How the Internet of Things could redefine product safety and liability in the EU

05 June 2018

How big is the Internet of Things (IoT)? It's likely that there will be tens of billions of connected devices in use by 2020. As this massive network of "things" keeps expanding, so do the number of questions about IoT-related product safety and liability issues.

When we're thinking about the standard of safety for IoT products, we need to look to the General Product Safety Directive (GPSD) and to other relevant product safety laws at both an EU and member state level.

In the event that a defective IoT product causes damage, the Product Liability Directive (PLD) is the key legislation that addresses product liability concerns. But advances in technology are outpacing the decades-old PLD. An evaluation now under way, however, should soon clarify some of the ambiguity arising from the evolving technology landscape, including new and more relevant definitions for defects, products, and producers.

In this hoganlovells.com interview, Valerie Kenyon, a partner focusing on product liability and safety in the Hogan Lovells London office, discusses the changes in and challenges to the EU's regulatory regime as the IoT continues to shape perceptions about product safety and liability.

Why are we so interested in IoT safety and liability?

Kenyon: IoT devices have become part of our everyday lives. They're in the hands and the homes of every conceivable demographic — not just adults or the tech savvy, but also children, the elderly, and vulnerable users. So it's important that there are modern and clear rules around the safety and compliance of these devices, and that businesses in the IoT space are aware of these rules and the risks and liabilities they may face.

In the EU product regulatory landscape, IoT products fall within the scope of the GPSD. Let's spend some time looking at the way the GPSD applies to connected devices.

How does the GPSD define a "safe" product?

Kenyon: According to the GPSD, a safe product "does not present any risk, or only the minimum risks compatible with the product's use, considered to be acceptable and consistent with a high

level of protection for the safety and health of persons."

The definition of a safe IoT product depends, in fact, on a host of factors, including the product's characteristics, composition, packaging, instructions, interaction with other products, safety warnings, and the categories of consumers likely to use it. So we can already see that IoT products are going to throw up some questions that we wouldn't necessarily need to think about in relation to conventional, nonconnected, electronic devices.

One question is, as a manufacturer, how do you warn about safety risks? If the consumer must have a mobile phone or an app in order to use the device, is it okay to give them safety information only on the phone or the app? In fact, is it preferable?

What about software? How do you feel about the situation in terms of safety, where a consumer has decided not to update their device with the latest safety-related patch? If something goes wrong, is the product to blame, or the consumer? And what about data-related risks, e.g. questions around hacking and cybersecurity?

These are just a few of the questions we're helping businesses with in the IoT product space. And some of these are really challenging issues, keeping experienced manufacturers, importers, and distributors very busy.

How is the EU legislator addressing these IoT-related issues?

Kenyon: The EU legislator is trying to keep up with these questions and develop policy in this area. In fact, we worked with the European Commission and the Alliance for Internet of Things Innovation (AIOTI) on recent policy documentation and raised these kinds of questions in relation to product safety and liability. In the United States, the Consumer Products Safety Commission (CSPC) had a public hearing on 16 May 2018 to receive information from all interested parties about potential safety issues and hazards with IoT products. It's important to keep an eye on the developing global landscape.

Where do IoT device manufacturers get the information they need to stay compliant?

Kenyon: Our team is constantly working within the realm of the GPSD and product safety laws. There's a range of EU product laws that may apply to your IoT product, depending on its features and characteristics. Typically, it's the responsibility of the manufacturer to ensure their devices are compliant, appropriately marked and labeled, and accompanied by the right documentation. Harmonized standards are very often used as a means of achieving compliance with EU product safety laws. But for emerging technologies, standards often cannot keep pace with the speed of product change and innovation.

Importers and distributors of IoT products have responsibilities, too. And it's important to know and understand your position in the supply chain to know how each relevant product safety law is going to affect you.

Again, for IoT products, this kicks up a number of compliance questions, and they're not necessarily all related to safety. For example, if your connected product doesn't fall squarely within any of the existing harmonized (or nonharmonized) standards, what's the best way to help establish that your product is compliant? To what standard should you test?

Which connected devices may need to comply with additional regulations?

Kenyon: Depending on the device, additional regulations may apply. For example, aviation rules will be relevant in the context of drones, and automotive rules would apply to connected cars. New technology can really show up gaps and challenges in the applicable regulatory regime.

You've said that it's important to think about IoT products and liability, even at this early stage. Why is that?

Kenyon: First, it's really important to reassure people. We want consumers to buy these products, know how brilliant they are, and how they can shape the world. And consumers want to know that it's safe to do so. Unfortunately, there's been some scaremongering in the press about IoT products, which is not especially helpful to this emerging technology.

We're also seeing stories about real-life dangers arising from connected products. Autonomous cars, at the moment, are one example. We need modern and appropriate safety and liability regimes so that consumers and regulators can be more comfortable, and so that businesses have more certainty.

What is the role of the PLD in the EU?

Kenyon: When we talk about liability for IoT products in the EU, we're talking primarily about the PLD plus local laws, such as negligence and contract liability.

The PLD sets out key provisions on liability, burden of proof, and what makes a product "defective." Here are three of the main features of the PLD: the first is that the producer shall be liable for the damage caused by a defect in a product. The second is that the injured person has to prove the damage, the defect, and the causal relationship between defect and damage. The third key point is that a product is defective when it does not provide the safety that a person is entitled to expect, taking all circumstances into account.

Can you provide a high-level overview of the PLD's application to

IoT products?

Kenyon: There's a real question mark about how each of the aspects we just mentioned apply to complex, connected IoT products. For example, does the meaning of a product extend to software and apps and the way that products communicate? Should a defect in an app for a product that causes harm come within the scope of the PLD? And who should be held responsible? For instance, if a network outage causes an accident, should the network provider be held responsible? And if a cyber attack causes an accident, is the manufacturer at fault for failing to make their product sufficiently safe against future cyber attacks? Or did the hacker's acts intervene?

These are interesting questions. What about, in the context of the consumer, if you fail to install an important safety-related software patch? At some point, do we think that the requirement and responsibility for safety should move toward the consumer if they fail to make fundamental software updates?

Where are we heading next? In the context of connected products, is cybersecurity the new product safety, and is data litigation the new product liability?

What is the future of the PLD, in the context of the IoT?

Kenyon: The PLD came into force in 1985 — some 30 years ago. The world was a very different place. Products were very different. You won't be surprised to hear that the European Commission has been evaluating the PLD in light of new technologies. A number of consultations have already happened and there are more of them in the future.

The most recent consultation addressed a number of issues relating to IoT products and technology — for example, whether apps and nonembedded software should be within the scope of the liability regime. Also, whether the unintended, autonomous behavior of an advanced robot could be considered to be a defect. Another example is how strict liability for damage caused by IoT products should be allocated among the different parties involved. This issue is particularly complex in the case of a connected object or sensor that relies on information from another object or sensor, which isn't necessarily in the control of a single producer.

The Commission has recently released an updated report on the application of the PLD as well as a comprehensive evaluation of its implementation in practice. These make clear that, although the Commission still considers that the PLD continues to be an adequate tool, rapidly evolving technologies may mean that well-established principles of the Directive need to be reconsidered.

It was acknowledged that concepts like "product," "producer," "defect," and "damage" might need to be reevaluated to take into account the fact that products can be produced in complex supply chains with numerous contributors and incorporate software and other service components developed by other manufacturers.

The Commission also considered the debate on the allocation of extent of the burden of proof but came to the conclusion that the requirement that an injured person should have to prove the link between the damage and the defect should continue.

Another key area for the Commission was the overlap between product liability and cybersecurity, noting that "consumers and businesses need to be aware of the security levels they can expect, and they need to know who to turn to if a failing in cybersecurity leads to material damage."

So where are we now?

Kenyon: In addition to the consultations on the future of the PLD, the European Commission is also setting up two new expert groups — one on liability, the other in relation to new technology. Both will be considering things like IoT and the product liability regime with the aim of reviewing the applicability of the PLD and developing principles to guide the adaptation of existing EU laws to deal with the potential challenges raised by new technology. At the same time it is considering the wider implications of AI technology, with the creation of an AI technology expert group to an appropriate ethical and legal framework for AI technology and applications. The commission is clearly putting real thought into what revisions are needed.

About Valerie Kenyon

Always focusing on practical and commercial advice, Kenyon and her team help companies manage their risks and meet their business objectives. As a partner and solicitor advocate, she focuses on product litigation; product-related commercial, advisory, and compliance work; and general commercial dispute resolution. She excels in tailor-made solutions for the complex world of products.

Contacts

Valerie
Kenyon
Partner
London

> Read the full article online