a specific standard, like an electrical standard, that already exists — although there are not a lot of standards that exist for IoT-type products — or the CPSC's definition of a general hazard, which has two elements: first, establishing that there is a defect, which is essentially when a product doesn't operate as it was intended. A defect could be almost anything: a design defect, a manufacturing problem, or a manual with confusing instructions that inadvertently causes misuse of the product and a potential hazard.

Once a company determines there is a defect, they address the second element: does the defect create the risk of a “substantial product hazard” — a term that means a serious injury or risk of death. You may have very few incidents, but if they have potential to cause real harm, the CPSC considers that a substantial product hazard. Or you could have tens of thousands of incidents, but if the nature of the problem is such that nobody would ever really be harmed, then even though the product may not function the way the consumer expected, there may be no regulatory risk because there is no health or safety issue. CPSC articulates a number of factors companies should consider in this fact-specific exercise.

A defect or related health hazard is the crux of CPSC’s mission. They also have other statutes and standards that they apply and enforce that relate to specific hazards, such as electrical shock, flammability, choking, dangerous chemicals, and a range of labeling requirements as well.

Some consumer product safety challenges associated with IoT devices include: 1. preventing or eliminating hazardous conditions designed into products intentionally or without sufficient consideration, and 2. preventing or addressing "incidents of hazardization," where an otherwise safe product becomes hazardous through malicious, incorrect, or careless changes to its operational code. Please elaborate.

Steinborn: One focus of the IoT in the home can trigger potential electrical hazards. The CPSC spends a lot of time overseeing product recalls involving electrical hazards; these are sometimes design or misuse issues. One of the challenges of the IoT is that when you have this connectivity and your connected components weren’t originally designed to fit together — for example, a refrigerator is retrofitted so you can use it with your smart phone — are you introducing a level of functional instability or uncertainty that would not exist if you looked at the two parts separately? How do you understand, measure, and validate these potential new risks? Similarly, there is great pressure to miniaturize components to fit added electronics into existing designs or to make existing designs even more compact, such that IoT retrofits do not require the consumer to accept larger, heavier or bulkier products. Such efforts can change the safety dynamics in play when ion batteries are involved or various materials that could be potentially be exposed to greater levels of heat or there is less opportunity for heat to vent.

When we’re assessing hazards with clients at the design phase, we stress the importance of looking at design features that are new or novel. I may know a lot about a refrigerator, but I may not have a lot of testing or data when I modify the components of that appliance in a way that changes how it functions. Sometimes those changes will be inconsequential; a lot of electronics, for example, have circuit boards that trip and shut down the device so you don't have a fire risk from overheating. But sometimes you might look at those design safety features and say, well, that was adequate for the traditional product that we've been selling for years, but what about the product with the new features? Those are the kinds of questions that the CPSC is expecting companies to look at for themselves. From a company's standpoint, you obviously want to address these questions up-front and not as a consequence of consumer complaints after the product is in the marketplace. At the latter stage, the CPSC mandatory reporting requirements come into play, a challenging determination with significant consequences if a firm fails to report when in hindsight it is determined that they should have notified the CPSC.

Finally, a range of issues could emerge that will put into play CPSC's jurisdiction. There are some potential consequences some cite from IoT product concepts that have been mentioned as being of concern (or should be of concern) to the CPSC. For example, one concern is the hacking of home surveillance cameras to spy on the occupants of the home. CPSC has also pledged its willingness to be part of a broader dialogue with other federal agencies so its reach could be broadened although its input may not always directly impact the scope of its jurisdiction over IoT products.

You said that some IoT device manufacturers may not have CPSC compliance on their radar. What penalties do companies face if they fail to report?

Steinborn: If you have a statutory obligation to report to CPSC and fail to do so in a timely fashion, CPSC is authorized to impose civil penalties of up to around US$16 million. The typical civil penalties of the last couple of years have been between US$3 million and US$6 million — no small potatoes — but you also have a reputational issue and residual product liability concerns. So you may be paying millions of dollars to the government, but you could also be facing claims by private claimants in a product liability context. It is not by accident that I work closely with my product liability litigators on many matters that begin as CPSC issues.

So why does CPSC matter? It matters because the Commission is small, but it puts the burden on the manufacturer to establish that the products are safe in one of two ways. The first is design: making sure the product is made well and safely manufactured. And the second is through monitoring of consumer complaints as a critical source of information of a possible defect that could pose a hazard. In our experience, companies fail to identify a product hazard in a timely manner due to the failure to properly monitor and analyze consumer complaints.

What mistakes do companies make when they face a product safety issue and are obliged to report it to the CPSC?

Steinborn: Unanticipated product defects arise from any number of sources and often the root cause is unknown. The mistakes companies make typically arise in how they evaluate and respond to information that is suggestive of a potential problem related to safety.

Companies should take care to avoid treating a potential safety problem as a typical customer affairs issue. For example, the customer is unhappy because their oven is giving off a smoky smell. So we give the customer a brand-new unit or replace the circuit board, the customer is happy and the file is closed. Then another customer calls with the same problem and the circuit board is replaced and again the file is closed. Evidence of repeated smoking units could be a sign of a potential fire hazard. Yet if the company were only tracking "fire" reports, there would be no indication of a potential hazard. But if the number of replaced circuit boards were tracked and seen as high, and the cause investigated, one would presumably recognize that the circuit boards are smoking and the existence of a potential hazard closely evaluated. Is there an underlying problem? Is this a disaster waiting to happen? Have you contacted the circuit board maker? Revisited customer contacts going back in time? There are a series of questions one should ask each time a situation arises where safety issue could be involved.

Do not delay making a determination on reporting to CPSC until a root cause is determined. Electrical hazards and other sophisticated product designs make a root cause determination difficult to determine. A multi-prong operating system that incorporates IoT capabilities only complicates the number of potential factors that must be considered. The decision to report to CPSC does not require a root cause analysis determination, and a company is generally not well-served by delaying consideration of reporting until a root cause is determined. Similarly, companies sometimes place undue emphasis on their inability to reproduce incidents reported to it by consumers. While reproducing a hazard is important, the empirical experience of consumer complaints will in many instances be viewed by CPSC as more probative than the inability of the company to recreate the reported hazard. The complexity of IoT systems might yield a hazard arising in one part of the overall system will inevitably complicate a hazard analysis. From CPSC's perspective, this complexity does not change the weight given to the number of incidents, the severity of the potential hazard, and the other factors the CPSC considers in determining when a report is required.

Companies faced with a situation where a product hazard investigation is warranted should bear in mind that the CPSC essentially examines the "timeliness of reporting" in hindsight. CPSC does not typically conduct monitoring/testing of products. Rather, companies that receive consumer complaints or other evidence of a product hazard are required to report to CPSC. We advise companies to undertake an internal review taking account the very factors that CPSC itself applies when a problem comes to its attention. When this analysis supports a conclusion not to report to CPSC, the firm should document the basis for its decision.

Now let's say six months from now, the company receives 15 more similar incidents of what looked like an isolated complaint, and maybe you've got some injuries. So you report to the CPSC and CPSC says, when was your first report? You say it was six months ago. They say, well, you may have a problem in terms of timeliness of reporting, so you might have to do the recall, but there is also a risk of civil penalties. The firm pulls out its file memo and explains to the CPSC staff that it responsibly investigated the original complaint and based on a thorough review, it determined that it had no reporting obligation. After carefully monitoring consumer contacts, in light of additional complaints, the company revised its assessment and reported in a timely fashion.

Another area of caution is when a company is expanding into a field outside its core expertise. Company A is an established appliance company, and they partner with somebody that has experience with IoT-related connectivity and functionality, creating novel product features to Company A's product from a design, manufacturing, and customer experience perspective. Sometimes companies lack the knowledge or ability to apply the kind of know-how that they apply to their core products to the new products, in terms of performance-testing those new products before and after release. The solution isn't to walk away from promising business opportunities. Rather, a company should be thoughtful about choosing business partners with requisite expertise, and leverage the benefits of third-party testing labs that can provide objective measures by which to evaluate safety. Some of the most interesting projects I've worked on involved developing proprietary testing protocols to evaluate and ultimately establish a reasonable measure of product safety. A multidisciplinary team that can understand how the novel product's component parts fit together is invaluable. The dynamic growth of IoT products will place a premium on companies that can navigate these unfamiliar waters with great success.

A final mistake to avoid: a company identifies a problem, but either does not fully investigate the safety issue, or decides to unilaterally fix the problem and not report it to CPSC. If they have a reporting obligation and choose to just fix it on their own, they're taking some risk. If they fix the problem in a way that doesn't work, they've got a whole lot more risk when safety issues are reported by consumers. So, a company not well versed in CPSC requirements might instinctively decide to simply fix a problem and move on — that is not how CPSC works. Rather, the law requires that the company notify CPSC if reporting is triggered, and fix the problem in cooperation with the CPSC. Of course, not every product problem requires CPSC notification.

So you advocate that clients have internal monitoring programs?

Steinborn: Yes. Some companies generate monthly reports and have a quality team review them and look for patterns. In IoT-related situations, you're well served to have a robust internal monitoring program; maybe more than you would have for your typical product, because if it's a novel design and you don't have a lot of experience with it, you want to be more proactive about monitoring consumer feedback. One should also consider who sits on that internal review team. IoT products and systems are inevitably more complex and the requisite expertise should be represented to ensure that the full spectrum of potential hazards arising from the internet-connected features of the product are well understood. Then you can fine-tune that monitoring over time as you gain more experience with the product.

For example, wearable technology often uses micro batteries. If it was a normal wristwatch, you wouldn't expect to have any issues, but if you put a little battery in there that allows you to sync up with another product, then you have a potential new safety dynamic. Companies should look at connectivity issues from both the design phase and the monitoring-what's-happening-in-the marketplace phase. From CPSC's perspective, companies are responsible for both. If people are reporting that a device around their wrist is giving them an overheating sensation, you would pay attention, elicit more information, obtain the product for careful examination, and monitor consumer contacts going forward more carefully.

With the exciting future ahead for IoT, and the inevitable involvement of the CPSC, where can people turn who want to learn more about the CPSC and how should companies think about CPSC in developing the great innovations that lie ahead?

Steinborn: CPSC offers many resources on its website, including its Recall Handbook. This information provides a useful overview on many topics, including reporting to CPSC. Ultimately, legal compliance requires a company to carefully monitor and assess key facts and reach its own decision about potential product safety issues. An appreciation for CPSC's mission, and a practical understanding of how the Commission operates, is vital to IoT product development, commercialization, and successful marketing. CPSC has demonstrated interest in IoT products and those unfamiliar with CPSC, or unfamiliar with how established CPSC requirements apply to this emerging category of products and technologies, will be well-served by remaining mindful of the CPSC regulatory framework. Companies that understand the CPSC framework and guide product development and marketing accordingly will ensure that their pathway to IoT will thrive, and if an unexpected situation arises, safety problems should be addressed in a manner that doesn't make a difficult situation worse by inadvertently tripping over CPSC reporting and related requirements.

About Steven B. Steinborn

Steven Steinborn offers clients 31 years of experience in guiding informed business decisions in the heavily regulated consumer and technology industries. He has counseled a wide range of consumer products companies on reporting obligations and other requirements arising before the U.S. Consumer Product Safety Commission. His goal is to provide practical advice to help companies reach their goals by counseling on a range of critical issues, allowing companies to make strategic decisions. He partners with his diverse portfolio of clients to bring new products to market, navigating challenges as they arise.

Contacts

Steven B. Steinborn

Partner

> Read the full article online