BULL&CO

ADVOKATFIRMA

White paper

Itechlaw Asia Conference, Bangalore, India, 29 January - 1 February 2019

HOW INSECURE THINGS OF THE INTERNET CAN BREAK YOU

By Kristian Foss, Bull & Co, Norway

As we are well into what Porter and Heppelmann in 2014 described as the third wave of IT, the number of things connected to the internet explodes. [1] Bathroom fans, door locks, barbecue grills, pacemakers, and light bulbs are some of the newcomers. Power grids, factory machinery and cars are becoming old-timers. Prices on equipment, processing power and bandwidth have dropped so low, while capacities has increased so much, that only our imagination limits the application of things connected.

Hardly a day goes by without news of a new data breach or cyber-attack. Increasingly, things connected to the internet play a crucial part. One much used method of attack is the botnet attack, that may employ everything from bread toasters to routers to stage massive distributed denial of service attacks (DDoS) on any target, including newspapers, Netflix and others, bringing down important infrastructure on the way. [2]

1. WHO WILL PAY THE PRICE OF INSECURITY?

A key legal issue of the rise of the Internet of Things (IoT) has therefore become the one of *security*. It is quite apparent that the suppliers of both things and systems have been unable to provide the security needed to mitigate the risk caused by the lethal mix of intense criminal activity, high vulnerability due to the number of devices connected and potentially huge consequences. The grand question is therefore, who will carry the burden of this rapidly growing risk?

To answer that question, we will look at some key legal issues related to defects in security, namely:

a) Insecurity as a defect
b) Data protection
c) Other basis for liability

---

[1] How Smart, Connected Products Are Transforming Competition by Michael E. Porter and James E. Heppelmann http://www.gospi.fr/IMG/pdf/porter-2014-hbr_how-smart-connected-products-are-transforming-competitionhbr-2014.pdf

[2] https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

BULL & CO ADVOKATFIRMA AS
Postadresse:
PO Box 2583 Solli, N-0203 Oslo

Medlem av Den Norske Advokatforening
Besøksadresse:
Observatoriegata 1B, Oslo

T 23 01 01 01
F 23 01 01 11
NO 981 459 326 MVA

E bull@bull.no
W www.bull.no

As these issues now has a direct bearing on most business operations, they should be of interest to anyone dealing with risk, from risk managers to shareholders. CEOs and board members should in particular take care, as they may even become personally liable for ignoring the threat.

2. INSECURITY AS A DEFECT

Any lack of security is relevant for both services and goods, but in different ways. Both insecure services and goods could contractually be defined as defects, and be regulated as any other defect. However, as we are discussing the *things* of the Internet, we will focus on product liability for goods, with controlling software.

In most countries within Europe, goods are subject to product liability regulation. Under the European Union (EU) system, product liability means in short that a producer is strictly liable for so called *safety defects* inflicting damage or death on

a) natural persons, and
b) property meant for private use or consumption.

(art. 1 cf. art. 9 of the Product Liability Directive (PLD) [3]).

From what I understand the closest Indian parallel is the Consumer Protection Act (1986).

A 'product' is any device or 'thing', a physical object, including those incorporated into other things or real estate. Even garbage is included in PLD's definition of 'product', if sold.

2.1 How safe must a car or a toaster be?

A key question is what is regarded a safety defect. The short answer: A product is defect if it "does not provide the safety which a person [and the public at large] is entitled to expect". [4] An objective assessment should likely be used under the directive, as is stated by the Norwegian Supreme Court interpreting Norwegian law implementing the directive. [5] Individual ignorance or misconception will therefore not free a producer of liability in a given case.

For illustration, let's look at connected, more or less self-driving cars with a security defect causing cars to wean off the road, killing or injuring persons and damaging property.

---

[3] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. Covering also the EFTA countries of Iceland, Liechtenstein and Norway, collectively the European Economic Area (EEA).

[4] PLD art. 7 (1) and its preamble

[5] Norwegian Supreme Court case Rt 2004 s 122 para 33

The ability of a car to drive independently may be classified in accordance with several standards. A much used standard is the Society of Automotive Engineers (SAE). [6] At level 0 there is no automation, while at level 5, the highest, the car can self-drive under all conditions.

If the car is at a low level of self-driving, such as SAE level 0-3, and it's true level of capabilities are communicated to the driver, driver expectations should be low.

However, if the producer is telling its customer that its cars can drive independently, or the car is in fact a SAE level 4 or 5 car, expectations will be higher.

With justified high expectations, e.g. of the car not weaning off the road because of the failure of the driver to take the wheel, the producer may become liable if that happens. Much comes therefore down to what the producer says about its products, and how the product itself communicates.

The dashboard of a Tesla will for example clearly tell the driver that it needs to keep its hands on the wheel, and even have the driver turn the wheel slight to prove hands are on.

If the driver then don't grab the wheel, a warning will sound, and the dashboard light up in increasingly strong graphics and sounds. If the driver repeatedly fails to take the wheel, auto pilot will be turned off (after the driver has taken the wheel again).

The type of device may also affect expectation. In the quite recent *Boston Scientific* case The European Court of Justice (ECJ) stated that persons are entitled to expect "particularly high" safety requirements for products, such as pacemakers, because of the "particularly vulnerable situation" of patients implanted with such devices. 7

2.2 What if the safety defect is caused by the software?

A security defect in things of the internet is often related to insufficient security of controlling software and systems to which the things are connected. The things as such, e.g. a door lock, a fire alarm, a car or fridge, may not in itself be insecure. But with the wrong kind of controlling logic, they may become unsafe. A lock may open, a fire alarm may not go off, a car may crash and a fridge can start a fire by being short circuited. This separates internet things from, say, a knife.

If people get hurt or killed because of software failure in an otherwise safe product, will the producer be liable?

Software controlled things were not high on the agenda when the 1985 directive was conceived by the EU in the early 1980s. Software is not mentioned in the directive. A 'product' is defined as "all movables, with the exception of primary agricultural products and game, even though incorporated into another movable or into an immovable" (PDD art. 2).

---

[6] SAE explained: https://www.gigabitmagazine.com/ai/understanding-sae-automated-driving-levels-0-5-explained. The standard: https://www.sae.org/standards/content/j3016_201806/ . Other standards exist too.

[7] *Boston Scientific Medizintechnik GmbH v AOK Sachsen-Anhalt Die Gesundheitskasse* (C-503/13) (premise 39).

In order to clarify whether the PLD applies to software and other new technological developments, the EU Commission conducted a thorough evaluation, issuing a working document in mid 2018. [8] The 108 page strong evaluation offer no clear answer, stating that:

> *"In summary, due to the lack of concrete cases and experience with damages caused by new technological developments, the Directive's effectiveness remains a highly contested subject. " (sec. 5.1.3)*

The evaluation concludes:

> *"Furthermore, the definition of product appears to no longer be as clear-cut as it may have been when the Directive was adopted for example in the light of new technological developments where the distinction between products and services becomes blurred or in the context of software. Given that the Directive applies to products, a clarification of its scope could therefore be envisaged." (sec. 6)*

The ambiguity is criticised by the European Consumer Organisation. [9]

Some authors of the Commission evaluation favours resolving the issue "by means of interpretation of the courts only" (sec. 5.4.1). In want of clair wording, guiding and case law, we will have to lean on other considerations, just as the courts will have to.

The word 'product', is as mentioned to include all "movables, with the exception of primary agricultural products and game, even though incorporated into another movable". This is a wide definition, covering nearly all things made by man, apart from food. Food is regulated in great detail elsewhere. The definition does not *exclude* software, even if 'movables' points in the direction of a physical thing.

For the consumer, and public, however it makes no practical difference if software controls the things we buy. The purpose of the PLD is to protect the users of the things. That need is not reduced by introducing software control. If software induced damages are not covered by the product liability regulation, the regulation would be rendered useless in an increasing number of cases, and also opening a loophole in the regulation.

On the other hand, producers need clear notice of potential liability. Even if the reach of the PLD is not entirely clear, it should come as no surprise to a producer if a court holds the producer liable also for damages caused by the controlling software such producer provides. The message should therefore, even under today's regulation, be clear enough for this argument to carry limited weight.

Excluding software controlled products from liability, would also mean having to draw the line between cases where the physical product itself is dangerous, and cases where the danger is caused by the software. In some cases the cause of the danger may even be

---

[8] Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0157&from=EN

[9] https://www.beuc.eu/publications/beuc-x-2017-039_csc_review_of_product_liability_rules.pdf section 2.2.

mixed. Simpler enforcement will therefore favour including software in the definition of 'product'.

Given the wide definition of 'product', the purpose of the regulation and enforcement considerations, I believe a European court likely will conclude that software is part of the product.

2.3 When must the product be safe?

The product liability directive states that defects should be assessed at the time the products are put into circulation, in practice, the time of sales. [10] How will that work if the software causing the danger is installed *after* the sale has taken place, as may be the case with products that are updated on a continuous basis?

On the face of the wording of the directive, liability may be excluded for subsequent, danger inducing changes and upgrades. It must be clear that later changes done by *others* than the producer, will not cause liability for the producer, unless the ability to make a product insecure, is in itself a safety defect.

But what about later changes done by the producer, after the sale?

This is a new situation, likely not thought of in the early 1980s and identified as a weakness in the directive. [11] However, if the purpose of the directive is to be realised; namely to "protect the physical well-being and property of the consumer", such later updates cannot be exempted from liability. This also plays well with PLD art. 1: "The producer shall be liable for damage caused by a defect in his product." Still, there is no denying the ambiguity, increasing the importance of other legal basis for liability, as discussed below.

2.4 Three caps on liability

In addition to the ambiguities identified above, producers of things of the internet are offered protection by the following:

First, it is the **safety standards** applicable at the time the product was put into circulation that will apply (PLD art. 6 (1) c) and (2)). Higher standards introduced at a later time will not be the yardstick to which an older product is held, even if software updates may take place.

This means that that even if a product could have been made safe under today's standards by a software upgrade and is not, the producer will not be liable. Instead, the person at loss, will have to rely on the tort system: It may be negligent not to mend a security defect, when potential consequences are considered. Or contractually: The agreement may state that the producer shall keep the product safe by use of software updates, if reasonably

---

[10] PLD art. 6 (1) b) and 7 b

[11] Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products concluded: "The Conference on the Evaluation of the Product Liability Directive gave the opportunity to confirm the need to pursue the reflection on the future of the Directive in order to ensure legal certainty, in particular in relation to its application to new technologies, such as Artificial Intelligence systems and advanced robots and internet of Things."

possible. If there is no contractual obligation to maintain security, the tort system will offer the victim less protection than if product liability could have been invoked.

A second element limiting liability is the double **time bar** system of the directive: No claim may be presented later than:

a. three years after the claimant "should reasonably have become aware, of the damage, the defect and the identity of the producer." .
b. 10 years after the product was put into circulation.

(art. 10)

These time bars may have a bearing on storage time for data that may serve as proof for a safe product, also relevant as a legal basis under data protection regulation.

Third, the damage is subject to a **500 Euro threshold** (PLD art. 9). That means that low value, high volume claims may not hit the producer. In the age of class action, this may constitute a significant limitation of liability, which is criticised by consumer advocates.

2.5 Who may become liable?

The *producer* is widely defined in the directive: In short

a) the manufacturer (finished product or part),
b) those offering a product for sale under its own name,
c) reseller, if the manufacturer is hard to identify, and
d) the importer.

(PLD art. 3)

This means that the whole chain of companies making or contributing to its distribution may become liable for unsafe aspects of the product. The idea is to make it simple (or at least possible) for the person damaged by the product to be compensated. This liability may not be limited towards the consumer. However, it may be regulated between the parties in the chain of distribution, which is a point you always need to consider when drafting the contract.

3. DATA PROTECTION AND IOT

If the supplier process personal data or have access to such for maintenance or otherwise, the supplier will be deemed a processor, and the GDPR applies directly.

If the supplier is a developer, not dealing with the personal data, it will not be a processor, and the GDPR does not apply directly. However, its customers, the controllers, will be obliged to ensure that the software complies with the GDPR. This legal requirement will likely translate into a contractual requirement.

This means that any supplier of software to be used by or with things of the internet, or that may be vulnerable to attacks by them, may be exposed to liability. With the exponential growth in risk that the IoT causes, this may become a heavy burden to carry.

The requirement for "information security" in the GDPR (art. 32), is a key requirement, and yet another reason for ensuring connected things are secure. The potential for huge fines, is well known, up to 4% of yearly turnover the entire enterprise (art. 83). Related, and perhaps more practical, is the risk of

- class action claims from data subjects (persons)
- damaged goodwill
- reduced revenues
- claims from customers

The long awaited e-Privacy Regulation, regulating the communication side of data privacy, will increase potential liability further as it contains direct regulation of "terminals" – also things. [12] A key requirement is that communications need to be confidential. The e-Privacy Regulation quite simply refers to its bigger sibling, the GDPR, for sanctions, so be aware.

Class action. Under the GDPR the persons to which the data relates can claim both the data controller and processor for monetary and non-monetary damages (art. 82). As it may be hard to establish a financial loss, non-financial damages are practical. Since numbers of affected persons can be huge, so can the claims, typically presented through class action.

Imagine 200 000 users each being awarded 100 Euro. 20 million Euro. Two million customers, means 200 MEUR, more than enough to bankrupt even mid sized companies. If data subjects can show financial loss, these numbers may increase dramatically.

This strict liability shall be allocated between the controller and processor "corresponding to their part of responsibility for the damage." Only if a party "proves that it is not in any way responsible", will it escape liability.

Damaged goodwill. A more likely consequence of a large and public data breach than class action is damaged goodwill. As many business main currency is trust, lost goodwill can mean **reduced revenues** and with it, lost stock evaluation. Add cost of public relation efforts, other corrective actions, legal assistance and notifications, and cost quickly pile up.

Claims from customers. Business customers of any supplier liable for providing the required security may very well hold such suppliers liable for all of the above. The security norm in the GDPR - adequate security - applies to both data controller (normally the customer) and the processor (normally the supplier). Unless the data breach is caused by a well-resourced and skilled attacker, a data breach with large consequences may be enough to state that security was not adequate.

Provided the security norm is overstepped and cause can be established, liability depends also on the **contract,** in addition to the GDPR. As you may have experienced, many customers are pushing for an increase in liability in the data protection agreements (DPA) required by the GDPR. Some customers even seem to imply that increased liability is a requirement in the GDPR. That is not the case. All the general considerations when allocating risk applies, so dig your supplier heels in when drafting the DPA.

---

12 http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-e-privacy-reform and https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0010:FIN . Now under final negotiations.

4. OTHER BASIS OF LIABILITY

Apart from liability under product liability and data protection regulation, the following basis may cause liability:

- contract
- negligence
- consumer protection regulation
- safety laws

4.1 Contract

The conditions and extent of liability under the above, will be determined by the law in the individual countries. However, both **contractual** liability and non-contractual **negligence** (tort) may form practical basis for liability, not least seen in connection with product safety rules, based on the EU General Product Safety Directive (PSD) and the Directive on security of networks and information systems (NIS). [13]

Often the contract will contain an obligation to comply with public regulation. As the PSD defines products wide; to "any product - including in the context of providing a service - which is intended for consumers [...] or likely, to be used by consumers even if not intended for them", many things of the internet will be covered (PSD art. 2 (a)). The NIS directive applies to providers of services "essential for the maintenance of critical societal and/or economic activities" (art. 5 (2)). In both cases, sufficient security is to be maintained.

4.2 Negligence – it may become personal

Negligence is relevant also towards shareholders of a company. If a company suffers a substantial loss due to insufficient security, the company will suffer a loss it may not be able to transfer to other parties. If such loss could have been avoided by the management, e.g. with better systems and policies, the board and the CEO may become personally liable.

4.3 Consumer protection

In the EU there is substantial consumer protection regulation, including for a number of things that may be connected to the internet. [14] These include toys, lifts and radio equipment, to name a few. Compliant products should be marked with the CE, familiar to many.

---

[13] Directive 2001/95/EC https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001L0095 and Directive (EU) 2016/1148 https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[14] https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en

This regulation is now to be strengthened further, with the various measures as part of the so called 'new deal for consumers' package of measures. [15] Already better enforcement rules are being implemented in the EU and EEA. [16]

Again, safety is an issue. The EU Commission states in its 2018 communication on the internet of things:

> "*(...) the Commission will further explore links between cybersecurity and product safety, identifying tools that can improve product security and safety by design."* [17]

The basis of the protection was laid down in the United Nations Convention on Contracts for the International Sale of Goods in 1980, as later implemented into Sales of goods acts in the various EU/EEA countries . [18] Much to the same effect, the EU implemented the Consumer sales and guarantees directive in 1999. [19] Of particular interest to the things of the internet is section 2, stating the default requirements for the goods; namely to be:

- "fit for any particular purpose for which the consumer requires them and which he made known to the seller at the time of conclusion of the contract and which the seller has accepted"
- "are fit for the purposes for which goods of the same type are normally used"
- "show the quality and performance which are normal in goods of the same type and which the consumer can reasonably expect, given the nature of the goods and taking into account any public statements on the specific characteristics of the goods made about them by the seller, the producer or his representative, particularly in advertising or on labelling"

The wording is quite far reaching, and may include safety aspects of a product. The main remedy is rectification, but damages may also be awarded, depending on the national implementation.

There are, however, some exclusions to liability, in particular if the consumer was or should have been aware of the lack of conformance to the mentioned requirements. Information is therefore key.

---

[15] http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2018)623547

[16] https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=620435

[17] Section 7; section on Internet of things. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1523866913149&uri=COM:2018:183:FIN

[18] https://www.uncitral.org/pdf/english/texts/sales/cisg/V1056997-CISG-e-book.pdf

[19] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31999L0044

Later this has been followed up with the Consumer rights directive of 2011, however mostly focusing on the conditions for contracting of the goods. [20]

4.4 New safety laws

Due to the new situation created by IoT and other technological development, new security legislation is being prepared to protect critical infrastructure of society. The best know may be the Directive on security of network and information systems (NIS Directive), mentioned earlier. [21] The directive is the first in an initiative to bolster cyber security in the EU/EEA. Under the directive, providers of so called "essential services", need to take appropriate security measures and to notify of serious incidents.

In Norway we saw the new National Security Act go into effect 1 January 2019. It applies to public bodies, and suppliers of restricted systems.

5. WHAT TO DO?

So where does all this leave anyone dealing with the things of the internet and internet of things? As is evident from this overview, safety requirements is the great common denominator. Many of the requirements overlap, due to the simple reason that they all share the same purpose - safety for consumer, and safety for society.

This means, the first thing to do is make your offering safe. To do so, establish and document:

- product development processes for built in safety and data protection
- rigorous quality and safety testing and management
- clear placement of responsibilities within our own organisation
- other required policies
- third party audits

The board of directors should instruct the CEO of the above. The CEO must in turn act to operationalise the same in her organisation. Both need to follow up on progress in a regular and structured manner.

However well you execute even the best plan, there will still remain risk. Such risk may now to a large extent be insured. Use a competent insurance broker to put in place at least:

- board and CEO insurance
- product liability insurance
- cyber insurance
- professional liability insurance

Acting on the above should protect both the company, the board and management, and ensure many good nights of sleep.

---

[20] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0083

[21] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

Attorney-at-law Kristian Foss (kf@bull.no) is partner in Bull & Co Law firm, Oslo, Norway, former in-house counsel in leading IT supplier EVRY and member of the Expert Committee for IT law at the Norwegian Centre for Continuing Legal Education. He has more than 20 years of experience with technology and contract law.