The connected home: From smart fish tanks to connected kitchen appliances, product companies must navigate GDPR and Product Liability Directive compliance, cyber risk, and other IoT challenges

23 July 2018

In this interview, Hogan Lovells Partner Valerie Kenyon and Senior Associate Anthea Davies — members of our Global Product Law team — discuss some of the exciting opportunities and challenges presented by the Internet of Things (IoT) and the connected home. Manufacturers of smart thermostats and fish tanks, connected baby products, intelligent kitchen appliances, and speakers that connect to voice-controlled intelligent personal assistant services are grappling with General Data Protection Regulation (GDPR) and EU Product Liability Directive compliance, cyber risk, and a host of other IoT-related issues.

What do we mean by the connected home?

Kenyon: The rise of the IoT shows how quickly technology is changing — products are becoming increasingly data-driven and intelligent, and the IoT is facilitating this. This is great for product manufacturers, which are brilliantly placed to take advantage of the opportunity to connect everyday devices to the internet, and to each other. This opens the door to a world of possibilities.

Davies: In today's home, you can have an array of connected products. We're talking about smart thermostats, connected baby products, intelligent kitchen appliances, and speakers that connect to voice-controlled intelligent personal assistant services — these are fast becoming the norm. Yet there is huge potential for more connectedness in the future. It isn't too far-fetched to picture a future where you no longer need a burglar alarm because a digital security "assistant" is placed by your door, much like the personal assistant currently in your living room. This is a space everyone has their eyes on at the moment, and it's interesting to think about the legal landscape alongside rapid technological advancement.

A connected product for the home could be designed and manufactured by one party, with software designed by another, with yet others in the product life cycle in charge of installation, maintenance, and software updates. What do you see is the potential impact in relation to product safety and product liability?

Davies: Let's think first about the conventional system of product liability under the EU Product Liability Directive (PLD). This has been the key EU legislation in this area since 1985; it "bites" when a product is shown to be defective and has caused harm. Those in the product supply chain are generally familiar with the landscape created by the PLD.

Kenyon: The future of the PLD in relation to technology (including connected devices) is a significant issue currently being considered at an EU level. Recently, for example, there's been a consultation on the PLD and the formation of the European Commission Expert Group on Product Liability and New Technologies. One of the big questions raised by the consultation and to be addressed by the Expert Group is whether the PLD adequately covers new technological products. Do liability considerations need to be revisited in light of IoT and the prevalence of connected devices? Issues include rethinking the definition of a "product" — should this include software and apps? In the context of the PLD, it is not clear that the current definitions will apply effectively to connected home devices. For example, if we take a connected fridge that has an interface with an app, is the PLD's definition of "product" sufficiently broad as to apply to both the fridge and the app?

Davies: Other questions that are being raised include: What is a "safe" IoT product? Where an artificially intelligent home product makes a decision causing harm, who will be held responsible? Should there be provision for when a consumer ignores a push notification, failing to download a safety-related update for their connected home product and is then subject to a cyber attack? The overlap between product liability and cybersecurity in relation to connected home products is significant. Use and abuse of personal data is very much in the news currently. When it comes to looking after their most sensitive personal data, users will rightly demand the highest protection and may well seek compensation if such standards are not met. This is a growing threat for product companies.

Kenyon: The EU legislator is trying to keep up with these questions and develop policy in this area. We have worked with the European Commission and the Alliance for Internet of Things Innovation on their policy documentation and raised these kinds of questions in relation to product safety and liability. In the United States, the Consumer Product Safety Commission held a public hearing on 16 May 2018 to receive information from interested parties about potential safety issues and hazards with IoT products. It's important to keep an eye on the developing global landscape — and we're working closely with clients to do that.

To be safe, is it enough for connect home products to follow existing laws and product standards? What does your team bring to the client's table?

Kenyon: A key challenge for product companies is how to ensure their product is safe when the product is not captured by current legal regimes. Another related challenge is how to be

prepared for new regulation coming later down the line. Innovative products — like connected devices around the home — are often capable beyond what law and regulation had in mind when adopted.

Davies: The application of technical standards (voluntary or otherwise) can be a really tricky issue — the product's abilities can advance beyond the standard. It may well be that a better level of safety can be achieved than is covered by an existing product standard. What then? Is following the standard needed, or conversely — is it not enough?

Kenyon: Our team of products lawyers have a detailed understanding of the relevant laws and regulatory regimes applicable to products and are tech-savvy and commercially focused. We often work alongside technical consultants and test houses; this is especially important when we're thinking about product standards. Our vast global network of product law practitioners are involved with, and monitor, legal developments around the world so we can help companies to stay ahead. Our team combines product regulatory and product litigation know-how: this is crucial, as considering potential risk and liability, as well as product compliance aspects, is vital when developing innovative products.

Davies: Our team frequently works closely with our in-house Science Unit, staffed with post-doctoral scientists, to deal with the complex scientific issues our clients face. Our Science Unit is especially helpful in issue-spotting potential developing areas of product liability. We help clients deal with the uncertainties and ambiguity that cannot be addressed within the borders of traditional areas of law and local regulation.

A clear trend is that technology is becoming increasingly complex and hackers are becoming increasingly sophisticated. A challenge for companies creating connected devices is staying ahead in terms of cybersecurity and product safety whilst also creating excellent products for the consumers, else lose the market. What's new here?

Davies: With the introduction of the GDPR on 25 May 2018, the producer or manufacturer of a connected home product *may* be the "data controller", too.

Kenyon: Imagine a fish tank in your living room with a thermostat that can be controlled via the internet as one of its features. A cyber-attacker raises the temperature of the water in the fish tank by hacking into the thermostat. This ends up killing your prize-winning tropical fish. You did not install the latest software patch and you hadn't spotted that this one related to the security of the system. Once in, the cyber-attacker causes havoc with the rest of the connected products in your home — your fridge, your lights, your sockets, your home security systems, etc. In a connected home, it is not just your data that is being controlled by connected home products and therefore vulnerable to cyber risks, but also the physical and tangible products themselves.

This is the type of factual landscape we're moving towards when it comes to liability issues.

Davies: Product companies have a lot to think about. The right legal and commercial input at an early point can mean a smooth and successful innovative product launch.

Kenyon: These are exciting times! Our team sees a world of opportunity for product manufacturers, especially in relation to the connected home.

Contacts

Valerie Kenyon
Partner
London

Anthea Davies
Senior Associate
London

> Read the full article online