# Following a cyber attack, IoT device manufacturers, data controllers, and sellers could face liability under the EU's Product Liability Directive and the GDPR

**23 May 2018**

Advancements in technology may provide consumers with a continuous stream of upgraded products, but they're also proving that current security and privacy regulations fall short within the Internet of Things (IoT). New devices with unprecedented capabilities are challenging traditional beliefs about liability and consumer protections. In an environment of ever-changing regulations, how do device manufacturers reduce liability risks?

In this hoganlovells.com interview, Christine Gateau, a Hogan Lovells partner based in Paris, introduces the concept of multiple sources of liability within the IoT. She discusses claims that can be brought against producers, data controllers, and traders, and how these claims may test the limits of the EU's Product Liability Directive (PLD) and General Data Protection Regulation (GDPR).

While device manufacturers and producers must secure their products against cyber attacks and breaches, they also need to protect themselves with strategies to anticipate when legal ambiguities may become liabilities.

## How do you define dual liability regarding IoT devices?

**Gateau:** Dual liability for connected objects is a new idea, so I would like to approach this topic from a new angle. If we look at the IoT, it is clearly an area where it's highly likely that the producer or manufacturer of an IoT product — a connected object — will also be the data controller of the data processed by that product.

In the case of cyber attacks, for example, the producer/manufacturer/data controller may face two kinds of liability in this area: rules set forth by the PLD and those from the GDPR. In fact, they may face more than two kinds. But both regulations will apply to products sold in the EU, no matter where the producer is based.

## What specific articles in the GDPR address liability?

**Gateau:** Articles 24 and 79 of the GDPR state that the data controller must "be able to demonstrate that processing [of data] is performed in accordance with this regulation."

With the GDPR, the supervisory authority must consider a wide range of factors when deciding

whether to impose a fine and how much to impose in the event of a data breach. This includes weighing the gravity of the breach, whether it was intentional or negligent, and the degree of cooperation with the supervisory authority.

The GDPR's accountability provisions also require that defendants prove they deployed appropriate technical and organizational measures to prevent the breach.

Articles 24 and 79 of the GDPR also say that the data controller should be able to demonstrate that processing is performed in accordance with this regulation, i.e., that the data should be kept safe.

## Which articles in the PLD are relevant to liability?

**Gateau:** We are talking about Article 1 of the PLD, which says that the producer should be held liable for damages incurred by a defective product. If an IoT device permits — or at least does not prevent — a cyber attack, it could be considered as a defect in the device.

## How does the PLD apply to connected objects in the IoT?

**Gateau:** The PLD addresses the right level of safety that a person can expect, and whether the safety level differs depending on the complexity or purpose of the product. But the PLD does not address questions such as, how is the product defined — is it comprised of the software and apps and the way the product communicates, or is it just the tangible product? Who is responsible for the cyber attack or breach: the manufacturer, system designers, network provider, or cyber attacker? How do you define "producer" — is it the producer of products or of software?

And how can the injured party prove damage, defect, and a causal link, as it will be increasingly difficult in the context of complex technology?

## What claims can parties in Europe bring against the device producer, data controller, or seller?

**Gateau:** The GDPR enables claims to be brought by data subjects or by third parties on behalf of data subjects, and to transform themselves into collective claims with a consolidation mechanism. There are three rights to actions: representative joint action, limited compensatory representative joint action, and limited class action. The GDPR does not create a European class action but opens the door for member states to provide for personal data collective actions.

Finally, there is the trader. A trader is any natural or legal person, either privately or publicly owned, who is acting for purposes relating to their trade, business, or profession. The European Commission's proposal for a directive on representative actions for the protection of the collective interests of consumers would cover all infringements by traders acting in the European Union that harm or may harm the collective interests of consumers.

The proposal would also cover protection of the collective interests of consumers and compensation of damage suffered by individual consumers. But it would not replace existing national collective redress mechanisms.

## Please tell us more about the European Commission's proposal for a directive to protect consumer interests. The New Deal for Consumers.

**Gateau:** If you add those two regulations, the PLD and GDPR, you then have multiple claims available to consumers, and therefore multiple sources of liability as a producer of the IoT device and as a controller of the data used by the device. You can also have multiple sources of liability as a trader and therefore the person putting into the market new products.

And here I'm talking about the proposal for the directive on representative action. It was just released recently and provides for a new way for consumer associations to launch a collective action to protect the collective interests of consumers.

With all those various sources of liability for manufacturers of IoT objects, it is really critical to have a very robust roll out that includes all the necessary steps to put a safe product on the market, and to ensure that if you happen to end up in court, then you will have a very solid defense if need be.

**About Christine Gateau**

"Highly knowledgeable" in IT and in e-commerce disputes (*Who's Who Legal: France*, 2015), litigation partner Christine Gateau is described as "really excellent" (*Chambers Europe 2018: Litigation*). From reviewing general terms and conditions to defending them in court, and from meetings with the French General Directorate of Consumer Affairs to negotiations with consumer associations, Christine Gateau successfully represents tech companies. Her deep knowledge of the industry and connections with the relevant stakeholders allow Christine Gateau to help clients navigate the evolving landscape of legislation governing the Internet and new technologies and build successful strategies for their development.

# Contacts

### Christine

## Gateau

Partner
Paris

> Read the full article online