Securing the Smart Home

A study on cybersecurity problems in smart home devices: does European product liability law offer meaningful legal solutions for consumers?

Information Law Research Master Thesis

Karlijn van den Heuvel (11112271)

Supervisor: Prof. Dr. Joris van Hoboken

Second reader: Prof. Dr. Chantal Mak

Final version, 17 April 2018. Words (excl. footnotes and references): 38,275

UNIVERSITEIT VAN AMSTERDAM

IViR

Abstract

This thesis examines whether the European product liability regime as established by the Product Liability Directive (Directive), provides meaningful legal solutions in the context of cybersecurity vulnerabilities in smart home devices that cause private harm. Besides providing an extensive factual background to this problem, the main legal inquiries are whether the Directive is applicable in this context and, where it does, whether it provides meaningful remedies from the perspective of the consumer. The overall conclusion is that the Directive is capable of providing some meaningful legal solutions for consumers in the context of cybersecurity vulnerabilities in smart home devices. The applicability of the Directive to this problem is however not self-evident.

First, the requirement that a product must be a tangible good is difficult to overcome for software components of a smart home device, whilst these parts are often the source of cybersecurity vulnerabilities. It is recommended to abandon the physical carrier reasoning in favour of a product definition that defines products independently of their means of transmission. For this, inspiration can be drawn from the proposal for a directive on digital content. Second, in relation to the assessment of defectiveness under the Directive it has been observed that the focus has traditionally been on offline product defects. Considering the growth of software based products, a transformation in thinking about safety to also include (cyber)security would be a desirable development for assessing defectiveness under the Directive. Because the defectiveness assessment is performed on the basis of open norms, i.e. the legitimate expectations of the average consumer, the inclusion of cybersecurity vulnerabilities can be achieved within the current wording of the Directive.

The Directive's system of remedies is limited to compensation of certain types of damages. Damage caused by death or personal injury or private property damage within the meaning of the Directive must be fully compensated. The recovery of non-material damage is however not included, which is a great deficit in the context of finding a remedy for privacy harms. Damage to the defective product itself is also not recoverable. Another limitation is that the availability of injunctions depends fully on the national laws of the Member States. Although some form of preventive action can be created by extending the ECJ's findings in *Boston Scientific*, the significance hereof is likely to be limited to situations where cybersecurity vulnerabilities cause life threatening risks. To overcome the limits of the Directive's system of remedies, it is theoretically possible to appeal to fundamental rights to obtain a procedural advantage before the national courts.

The limitations of the Directive's system of remedies make it a less evident route for preventive measures (e.g. an injunction for the provision of a security update) and the exclusion of non-material damages makes it a less attractive legal route when recovering damages for privacy harms. Without amendment of the Directive, the threat of liability that emanates from the Directive is therefore restricted. Other legal approaches may prove to be more fruitful in this context. However, the fact that the Directive does offer a meaningful solution to consumers in certain circumstances makes it applicability to cybersecurity vulnerabilities in smart home devices worthwhile.

Table of Contents

Cover image: https://www.bcc.nl/specials/smart-home

Chapter 1: Introduction

1.1 The problem

We use more and more objects that are connected to the internet. We are surrounded by computers, smartphones, tablets, game consoles, e-books and interactive TV's. Keeping in mind that most people did not use the internet 20 years ago,[1] these are astonishing developments. The next big promise is the Internet of Things (IoT): connecting everyday objects - 'things' - to the internet. These smart devices sense and gather information about their surroundings, facilitate data analysis, communicate with the user and other smart objects, and are capable of making smart decisions based on the analysed data. Various forecasts predict a huge growth of the IoT.[2] This means that the amount of connected devices will surge, thereby creating ubiquitous connectivity and potentially transforming life as we know it.[3] A quickly growing part of the IoT is the consumer-oriented smart home, which includes smart devices that can be utilized in the home. Examples include smart thermostats, locks and baby monitors.

The promises and excitement about the IoT and smart home devices are accompanied by warnings about privacy and (cyber)security. Recently, we have been confronted with various incidents involving badly secured IoT devices. There has been a lot of attention in the media for Distributed Denial of Service (DDoS) attacks in which smart devices were used to perform the attack. It has been reported that in 2017, DDoS attacks increased 91% because of the IoT.[4] Notably, the Mirai botnet used smart devices to attack DNS-provider Dyn and other websites in October 2016. Use was made of easily hackable IoT devices, including routers, IP cameras and digital video recorders.[5] ENISA, the European Union Agency for Network Information and Security, noted that "[t]hese massive attacks have highlighted the risks resulting from inadequate security mechanisms in Internet of Things (IoT) devices,

[1] International Telecommunication Union, World Telecommunication/ICT Development Report and database, 'Individuals Using the Internet (% of population)' (The World Bank, undated) <https://data.worldbank.org/indicator/IT.NET.USER.ZS> accessed 7 February 2018.

[2] Louis Columbus, '2017 Roundup Of Internet Of Things Forecasts' (*Forbes*, 10 December 2017) <https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#3fb953c1480e> accessed 7 February 2018.

[3] European Commission, 'Advancing the Internet of Things in Europe' SWD(2016) 110 final, 6.

[4] Alison DeNisco Rayome, 'DDoS attacks increased 91% in 2017 thanks to IoT' <*TechRepublic.*, 20 november 2017) <https://www.techrepublic.com/Article/ddos-attacks-increased-91-in-2017-thanks-to-iot/> accessed 6 February 2018.

[5] Sam Thielman and Chris Johnston, 'Major cyber attack disrupts internet service across Europe and US' *The Guardian* (London and New York City, 21 October 2016) <https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service> accessed 6 February 2018.

together with their devastating effects on the Internet itself” and that “[t]hese devices seem to be a low hanging fruit for cyber-attacks”.[6] Therefore, IoT security issues must be addressed.[7]

There has been less attention in the media for incidents with smart devices that cause private harm. However, multiple technical demonstrations by white hat hackers or security companies have shown the lack of cybersecurity in consumer IoT devices. In particular, it has been repeatedly shown how easy it is to hack and gain control of various smart home devices.[8] For example, it has been shown that it is possible to perform a ransomware attack on a smart thermostat.[9] The hackability of various smart baby monitors has been demonstrated, whereby third parties can gain access to the video images, listen in on conversations and use the speaker functionality.[10] Various reports show the lack of cybersecurity in smart locks,[11] including a recent exploit of a software flaw in Amazon’s new delivery service.[12] Another security researcher found that various Blue-tooth enabled smart locks sent passwords in plain-text, allowing easy control of the device.[13] He was also able to lock out the authorised users by changing the admin passwords . This could only be undone by resetting the device, which required a change of battery and that was only possible when the door was open.[14]

Besides these demonstrations and hypothetical musings, a few actual incidents with smart home devices have also been reported. In 2016, a software bug in a series of smart thermostats drained the

[6] ENISA, ‘Major DDoS Attacks Involving IoT Devices’ (ENISA Suggested Reading, 3 November 2016) <https://www.enisa.europa.eu/publications/info-notes/major-ddos-attacks-involving-iot-devices> accessed 6 February 2018.

[7] Ibid.

[8] NB. White hat hackers are ethical hackers or computer security experts that test the security of information systems with the purpose of increasing security rather than for malicious purposes (like black hat hackers).

[9] Matthew Hughes, ‘Thermostats can now get infected with ransomware, because 2016’ (*The Next Web*, 8 August 2016) <https://thenextweb.com/gadgets/2016/08/08/thermostats-can-now-get-infected-with-ransomware-because-2016/#.tnw_MJak6uyF> accessed 6 February 2018.

[10] Mark Stanislav and Tod Beardsley, ‘HACKING IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities’ (*Rapid7*, 29 September 2015) <https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf> accessed 6 February 2018.

[11] Megan Wollerton, ‘Here's what happened when someone hacked the August Smart Lock’ (*CNet*, 25 August 2016) < https://www.cnet.com/news/august-smart-lock-hacked/> accessed 6 February 2018; Iain Thomson, ‘If you use ‘smart’ Bluetooth locks, you're asking to be burgled’ (*The Register*, 8 August 2016) <https://www.theregister.co.uk/2016/08/08/using_a_smart_bluetooth_lock_to_protect_your_valuables_youre_an_idiot/> accessed 6 February 2018; Jennifer Kite-Powell, ‘This Company Staged A Hack With Multiple Devices To Show Your Home's Vulnerability’ (*Forbes*, 19 September 2017) <https://www.forbes.com/sites/jenniferhicks/2017/09/19/this-company-staged-a-hack-with-multiple-devices-to-show-your-homes-vulnerablity/#503922895322> accessed 6 February 2018.

[12] Gerald Lynch, ‘Amazon Key smart lock security integrity called into question by hack’ (*Techradar*, 5 February 2018) <http://www.techradar.com/news/amazon-key-smart-lock-security-integrity-called-into-question-by-hack> accessed 6 February 2018.

[13] Roberto Baldwin, ‘Researcher finds huge security flaws in Bluetooth locks’ (*engadget*, 8 October 2016) < https://www.engadget.com/2016/08/10/researcher-finds-huge-security-flaws-in-bluetooth-locks/> accessed 23 February 2018.

[14] Ibid.

batteries and caused it to turn off, leaving its users literally in the cold.[15] This could result in consumer damage of all sorts, including personal damage, property damage and pure economic damage. More recently, there has been a report of a hacker that remotely raised the temperature in a house with 12 degrees on a smart thermostat.[16] Such an incident could result in the same types of damages as listed above, for example an excessive heating bill. Various incidents involved baby monitors. It has been reported several times that a smart baby monitor was hacked and used to talk to the child in its crib.[17] Also widely reported was a Russian website that live-streamed footage of webcams, including baby monitors.[18] Another recent example includes a smart speaker that listened in on users without being activated and uploading the sound files to the manufacturer's servers.[19] These types of incidents clearly involve privacy harms and can be considered as "creepy".

A question that arises when these types of incidents occur is whether law provides a remedy for the various types of (potential) damage. In other words, who is responsible for cybersecurity in smart home devices? Who is liable when a lack of cybersecurity causes private harm and which remedies are available in law? Despite the fact that there have only been a few reported cases in which smart devices caused private harm, this is clearly a topic that is worthy of further investigation. The various demonstrations by white hat hackers and security companies indicate that smart home devices currently lack basic cybersecurity. The IoT consumer market is expected to surge in the next coming years, so the potential for misuse will grow as well. It is therefore likely that we will be confronted with more incidents involving private harm. This will be the case especially when manufacturers will push their products to the market rather than ensure that their products are safe both in the offline and the online world.

[15] Nick Bilton, 'Nest Thermostat Glitch Leaves Users in the Cold' *The New York Times* (New York City, 13 January 2016) <https://www.nytimes.com/2016/01/14/fashion/nest-thermostat-glitch-battery-dies-software-freeze.html> accessed 6 February 2018.

[16] Matthew Hughes, 'Hacker remotely raises home temperature 12ºC (22ºF) on smart thermostat' (*The Next Web*, 21 July 2017) <https://thenextweb.com/insider/2017/07/21/hacker-remotely-raises-home-temperature-12oc-22of-smart-thermostat/> accessed 6 February 2018.

[17] Eleanor Ross, 'Baby Monitors 'Hacked': Parents Warned to be Vigilant After Voices Heard Coming From Speakers' (*The Independent*, 30 January 2016) <http://www.independent.co.uk/life-style/gadgets-and-tech/news/baby-monitors-hacked-parents-warned-to-be-vigilant-after-voices-heard-coming-from-speakers-a6843346.html> accessed 6 February 2018.

[18] The Huffington Post, 'Parental Warning: Your Baby Monitor Can Be Hacked' (*Huffington Post*, 23 August 2016) <https://www.huffingtonpost.com/healthline-/parental-warning-your-bab_b_11668882.html> accessed 7 February 2018.

[19] Matt Weinberger, 'Google had to disable a feature on its new $50 smart speaker after the gadget listened in on some users' (*Business Insider*, 10 October 2017) <http://www.businessinsider.com/google-home-mini-accidentally-listening-to-users-2017-10?r=UK&IR=T> accessed 22 February 2018.

1.2 Research question

The purpose of this thesis is to find out whether the European product liability regime as established by the Product Liability Directive,[20] provides meaningful solutions for consumers in the context of cybersecurity vulnerabilities in smart home devices that cause private harm. The research question that will be answered is the following:

> **To which extent does the European product liability regime offer meaningful solutions to the problem of attributing responsibility for cybersecurity vulnerabilities in consumer smart home devices?**

The focus of this thesis will thus be limited to cybersecurity in consumer smart home devices as subject matter and European product liability law as legal framework. In the following sections these choices will be explained.

1.2.1 Smart home devices

This thesis focuses on private harm caused by smart home devices due to a lack of cybersecurity. Rather than using the term "IoT devices" or "smart devices" in the research question, the choice was made to focus solely on smart home devices. This was done to limit the research to one particular consumer IoT market rather than taking into account the wide scope of B2B and B2C applications that the term IoT covers. In this way, the subject-matter of this thesis is clear from the outset and manageable.

The smart home was a natural choice of a consumer IoT market. It is a well-recognised part of the IoT that is expected to grow significantly in the next coming years, which means that the issue of liability for a lack of cybersecurity in these devices will become more relevant also. Furthermore, the demonstrations and incidents reported in the previous sections that caused private harm involved smart home devices. As such, it makes sense to limit the scope of this research to smart home devices only and their particular characteristics.

1.2.2 Cybersecurity

Cybersecurity is a complex, broad and ambiguous term. It is often used interchangeably with "computer security", "information security" or "ICT security", though generally considered to be broader than these terms. The exact meaning and scope of the term cybersecurity remain ill-defined.[21] A problematic

[20] 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 [1985] OJ L 210/29 (Product Liability Directive).

[21] Axel Arnbak, 'Securing Private Communications' (PhD dissertation, University of Amsterdam 2015) 160 ("*The fact of the matter and of the computer science literature is that decades of academic debate have not actually led to*

element is the fact that cybersecurity risks are constantly changing and evolving, making it difficult to give a sustainable definition of what cybersecurity aims to protect. To lend words from the Internet Society: "*[a]s a catchword, cybersecurity is frighteningly inexact and can stand for an almost endless list of different security concerns, technical challenges, and "solutions" ranging from the technical to the legislative*."[22] The lack of clear defining characteristics makes it a difficult term to use.

Despite the difficulties in usage of the term cybersecurity, it is chosen as a key concept in this thesis because it refers to a particular set of problems that arises when products become "smart". We are interested in "online" or "virtual" problems with smart home devices; computer security issues. For example, a design flaw in software that causes unavailability of service or allows a malicious third party to gain access to the device. Using "cybersecurity" as main term instead of "security" is intended to call to mind this set of problems relating to smart home devices. Product issues involving cybersecurity are to be distinguished from more traditional or "offline" product issues that may cause harm, e.g. use of wrong material. As a shorthand for 'cybersecurity', the term 'security' will also be used in this thesis.

1.2.3 European product liability law

Allocation of liability in the IoT is a topic that is taken into account in the Digital Single Market (DSM) Strategy for Europe.[23] This policy was adopted in 2015 and consists of various legislative initiatives to create a Digital Single Market in Europe.[24] In the 2017 review report of the DSM, safety and liability in the IoT were explicitly mentioned as a part of developing the European Data Economy.[25] It was stated that the European Commission (EC) will consider whether the current legal framework needs to be adapted in order to remain fit for purpose in light of new developments such as the IoT, especially from the angle of civil law liability.[26] This resonates with a call from the EC in 2016 to conduct a "mapping exercise" to clarify to which extent parts of the IoT are covered by existing (legal) frameworks that regulate liability in order to evaluate the current legal framework against new technological developments.[27]

The various policy documents show an interest in regulating liability in the IoT at the European level. A comprehensive study into all types of liability in the IoT, even when limited to smart home devices, is however too broad a topic for this thesis. One can imagine various forms of liability that may

a refined definition of 'security'."); Rolf Weber and Evelyne Studer, 'Cybersecurity in the internet of things: Legal aspects' *Computer Law and Security Review* 32 (2016) 715, 716.

[22] Internet Society, 'Some Perspectives on Cybersecurity: 2012' (Internet Society 2012) 1.

[23] European Commission, 'Shaping the Digital Single Market' <https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market> accessed 8 February 2018.

[24] Ibid.

[25] European Commission, 'A Connected Digital Single Market for All' COM(2017) 228 final, 12.

[26] Ibid.

[27] European Commission, 'Advancing the Internet of Things in Europe' (n 3) 23.

exist for the variety of legal actors involved in the IoT ecosystem. The focus on one area of law was therefore practically motivated. This approach enables a profound examination of one area of law in context of cybersecurity in smart home devices, rather than a merely explorative study of the various regulatory possibilities. This thesis can be seen as being a part of a bigger project into liability within the IoT, or as part of a comprehensive "mapping exercise" of the current legal framework as indicated by the EC.

One of the existing legal frameworks is product liability. This is an area of law that establishes liability for producers of defective products. The Product Liability Directive (Directive) provides a harmonised regime of strict liability for defective products. This Directive was adopted in 1985 and has not been substantially revised since.[28] For various reasons, it is the area of law that this thesis focuses on. It must however be kept in mind that this is but one possibility in a broader legal framework governing cybersecurity issues in smart home devices. Other relevant areas of law that one might consider in this context include product safety law, data protection law and consumer contract law.

A reason to look to the Directive is that there is an apparent interest in using product liability law to increase cybersecurity in smart devices. Producers of smart devices are in a good position to increase the level of cybersecurity, as they have control over the products that they put on the market. The idea is to incentivise producers to provide an adequate level of cybersecurity in their products by making them liable for a lack of cybersecurity.[29] Various persons have expressed their support for this approach. This includes Digital Commissioner Mariya Gabriel, who expressed her support for applying product liability rules to IT products in a hearing of the European Parliament.[30] The application of product liability to the IoT has also been advocated by ENISA director Udo Helmbrecht and others as a way to incentivise manufacturers and other service providers to increase cybersecurity.[31] All this indicates that there is an interest at the European level to apply the regime of the Directive to IoT products, which includes smart home devices.

Furthermore, the EC started an evaluation of the Directive in 2016 to find out whether it is still fit for purpose in light of new technological developments such as the IoT.[32] The on-going evaluation must be seen in context of the fifth application report of the Directive as required by article 21 of the

[28] NB. Directive 1999/34/EC extended the scope to include agricultural products and game, which was an optional exclusion under art. 2 and art. 15(1) of Directive 85/374/EEC.

[29] For US Law, this topic has recently been explored by: Benjamin C. Dean, 'An Exploration of Strict Products Liability and the Internet of Things' (Center for Democracy & Technology, April 2018).

[30] Jan Philipp Albrecht, 'Hearing, Security in the Internet of Things?' (*Jan Philipp Albrecht*, 21 June 2017) <https://www.janalbrecht.eu/2017/06/2017-06-21-security-in-the-internet-of-things/> accessed 13 February 2018.

[31] Ibid.

[32] European Commission, 'Evaluation of the Directive 85/374/EEC concerning liability for defective products - Roadmap' (2016), 1 <http://ec.europa.eu/DocsRoom/documents/18842/> accessed 2 January 2018.

Directive.[33] One of the reasons for taking the reporting obligation as an opportunity to conduct this evaluation was that various academic legal experts have suggested that the Directive may no longer be fit for purpose and needs revision in light of digital developments.[34] Key questions in the evaluation are whether IoT products are "products" within the meaning of the Directive, and how to allocate strict liability for damages between the different participants in the IoT.[35] The EC also asks more generally whether the definitions of product, producer, defect, damage or the category of exemptions should be clarified or adapted in light of new technological advances.[36] From the public consultation held in 2017, it follows that almost half of the respondents are in favour of a revision of the Directive.[37] To the knowledge of the author, the fifth application report has not yet been published and the evaluation remains listed on the EC's planning of evaluations and studies.[38] With a profound examination the topic, this thesis can therefore contribute to the evaluation of the Directive.

It must be noted that the attention for cybersecurity in the IoT is not restricted to the European level. There is also attention for this topic at the national level in Europe and beyond. In a testimony before the U.S. House of Representatives, cybersecurity expert Bruce Schneier urged the U.S. government to impose minimum security standards and liability on IoT manufacturers.[39] In France, a desire to place liability for cybersecurity in the hands of companies that put products on the market was expressed in the recent Strategic Review of Cyberdefense (*Revue Stratégique Cyberdéfense*).[40] In the Netherlands, a member of Parliament asked the government to look into possibilities for liability in IoT devices that lack cybersecurity, in particular software liability.[41] This initiative was taken up in the latest coalition agreement that sets out the cabinet's plans up to 2021, stating companies will be incentivised to

[33] Ibid.

[34] European Commission, 'Evaluation of the Directive 85/374/EEC concerning liability for defective products - Roadmap' (n 32) 7.

[35] Ibid.

[36] Ibid, 5.

[37] European Commission, 'Brief factual summary on the results of the public consultation on the rules on producer liability for damage caused by a defective product' (2017) GROW/B1/H1/sc(2017) 3054035, 3.

[38] European Commission, 'Commission's Forward Planning of Evaluation and Studies – 2017 and beyond' (2017) <https://ec.europa.eu/info/sites/info/files/20170504-studies-and-evaluations-2017-planning_en.pdf> accessed 27 March 2018, 53 (no. 226).

[39] Bruce Schneier, 'Testimony before the U.S. House of Representative in the Joint Hearing entitled Understanding the Role of Connected Devices in Recent Cyber Attacks' (16 November 2016) <https://www.schneier.com/essays/archives/2016/11/testimony_at_the_us_.html> accessed 5 December 2017.

[40] Lukasz Olejnik, 'Highlights of the French cybersecurity strategy' (*Security, Privacy & Tech Inquiries*, 13 February 2018) <https://blog.lukaszolejnik.com/highlights-of-french-cybersecurity-strategy/> accessed 14 February 2018.

[41] Initiatiefnota van het lid Verhoeven: Het Internet der Dingen: maak apparaten veilig!, *Kamerstukken II* 2016/17, 34613, 2, 7.

create safer software via software liability.[42] The European efforts must therefore be seen against the background of national initiatives to increase cybersecurity in the IoT.

1.3 Research design

1.3.1 Legal framework

The primary legal framework of this thesis is the Product Liability Directive (Directive).[43] As indicated above, the solutions that the Directive offers must be seen against the backdrop of a broader legal framework in which consumers can find remedies for private harm caused by cybersecurity issues in smart home devices. As such, it must be seen as a legal instrument that may prove useful in solving some issues in this area rather than being a panacea across the board. Other areas of law that one might consider in this context include consumer contract law (notably the proposal a directive on digital content[44]), data protection law and product safety law. Whilst the research focus is on the Directive, references will be made to these areas of law where appropriate. In particular, after discussing the various possibilities and shortcomings of the remedies offered by the Directive, we will briefly turn our attention to remedies available in these legal fields.[45] The attention for other areas of law is motivated by the desire to provide a refined overall conclusion that places the Directive in context with some other regulatory options.

This thesis takes a European perspective of product liability law. Overall, the text of the Directive is leading in the legal analysis. Because of this, there will only be limited attention for the Member States' implementations of the Directive; mostly where the Directive leaves room for divergence at the national law level. It is important to realise that, from a technical legal viewpoint, directives do not have so-called horizontal direct effect.[46] The Court of Justice of the European Union has repeatedly held that directives cannot create obligations for individuals, meaning that their breach cannot give rise to private law liability.[47] This means that parties in a private dispute cannot directly invoke directives, except where certain requirements are met. Therefore, judgment will be made on the basis of the national implementation of the Directive that is applicable to the case. The text of the Directive does however have

[42] VVD, CDA, D66 & ChristenUnie, 'Regeerakkoord 2017-2021: Vertrouwen in de Toekomst' (10 October 2017) 3.
[43] Directive 85/374/EEC (n 23).
[44] European Commission, 'Proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content' COM (2015) 634 final (proposal for a directive on digital content).
[45] See: Chapter 7.3.
[46] Dorota Leczykiewics, 'The Constitutional Dimension of Private Law Liability Rules in the EU' in D. Leczykiewics and S. Weatherill (eds) *The Involvement of EU Law in Private Law Relationships* (Hart Publishing, 2013) 199, 209.
[47] E.g. Case 152/84 *M. H. Marshall v Southampton and South-West Hampshire Area Health Authority (Teaching)* [1986] ECR 723, para 48.

an indirect effect by influencing the interpretation of the national law in accordance with the principle of conform interpretation.[48]

Whilst acknowledging that, from a technical perspective, it is not the Directive that is invoked in a claim involving the European product liability regime (but the national implementation thereof) there is sufficient ground to rely primarily on the text of the Directive for the purposes of this thesis. An important reason for adopting a Europeanist perspective is the ongoing evaluation of the Directive. As such, the aim of this thesis is not to consider and compare national implementations of the Directive, but to consider whether the Directive applies to smart home devices and whether it offers meaningful solutions to the problem of cybersecurity vulnerabilities in these devices.

Besides, the Directive aims for full harmonisation.[49] This means that Member States are not at liberty to derogate from the rules provided by the Directive. They are not allowed to create more lenient nor more stringent rules at the national level whilst implementing the Directive, except where this is expressly provided. The Directive only provides two possibilities for derogation.[50] For this reason, the rules at the national level should substantively be the same as the rules in the Directive. Many countries have almost literally copied the text of the Directive into national law, so that the national rules are practically a mirror image of the provisions in the Directive.[51] For this reason also, a consideration of the European product liability regime at the national level is of less interest for the purposes of this thesis.

Having said this, it is important to also recognise the limits of the harmonising power of the Directive. As mentioned, Member State cannot derogate from the rules provided by the Directive because it aims for full harmonisation, which means that they lose legislative competence in the field covered by the Directive.[52] The extent to which this is the case is to be determined by the contents of the Directive. There are two elements to this.

First, the Directive does not fully harmonise the national laws because it complements rather than substitutes national product liability law.[53] Article 13 of the Directive provides that it does not prejudice systems of contractual or non-contractual liability in the Member States nor special liability regimes existing at the moment of implementation. This means that Member States are at liberty to maintain a

[48] Louise Dommering-van Rongen, ‘Produktenaansprakelijkheid: Een nieuwe Europese privaatrechtelijke regeling vergeleken met de produktenaansprakelijkheid in de Verenigde Staten’ (PhD thesis, University of Utrecht 1991) 38.

[49] Article 13 Product Liability Directive. See e.g.: Duncan Fairgrieve et al. ‘Product Liability Directive’ in Piotr Machnikowski (ed), *European Product Liability, an Analysis in the State of the Art in the Era of New Technologies* (Cambridge, Intersentia 2016) 27-31.

[50] Article 15(1)(b) Product Liability Directive (option to implement the risk development defense into national law); Article 16(1) Product Liability Directive (option to implement a financial cap into national law).

[51] Piotr Machnikowski, ‘Conclusions’ in Piotr Machnikowski (ed), *European Product Liability, an Analysis in the State of the Art in the Era of New Technologies* (Cambridge, Intersentia 2016) 672; Louise Dommering-van Rongen (n 47) 45.

[52] This is called “Sperrwirkung”. See more elaborately: Louise Dommering-van Rongen (no 47) 47.

[53] Arthur S. Hartkamp, *Asser 3-I Europees recht en Nederlands vermogensrecht* (Wolters Kluwer 2015) 272.

system of liability based on tort or contract law for defective products.[54] In case a claim under the European regime of product liability is not successful, other litigation opportunities may exist at the national level. For example, in the Netherlands it is also possible to start proceedings against a producer for a defective product on basis of fault-based tort law.[55] These types of national product liability claims will not be covered in this thesis.

Second, the Directive does not fully harmonise all topics in the Directive. Certain elements of a product liability claim under the Directive are left to be decided according to national laws. Most notably, the Directive only gives limited guidance on the meaning of key concepts like causality and damages. One must look to applicable national law to figure out the exact workings of these elements for a product liability claim under the European regime. This leads to divergences at the national level and significantly limits the harmonisation that the Directive achieves. For these parts of the claim, this thesis will look into Member State law for illustrative purposes. A full review of these matters before national law is however not intended nor aspired.

1.3.2 Methods

When studying the impact of novel technological developments on law, such as questions of how to deal with cybersecurity problems in smart home devices, one must find a way to deal with a bourgeoning field of law. One particular problem that must be dealt with is the lack of existing case law. Legal researchers often rely on case law to trace and analyse legal responses to societal (including technological) developments. Most interesting are ground breaking cases that push the boundaries of legal interpretation; cases that have been theorised as relating to the penumbra of uncertainty surrounding a rule rather than its core meaning.[56] The type of legal research in this thesis is more future-oriented; whilst anticipating case law and other legal developments in the field of cybersecurity in smart home devices in the upcoming years, including in relation to product liability law, there is little to no case law as of yet.[57]

Because of the importance of facts and circumstances in any legal analysis, especially when analysing a tort law regime such as product liability law which contains many open norms, the first part of this thesis provides an extensive factual background of cybersecurity problems in smart home devices.

[54] Article 13 Product Liability Directive ("*This Directive shall not affect any rights which an injured person may have according to the rules of the law of contractual or non-contractual liability or a special liability system existing at the moment when this Directive is notified*").

[55] Article 6:162 Dutch Civil Law.

[56] Herbert L A Hart, 'Positivism and the Separation of Law and Morals' (1958) 71 Harvard Law Review 593, 607.

[57] A relevant case in this context is the Dutch case Consumentenbond v. Samsung about the provision of updates in Samsung smart phones based on *inter alia* consumer contract law and general tort law. For the writ of summons (in Dutch) see: https://www.consumentenbond.nl/binaries/content/assets/cbhippowebsite/actie-voeren/updaten/dagvaarding-consumentenbond---samsung-11-nov-2016.pdf. For an English summary of the case so far, see: Paul Verbruggen et al., *Towards Harmonised Duties of Care and Diligence in Cybersecurity* (European Foresight Cyber Security Meeting 2016) 83-84 <https://ssrn.com/abstract=2814101> accessed 23 August 2017.

This approach aims to compensate for the lack of case law and other relevant legal materials. As such, Part I elaborately explains cybersecurity problems in smart home devices. This is done in a deductive fashion, meaning that we will move to three particular incident scenarios and corresponding meaningful technical and legal solutions via an explanation and discussion of more general phenomena and concepts. The factual background will be used as a foundation for the legal analysis in Part II. It can be seen as a contextual framework against which the value of the Directive can be tested.[58] The results hereof are summarized in a table that outlines legal solutions that are meaningful from the perspective of the consumers and which forms the connecting link between Part I and Part II.

The research conducted for Part I of this thesis consisted of desk research. Various sources outside of law were studied, including texts from computer science and sociology. It would be wrong however to say that an external legal perspective is adopted, because these sources are not used to study law but to study a technological phenomenon. Conceptual analysis has been used to come to an understanding of the key terms in this thesis. One reason for using this method is to maintain a structure within meaningful discussion can occur.[59] A common understanding of key terms is established so that common ground is created for further discussion and investigation. This takes the form of defining the following terms for the purpose of this thesis: the smart home, the Internet of Things and cybersecurity.

In the legal analysis of Part II, the primary method of legal research is doctrinal research. This is research into the law and legal concepts.[60] It has been described as the research process which is used to "identify, analyse and synthesise the content of the law."[61] Some defining characteristics of this legal research method are the following.[62] First, doctrinal work only uses authoritative legal sources such as legislative texts, case law and scholarly legal writing. It is often said that a doctrinal legal scholar adopts an internal legal perspective; remaining within the legal universe. Second, the law is presented as a coherent system in which decisions in individual cases must find their place. Third, deciding cases that relate to the penumbra of uncertainty surrounding a rule rather than its core meaning (also called "hard cases") requires stretching or even replacing (parts of) but always in such a way that the system of law is

[58] NB. "Value" is used here to indicate the worth or meaningfulness of the Directive in the context of cybersecurity vulnerabilities in smart home devices.

[59] Brian Bix, 'Conceptual Questions and Jurisprudence' (1995) 1 Legal Theory 465, 469.

[60] Terry Hutchinson and Nigel Duncan, 'Defining and Describing What We Do: Doctrinal Legal Research' (2012) 17 Deakin Law Review 83, 85.

[61] Terry Hutchinson, 'Doctrinal research: researching the jury' in Dawn Watkins and Mandy Burton (eds) *Research Methods in Law* (Taylor & Francis Group 2013) 9-10 ("*In this method, the essential features of the legislation and case law are examined critically and then all the relevant items are combined or synthesised to establish an arguably correct and complete statement of the law on the matter at hand*").

[62] Rob van Gestel and Hans W Micklitz, 'Revitalizing Doctrinal Legal Research in Europe: What About Methodology?' (2011) EUI Working Paper LAW 2011/05, 26 <https://ssrn.com/abstract=1824237> accessed 3 April 2018.

coherent again. This thesis involves a critical examination of whether we can interpret (or stretch) the Directive so that its application to cybersecurity problems in smart home devices has merit.

For the research conducted in part II, the main legislative texts that is analysed is the Directive. Some other legal instruments at both the European and national level are also mentioned, e.g. the proposal for a directive on digital content and the national implementations of the Directive. Case law is mostly limited to cases before the Court of Justice of the European Union (CJEU) in which it interpreted various provisions of the Directive. As mentioned, case law on the subject matter of this thesis is scarce to non-existent. Work from various legal scholars has been studied in the course of writing this thesis, limited to writings in English and Dutch.

1.4 Structure of thesis

This thesis is divided in two parts, starting with a factual background to the problem of cybersecurity problems in smart home devices. Part I consists of two chapters. Chapter 2 focuses on smart home devices and the broader technological development that they form a part of; the Internet of Things. Chapter 3 covers cybersecurity problems in smart home devices and introduces the three security incident scenarios. These chapters are necessary building blocks to gain a profound understanding of the issues at stake and function as a foundation for the rest of the thesis.

The legal analysis in the second part of this thesis aims to find out whether the Product Liability Directive provides meaningful solution in the context of cybersecurity vulnerabilities in smart home devices. The focus is on private harm and private law remedies. Part II consists of four chapters. Chapter 4 gives an introduction into European product liability law. Chapter 5 focuses on the question of whether smart home devices are products within the meaning of the Directive. Chapter 6 analyses whether cybersecurity vulnerabilities constitute defects within the meaning of the Directive. Chapter 7 concludes the legal analysis with a discussion of the remedies that are available under the Directive and whether they are meaningful. All this is followed by the conclusion of the complete thesis in Chapter 8.

PART I: FACTUAL BACKGROUND

Chapter 2: Smart home devices

The smart home is part of a bigger development called the Internet of Things (IoT). In this chapter, we will explore the smart home and how smart home devices function. The information in this chapter aims to deepen our understanding of the subject matter of this thesis, so that we are able to comprehend cybersecurity problems in smart home devices. As such, it serves as the foundation of the legal analysis in part II, together with chapter 3 on cybersecurity.

In section 2.1, the smart home will be introduced and defined for the purposes of this thesis. Attention will be given to the potential and the risks related to smart home devices. In section 2.2, we consider how smart home devices function by examining the broader development that they form part of: the Internet of Things. Section 2.3 presents three smart home devices that will be used as case studies throughout this thesis: smart thermostats, smart locks and smart baby monitors.

2.1 The Smart Home

The smart home is a part of the Internet of Things (IoT). All smart home devices are therefore IoT devices; they are a subspecies. The smart home can be defined as "a residence incorporating a range of sensors systems and devices that can be remotely accessed, controlled, and monitored via a communication network".[63] Or, put more simply, a home becomes "smart" when its owner or inhabitant uses IoT devices in it. The application areas of the smart home are commonly categorized as belonging to the area of energy, security, entertainment and healthcare.[64] It includes internet-connected appliances, lighting, switches, door locks, thermostats and other objects designed for the home environment.[65] All smart home technology aims at making your home more comfortable, controllable, secure and sustainable. Or, in the words of a smart home manufacturer, it is about creating "a thoughtful home [...] that takes care of the people inside it and the world around it."[66]

The potential for the smart home market is big. In 2016, the European Commission has identified the Smart Home as one of the IoT market sectors with the most realistic business opportunities now and within five years, alongside Smart Manufacturing, Smart Personal Health and Wellness, Smart Cities, and more.[67] A recent study values the worldwide Smart Home market at USD 33,5 billion in 2017, expecting

[63] Joseph Bugeja et al., 'On Privacy and Security in Smart Connected Homes' (2016 European Intelligence and Security Informatics Conference, Uppsala, August 2016) 1.
[64] Ibid.
[65] Eric Zeng et al., 'End User Security & Privacy Concerns with Smart Homes' (Symposium on Usable Privacy and Security, Santa Clara, California, July 12-14 2017) 2.
[66] Nest, 'About Us' (2017) <https://nest.com/about/> accessed 29 November 2017.
[67] European Commission, 'Advancing the Internet of Things in Europe' SWD(2016) 110 final, 26.

it to grow at a rate of 27,5% per year to USD 113 billion in 2022.[68] In 2015, this was USD 9.8 billion and expected to rise to only USD 43 billion in 2020.[69] With a market value of 15.4 billion, in 2017 the most revenue was generated in the US.[70] In Europe, the revenue was almost USD 8 billion.[71] There has also been a rapid increase in the offer of smart home devices over the past few years.[72] A quick search into the current online offer of smart home devices returns smart thermostats, locks, smoke detectors, surveillance cameras, lights, switches, alarm clocks, TV's, toys, baby monitors, and more. Several providers are offering full smart home platforms, for example Samsung (SmartThings), Apple (HomeKit) and Amazon (Echo). These tech giants are all hoping to obtain a smart home monopoly and tend to create lock-in effects via direct and indirect network effects, which is disadvantageous for new competitors.[73]

The promises and potential surrounding the smart home can be offset by concerns about cybersecurity and privacy. In the next chapter, we will delve into the issue of cybersecurity. Cybersecurity problems also relate to privacy, as a lack of security can lead to various privacy harms. In general, (personal) data is the backbone of any smart device. This raises privacy concerns, in particular with regard to the protection of personal data. The smart home raises additional privacy concerns. Besides one's body, the home is considered to be one of the most private parts of life. This is reflected in law also. In Europe, the fundamental right to privacy protects private and family life, which includes one's home and correspondence.[74] Also the U.S. constitution, which does not constitutionally recognise a general right to privacy, protects "the sanctities of a man's home and the privacies of life".[75] The fact that smart home devices are located in a constitutionally protected place as well as protected by human rights distinguishes them from other smart devices.[76]

When someone uses smart home technology in their house, they will be sharing personal and sensitive information with private companies. This may be problematic in itself from a privacy perspective. In a recent consumer survey on mobile technology, more than 40% of respondents found that

[68] Statista, 'Smart Home Worldwide' <https://www.statista.com/outlook/279/100/smart-home/worldwide#> accessed 29 November 2017.

[69] Ibid.

[70] 'Ibid.

[71] Ibid.

[72] Zeng et al. (no 65) 2.

[73] Hadi Asghari, 'Cybersecurity via Intermediaries' (PhD dissertation, University of Delft 2016) 19. See also: Musa G. Samaila et al., 'Security Challenges of the Internet of Things' in Batalla et al. (eds) *Beyond the Internet of Things: Everything Interconnected* (Springer International Publishing AG 2017) 64.

[74] Article 8 European Convention of Human Rights; Article 7 Charter of Fundamental Rights of the European Union.

[75] Olmstead v. United States, 277 U.S. 438 (1992), 473 ("*Protection against such invasion of "the sanctities of a man's home and the privacies of life" was provided in the Fourth and Fifth Amendments by specific language.*")

[76] NB. Another type of smart device that raises particular privacy concerns are health wearables, as they collect information about someone's health and fitness.

smart home technology reveals too much about their personal lives.[77] Also, nearly 40% of respondents worried about their use of smart home devices being tracked.[78] This shows that consumers feel uneasy about welcoming smart technology into their homes where they fear they are being watched, listened to or tracked.[79] These consumer concerns might harm the further growth of the smart home technology market.

2.2 The Internet of Things

To examine the way smart home devices function, this section examines the broader development that they form a part of: the Internet of Things ("IoT"). First, we further define the IoT for the purpose of this thesis. Second, we look into the basic technological functioning of the IoT and the way that (personal) data travels through various layers of communication.

2.2.1 Defining the Internet of Things

Broadly speaking, the term IoT refers to "the growing number of everyday physical objects or "things" that have been embedded with technology to enable them to interact with their physical environment, people and other devices in real-time."[80] In other words, the IoT is about connecting previously unconnected (offline) physical objects to the internet. This development covers a wide variety of sectors, including transport, energy, security, health and entertainment. It covers connected cars, smart thermostats and smart locks, pacemakers, insulin pumps and health wearables like Fitbit, smart toys and smart TV's. Besides the consumer market, the IoT also brings many business and industrial opportunities like smart manufacturing and smart cities.

Because of the fact that the IoT is such a widespread phenomenon, it is hard to give one clear definition that covers all without being too generalized. Contributing to this difficulty is that the IoT is a young industry whose technology and participants are in a state of great flux.[81] In all this commotion there is a plethora of definitions offered in official or expert reports and academic writings.[82] For example, the US Federal Trade Commission (FTC) simply admits that there is no widely accepted

[77] Deloitte, '2017 Global Mobile Consumer Survey: US edition' (Deloitte, 2017) 12. <www.deloitte.com/us/mobileconsumer> accessed 22 February 2018.
[78] Ibid.
[79] Caroline Cakebread, 'Consumers are holding off on buying smart-home gadgets thanks to security and privacy fears' (*Business Insider*, 15 November 2017) <http://www.businessinsider.com/consumers-holding-off-on-smart-home-gadgets-thanks-to-privacy-fears-2017-11?international=true&r=US&IR=T> accessed 22 February 2018.
[80] Mauricio Paez and Mike La Marca, 'The Internet of Things: Emerging Legal Issues for Businesses' (2016) 43 North Kentucky Law Review 29, 31.
[81] Swaroop Poudel, 'Internet of Things: Underlying Technologies, Interoperability and Threats to Privacy and Security" (2016) 31 Berkeley Technology Law Journal 997, 1000.
[82] For an overview of various definitions, see: Roberto Minerva et al., 'Towards a Definitions of the Internet of Things (IoT)' (IEEE Internet Initiative 2015).

definition of the IoT.[83] They have used an accessible definition of the IoT, namely "devices or sensors - other than computers, smartphones or tablets - that connect, communicate or transmit information with or between each other through the Internet."[84] Or, even more simplified: "the ability of everyday objects to connect to the Internet to send and receive data."[85] This is however a rather narrow and object focused definition of the IoT. Similarly common sense and accessible definitions are used in various academic writings as a starting point.[86]

A more technical definition is offered by the International Telecommunication Union (ITU), a UN agency for ICT, defining the IoT as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies."[87] They provide additional definitions of what constitutes a "thing" and a "device" also.[88] The Article 29 Working Party[89] focuses on the role that data plays in the IoT, defining it as: "an infrastructure in which billions of sensors embedded in common, everyday devices - 'things' as such, or things linked to other objects or individuals - are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities."[90] Yet another approach is taken by ENISA, that focuses on the IoT as an ecosystem rather than an infrastructure and places emphasis on intelligent decision making by devices: "[the IoT is] a cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision making."[91]

[83] FTC Staff Report, 'Internet of Things: Privacy and Security in a Connected World' (FTC 2015) 5 <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf> accessed 22 November 2017.

[84] Ibid, 6.

[85] FTC Staff Comment, 'Comments on the Benefits, Challenges and potential Roles for the Government in Fostering the Advancement of the Internet of Things' (FTC 2016) 3.

[86] E.g. Teodor Mitew, 'Do objects dream of an internet of things' (2014) 23(168) The Fibreculture Journal 3, 5 <http://twentythree.fibreculturejournal.org/fcj-168-do-objects-dream-of-an-internet-of-things/> accessed 13 November 2017 ("*In simple terms, the IoT stands for the connection of usually trivial material objects to the internet - ranging from tooth brushes, to shoes or umbrellas*."); Zeng et al. (68) 2 ("*The Internet of Things (IoT) is a broad term for internet connected devices, which has come to encompass everything from connected cars, wearables and connected industrial/manufacturing equipment*.").

[87] International Telecommunication Union Recommendation Y.2060, 'Overview of the Internet of Things' (ITU, 2012) 1 <https://www.itu.int/rec/T-REC-Y.2060-201206-I> accessed 17 October 2017. Definition adopted by the Cloud Service Alliance, 'Security Guidance for Early Adopters of the Internet of Things (IoT)' (CSA 2015) <https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf> accessed 17 October 2017. See also: Samaila et al. (n 75) 54.

[88] International Telecommunication Union Recommendation (n 87) 1.

[89] NB. From 25 May 2018 onwards: European Data Protection Board.

[90] Article 29 Data Protection Working Party, 'Opinion 8/2014 on the Recent Developments of the Internet of Things' 14/EN WP223, 4.

[91] ENISA, 'Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures' (ENISA, November 2017) 18.

In this thesis the definition of the Organisation for Economic Co-operation and Development (OECD) will be adopted:

> *[the IoT is] an ecosystem in which applications and services are driven by data collected from devices that sense and interface with the physical world.*[92]

The OECD's definition is workable because, unlike the ITU's definition, it is not too technical whilst having all the key elements. It is similar to the definition offered by ENISA in its approach of the the IoT as an ecosystem, though with less of a focus on intelligent decision making. It is furthermore not overly simplified like the FTC's definition and does not single out the role of (personal) data like WP29's definition.

2.2.2 Basic technological underpinning of the Internet of Things

To better understand the OECD definition provided in the previous subsection, and also the complexity of the IoT ecosystem, it is helpful to explain the following basic steps that underpin the IoT:[93]

1. embedded **sensors** in IoT devices detect and capture data from the surrounding environment;
2. the collected data is transmitted to **the internet** and often stored in the cloud (a server);
3. the data is analysed for insights and intelligence that will guide **decision making**, either by humans via mobile applications or by machines themselves (M2M communication);
4. **actuators** (switches that can move or control a system or device) in the ecosystem are used remotely to execute the decisions.

Something to take note of is the role of the smartphone (or tablet) in the IoT. Smartphones are often not seen as being part of the IoT nor as IoT devices.[94] However, smartphones also contain sensors that capture data from the surrounding environment, e.g. location data, which may be part of an intelligent decision of a smart device. In this sense, the smartphone can serve as an extension of the IoT device with its own sensors. Furthermore, smartphones often serve as wireless hub or remote control for IoT devices through mobile apps.[95] A user can get access to the data send commands via the smartphone application. Therefore, whilst not exactly a smart object in themselves, smartphones do play important roles in the IoT ecosystem.

Let's illustrate the four steps by the example of a smart thermostat. A smart thermostat has sensors that measure temperature and motion in a house (step 1). The device is connected to the Wifi which enables the data to be transmitted to the internet via the local network. The data is stored on a

[92] OECD Working Party on Communication Infrastructures and Services Policy, 'The Internet of Things: Seizing the Benefits and Addressing the Challenges' (OECD 2015) 9.

[93] Partially taken from: Paez and La Marca (n 80) 31.

[94] Paez and La Marca (n 80) 31. See also definition in: FTC Staff Report (n 83) 6.

[95] Paez and La Marca (n 80) 31.

server hosted by the device manufacturer that also provides the user's application (step 2). The data is analysed and visualised in the user application (on a smartphone or tablet), through which the user can check the temperature in the house from another location and remotely change this. On the basis of the collected data, e.g. the current temperature and whether someone is home or not, combined with user preferences and data from the smartphone (e.g. is someone about to come home?), the thermostat is capable of making intelligent decisions about heating (step 3). The decision is then communicated back to the device which controls actuators in the home that execute the command; switching the boiler on or off (step 4).

Even this relatively easy example is complicated (and all that merely to turn the heating on or off!). For the purposes of this thesis, an important takeaway is the wide variety of actors that are involved in the execution of these four steps. This can be clarified further by looking at a schematic representation of the various layers through which data travels in an IoT ecosystem. See figure 1 for the layered IoT model that we will examine here. This model is a combination of two models found in the literature.[96] It bears resemblance to other layer models provided in telecommunications generally.[97]

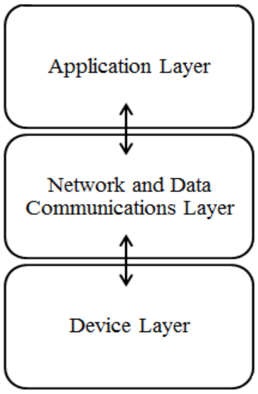

Figure 1: Layered model of the IoT

The three layers of figure 1 can be described as follows. The device layer comprises the IoT device that collects and uploads data, and that receives commands back from the layers above.[98] The data collected at the device level is transmitted to the network and data communications layer, which provides network services like transport and connectivity.[99] In this layer, other data communication services like data storage (in the cloud) are performed.[100] Lastly, the data is visualised and analysed in the application

[96] Poudel (n 81) 1001; Minerva et al (n 82) 11.
[97] E.g. Egbert Dommering and Nico van Eijk, 'Convergenties in regulering: reflecties op elektronische communicatie' (Dutch Ministry of Economic Development, 2010) 12.
[98] Poudel (n 81) 1001.
[99] Ibid.
[100] Ibid.

layer that contains high-level programs and applications.[101] In the IoT environment, the data travels up from the device through the layers to enable decision making at the top and commands travel back to the device to be performed by actuators that convert the electrical signal into motion.

As mentioned already, an important thing to note is the variety of actors that have a role in the IoT ecosystem. Using the layer model of the previous paragraph, and without aiming to name every possible entity involved with this ecosystem, we can identify the following. First, the device layer includes the user that controls the device and the device manufacturer, including various third party manufacturers of the hardware components (sensors, chips, RFID tags) and firm/software components. Second, the network and common services layer consists of internet service providers like internet access providers and hosting providers. Third and last, the application layer comprises of a variety of application service providers, which may be the same as the device manufacturer (vertical integration). In that scenario, the device manufacturer also provides the smartphone application via which the user communicates with the device. We can also think about including *the device itself* as an actor in this list, because a smart device is capable of making decisions based on data analysis (intelligent decision making) and can communicate with the user and other machines,[102] which may mean that it has agency of its own.[103] This is an interesting perspective to note, though a full exploration of the topic falls outside the scope of this thesis.

So far, we have at least four different types of actors with a role to play in the IoT ecosystem: end-users, device manufacturers, network and communication providers, and application service providers. Each type involves more than one actor. For example, under device manufacturers we can include the manufacturer of the final device, but also the manufacturers of various components such as hardware (e.g. chips, processors etc.) and software (e.g. firm/software on the device, user interface application etc.). The question quickly becomes: what is expected from each of them with regard to cybersecurity and who is responsible when things go wrong?

This section has shown the complexity of this question by giving a basic explanation of how data travels through the IoT ecosystem and the various actors that are involved to achieve this. From now on, the focus will be on the relationship between the end-user and the device manufacturers. In particular; is the manufacturer of the final device legally responsible for an adequate level of cybersecurity in the smart devices that it puts on the market? Where relevant we will assume that this device manufacturer is also the application service provider, i.e. the smart home device is bundled with a mobile application. Problems relating to network security or cloud providers will not be included.

[101] Ibid.

[102] ENISA, 'Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures' (n 91) 19.

[103] See e.g. Mitew (n 86).

2.3 Three smart home devices

In the last section of this chapter, three smart home devices will be introduced that serve as case studies throughout this thesis. The purpose is to gain an understanding of the functionalities of the three smart home devices, how they differ from their traditional "offline" counterparts in terms of both functionality and security, and how they function in the existing home infrastructure. In each smart home device, we consider the trade-off between increased functionality and loss of security. We will look into smart thermostats, smart locks and smart baby monitors respectively.

2.3.1 Smart thermostats

The function of any thermostat is to regulate the heating in a home. A normal "offline" thermostat is operated manually by a person and possibly programmed to run a heating schedule. A smart thermostat automates this process. It is capable of learning heating preferences, so that it is not necessary to turn the heating on or off when you wake up, go to sleep or leave the house. It is also possible to manually change the heating, either on the device itself or remotely by using an app on your phone or tablet. Some smart thermostats also send you notifications when the home temperature is too far below or above your set "safety temperature".[104] Examples of current producers of smart thermostats offering their products in Europe include Nest Labs Inc. and Eneco B.V. (Toon thermostat).[105]

As explained in section 2.2, a smart thermostat is capable of all this because of the embedded sensors, collection of data, online storage and analysis of data leading to decision making and execution by actuators. Some smart thermostats have up to 10 temperature sensors, and sensors for indoor humidity, proximity, near-field and far-field activity and ambient light.[106] The collected data travels through the various communication layers to reach a server, where it is analysed for decision making. The data is also visualised for the end-user in a mobile application, which serves as communication channel between the device and the end-user as well. Viewed as such, a smart thermostat is more than merely a product; it also provides services to the end-user. Typically the owner of a smart home device will have a user account via which access to and communication with the smart home device is possible, for example obtaining real-time information on heating.

A smart thermostat is embedded into the heating infrastructure of the house. This comprises both products and services also. On the one hand, it is made up of physical parts (products) like water pipes, actuators, radiators and boilers. One the other hand, it requires water, gas and electricity to function, which is provided by utility service providers. The smart thermostat relies on the existing heating

[104] Functionalities derived from the Nest Labs Inc. 3rd Generation Learning Thermostat and Toon Thermostaat.
[105] See https://nest.com/thermostats/ and www.toon.nl. Both on sale on e.g. online retailer www.bol.com.
[106] Nest, 'Nest thermostat technical specifications' <https://nest.com/support/Article/Nest-Learning-Thermostat-technical-specifications> accessed 29 November 2017.

infrastructure in the house in order to fulfil its traditional purpose of heating the house. In case of a failure elsewhere in this infrastructure, e.g. unavailability of utility service, it will not be able to perform this task.

Because of the connection to the internet, a smart thermostat creates cybersecurity concerns. It therefore adds to the possible causes of failure of the heating system. In particular, a third party may be able to gain access to the device and control it from a remote place. Moreover, the collection of information regarding heating preferences and whether someone is home or not constitutes processing of personal data and relates to the privacy of the home. A traditional thermostat does not collect this personal data, which means it is also not at risk. Placed in a wider perspective, other relevant developments in this context include smart energy grids and smart meters (which measure the energy consumption in a house).[107]

2.3.2 Smart locks

Home security is another popular area for smart home devices. This includes for example smart alarm systems and smart security camera's. Here, we focus on smart locks. Examples of current producers of smart locks offering their products in Europe include August Home Inc. and Nuki Home Solutions GmbH.[108]

A normal "offline" lock consists of two physical parts: a lock and a key. It furthermore relies on a key-recovery infrastructure, e.g. the locksmith in the neighbourhood is capable to copy most keys or to replace a lock where the key is lost. Some keys can only be replaced via a special service that is more expensive or requires identification. The key-recovery adds a service element to the traditional key infrastructure. Practically all traditional locks have insecurities and can be broken. Another option is to circumvent the locked door by accessing the house via alternative ways, e.g. a window. Moreover, the strength of any lock can be undermined by the owner's behaviour. When you use a strong lock but put the key under the mat, how secure is your house?

In the case of a smart lock, the physical lock can be operated by a smartphone or other token that functions as the key. Some smart locks also have additional functionalities like tracing who enters and exits the house, sending notifications when someone is at the door, etc. A mobile application deals with access permissions and as such functions as key-recovery infrastructure. Where you lose your phone or other token, you use the mobile application to revoke permission and to activate another device or

[107] See e.g. Patrick McDaniel and Sean W. Smith, 'Security and Privacy Challenges in the Smart Grid' (2009) 7(3) IEEE Security and Privacy, 75; Costas Efthymiou and Georgios Kalogridis, 'Smart Grid Privacy via Anonymization of Smart Metering Data' (First IEEE International Conference on Smart Grid Communications, October 2010).
[108] See http://august.com/ and https://nuki.io/en/.

token.[109] In some cases, you can also simply remove the smart lock from your door and restart using your old lock. Like traditional locks, smart locks can be compromised. It also creates additional security issues compared to traditional locks, i.e. cybersecurity issues.

Both in terms of functionality and security, a distinction can be made between smart locks which work on low-range communication technologies (e.g. BlueTooth) and those that connect to the internet. In case of the former, you can use your phone or another token as a key to operate the door only when you are near. This also means that only people who are near are able to intercept data traffic and compromise the smart lock. In case of the latter, it is possible to operate the door from a remote location. In terms of functionalities, it is likely to have additional features like tracking and notifications. Because of the connection to the open internet, the attacker can try to hack the smart lock from a remote place instead of having to be on site.

Any lock or house can be compromised. A smart lock gives attackers an additional route for this, namely by taking advantage of cybersecurity vulnerabilities. The key-recovery infrastructure may be insecure, allowing third parties to give themselves permissions and gain access to the house. If someone hacks your smart lock, does this constitute proof of trespassing for the purpose of your insurance? Also, internal software flaws may cause the smart lock to shut down, excluding an owner from their home. The collection of data about the owners' whereabouts raises privacy concerns that are new to this type of product.

2.3.3 Smart baby monitors

Baby monitors allow parents to listen in on their baby from another location in or around the house. More traditional baby monitors or baby phones function on radio technology. Smart baby monitors additionally rely on connection to the internet via the local Wi-Fi. It may have the following functionalities.[110] It can have a microphone and camera, whereby the audio and video feeds are transmitted over the internet to be viewed on a smartphone or tablet and to take snapshots. To ensure that user has his or her baby in view, it may also be possible to remotely tilt, pan or zoom the camera. It could also be that the baby monitor has a speaker, so that it is possible to speak to the child from another place, or put on lullabies. Furthermore, it may have sensors that can measure temperature, humidity, noise and activity in the room. On the basis of this information the device may be capable of sending you notifications like "all is calm in Max's room".

[109] August Support, 'Lost Phone' < http://support.august.com/customer/en/portal/Articles/2169319-lost-phone?b_id=10919&> accessed 23 February 2018.

[110] Functionalities derived from the 'Supreme Connect Premium Digital Baby Monitor' from producer Luvion (see: https://www.luvion.nl/babyfoon-met-camera/) and Motorola's 'Smart Nursery 7 Portable Wi-Fi Video Baby Monitor (see: https://motorolastore.eu/baby-monitors/smart-nursery/smart-nursery-7-video-baby-monitor.html)

Examples of current producers of smart baby monitors in Europe are eBuyNow eCommerce Limited (brand name Motorola) and Lucunculus BV (brand name Luvion).[111]

The additional functionalities of smart baby monitors come at a cost when cybersecurity in these products is lacking. The video and/or audio streams may be intercepted by unauthorised third parties. Moreover, the smart baby monitor may be remotely accessed and operated by unauthorised persons. Although someone else may listen in on a traditional baby monitor that functions on radio technology, the majority of these problems involving smart baby monitors are new and relate to the added internet connection. Unlike the other smart home devices that we discussed, smart baby monitors are not embedded in the house in a semi-permanent way like a thermostat or a lock. It only relies on the Wi-Fi connection in the house to function properly.

2.4 Chapter conclusion

In this chapter we explored the domain of smart home devices. The smart home has been defined as "a residence incorporating a range of sensors systems and devices that can be remotely accessed, controlled, and monitored via a communication network."[112] We have also examined and defined the broader development that it is a part of, the Internet of Things: "an ecosystem in which applications and services are driven by data collected from devices that sense and interface with the physical world.[113] In particular, we have considered the variety of actors that are involved in this complex ecosystem. As such, whilst the legal analysis in Part II focuses on the responsibility of device manufacturers, their role is placed in a broader perspective.

The excitement about the smart home can be offset with concerns about privacy and security. With regard to privacy, smart home devices raise significant concerns because the fundamental privacy of the home is violated. This also relates to cybersecurity problems in smart home devices, which we will consider in the next chapter. There, we will also return to the three smart home devices considered at the end of this chapter.

[111] See https://motorolastore.eu/baby-monitors and https://www.luvion.nl/babyfoon-met-camera/

[112] Bugeja et al. (n 63) 1.

[113] OECD (no 92) 9.

Chapter 3: Cybersecurity problems in smart home devices

Various incidents with smart home devices demonstrate a general lack of cybersecurity in smart devices, including smart home devices.[114] This chapter aims to deepen our understanding of this problem. In the first half of this chapter, we will examine the concept of cybersecurity more clearly and look at three common security vulnerabilities in smart devices and technical solutions. In the second half, we will consider three security incident scenario's involving these vulnerabilities and identify remedies in private law that can be used to compensate or prevent the harms they may cause.

This chapter is not intended to provide a full account of the concept of cybersecurity and all possible security issues in smart home devices. Rather, the aim is to get an understanding how certain cybersecurity vulnerabilities may cause problems in smart home devices and consequently risk and harm to consumers. We use this frame of reference to identify meaningful legal solutions.

3.1 Understanding cybersecurity

Cybersecurity is a complex, broad and ambiguous term whose exact scope and meaning are unclear. [115] It is used as a key term in this thesis to target a particular type of problem with smart home devices and to distinguish it from more traditional product issues.[116] The lack of consensus on the meaning and scope of the term makes it important to clarify some issues. This will be done by answering two questions. First, cybersecurity from the perspective of whom? Second, what does it mean to have cybersecurity?

First, cybersecurity from the perspective of whom? Put differently; who is the intended beneficiary of improved cybersecurity of smart home devices? The individual or society at large? The answer to this question depends on the conception of cybersecurity that you adhere to. Privacy scholar Helen Nissembaum has distinguished between two perspectives on cybersecurity that capture this difference: "technical computer security" and (confusingly) "cyber-security".[117] Though these two perspectives are not completely incompatible, they emphasize different issues and have a different scope.[118] They each answer to different types of threats and have different justificatory force; the national security discourse generally warrants more radical and far-reaching measures compared to the technical computer security discourse.[119]

[114] See: Chapter 1.1.

[115] Axel Arnbak, 'Securing Private Communications' (PhD dissertation, University of Amsterdam 2015) 160; Rolf Weber and Evelyne Studer, 'Cybersecurity in the internet of things: Legal aspects' *Computer Law and Security Review* 32 (2016) 715, 716.

[116] See: Chapter 1.2.2.

[117] Helen Nissenbaum, 'Where Computer Security Meets National Security' (2005) 7 Ethics and Information Technology 61.

[118] Ibid, 63.

[119] Ibid, 69.

This thesis adheres to the first conception of cybersecurity: technical computer security. In technical computer security, the focus is placed on the people who use, own or may be affected by computers and networks. It seeks to secure people at an *individual level*; protecting their person and their property from harm. For example, protecting individuals against a ransomware attack. As such, this approach fits with the research focus on private harm caused by cybersecurity vulnerabilities in smart home devices and remedies in private law. It can be contrasted with the second perspective – cyber-security – which focuses on security at a *collective level* and is closely tied to the field of national security. Its aim is to keep society as a whole safe from harm. This includes preventing cyber-attacks on critical infrastructure (e.g. banks, hospitals, harbours), as these types of attacks have a disruptive effect on society. For example, a study of the DDoS attacks by the Mirai botnet would adhere to this conception of cybersecurity.[120]

The second question we ask is: what does it mean to have cybersecurity? More specifically, how to ensure technical computer security in smart home devices? The generally accepted conceptual framework in this context is the so-called CIA-triad.[121] It stands for Confidentiality, Integrity and Availability. Together, they are considered to be the principal attributes of technical computer security. They can be defined as follows:[122]

- Confidentiality: “the assurance that data, programs and other system resources are protected against disclosure to unauthorized persons, programs or systems.”
- Integrity: “the assurance that data, programs, and other system resources are protected against malicious or inadvertent modification or destruction by unauthorized persons, programs or systems.”
- Availability: “the assurance that use of data, programs, and other systems resources will not be denied to authorized persons, programs or systems.”

In other words, confidentiality is about ensuring that only the intended recipients are given access to systems and information. Integrity is the security attribute that seeks to ensure that systems and information are not tampered with by entities that are not allowed to. Availability seeks to ensure that systems and information are accessible and functioning for those who are permitted access.

At a first glance, the CIA-triad may be hard to relate to a particular security incident. By focusing on the security attributes that a system should have, it abstracts from particular threats or incidents. Put simply, insufficient technical computer security, i.e. a shortcoming in any of the attributes, creates

[120] ENISA, ‘Major DDoS Attacks Involving IoT Devices’ (ENISA Suggested Reading, 3 November 2016) <https://www.enisa.europa.eu/publications/info-notes/major-ddos-attacks-involving-iot-devices> accessed 6 February 2018.

[121] Arnbak (no 115) 155-161.

[122] Arnbak (no 115) 156; Charles P. Pfleeger, ‘Data Security’ in Anthony Ralston et al. (eds) *Encyclopedia of Computer Science 4th Edition* (Nature Publishing Group 2000) 504.

vulnerabilities that pose *threats* to security. Those threats may materialize in *security incidents* and these incidents may create *harm*. The process of how vulnerabilities lead to harm is depicted in figure 2.

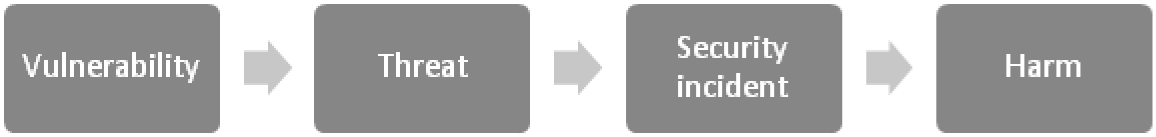

Figure 2: the process leading up to a security incident which may result in harm.

In figure 2, a vulnerability represents “weaknesses or mistakes in a device or system that allow an unauthorized entity to locally or remotely execute demands, access or modify unauthorized data, interrupt normal operation of a system, and/or damage a system.”[123] Such vulnerabilities lead to threats, which can be defined as “a potential to exploit a vulnerability [...]”[124] When a threat materialises, we are confronted with a security incident. Thus, taken altogether, a security incident arises from “a lack, failure or breach of confidentiality, integrity and/or availability of data or other system resources”.[125] Depending on the circumstances, this security incident may cause harm. It is important to notice the broad scope of the definition of a security incident. It does not only cover an intentional breach of the security attributes (e.g. malicious hackers), but also a lack or failure of these security attributes in a system or device (e.g. not having an update mechanism), which may be unintentional.

Having adequate technical computer security does not only mean preventing security incidents from occurring, but also responding to them in an appropriate fashion. Risk analysis is the process of identifying risks and threats and taking measures aimed at prevention, detection, repression, recovery and correction of security incidents.[126] The security attributes of the CIA-triad give guidance to this process as security goals, but they are not in themselves sufficient.[127] The process of getting from security goals to security requirements and technical specifications is a whole area of study in itself.[128] It goes beyond the scope of this thesis to look into this. In the next section, we will look into security vulnerabilities in smart home devices and the threats they pose to consumers.

[123] Musa G Samaila et al., ‘Security Challenges of the Internet of Things’ in Batalla et al. (eds) *Beyond the Internet of Things: Everything Interconnected* (Springer International Publishing AG 2017) 71.
[124] Ibid, 70.
[125] Arnbak (no 115) 157.
[126] Cbp, ‘Richtsnoeren voor beveiliging persoonsgegevens’ (Cbp, 2013) 15.
[127] Arnbak (no 115) 165.
[128] Ibid, 165-171.

3.2 Common cybersecurity vulnerabilities in smart devices

A host of security vulnerabilities can be identified within the IoT ecosystem. Cybersecurity problems exist and arise in all the different transport layers of the communication model.[129] This thesis focuses on the responsibility of device manufacturers (incl. producers of hardware and software components) and thus mostly relates to the device layer of the communication model.[130] In this section we will discuss three common cybersecurity vulnerabilities in smart devices: what are they and what threats do they pose? It is important to note that cybersecurity is a dynamic and debated field. With new technological developments also new cybersecurity issues arise that need to be addressed. Computer scientists debate about best practices in cybersecurity, i.e. the best ways to achieve an adequate level of cybersecurity. Because of the dynamic and evolving nature of this field, it is difficult ground for a legal analysis.

The security vulnerabilities are taken from the top 10 security flaws in the IoT by the Open Web Application Security Project (OWASP).[131] This top ten relates to all IoT devices and includes, but is not limited to smart home devices. All three can be (at least partially) attributed to device manufacturers. The assumption throughout is that taking measures against these common cybersecurity vulnerabilities belong to basic cybersecurity practices that can be expected from manufacturers of smart home devices. The following three cybersecurity vulnerabilities will be considered:

1. Soft/firmware vulnerabilities;
2. Insufficient authentication/authorization; and
3. A lack of transport encryption.

The vulnerabilities relate mainly to the software components of smart devices. Security flaws relating to hardware will not be included in the discussion. This is not to say that hardware problems with smart devices are irrelevant for cybersecurity. Poor physical security is also listed as a cybersecurity concern by OWASP.[132] This includes, for example, the need to ensure that USB ports or other external ports cannot be used maliciously to hack the device.[133] These are concerns that are of particular interest for smart devices that are not within the home, but accessible from a public place. Smart home devices are a more difficult target for physical attacks because of their location in the house. For this reason, cybersecurity vulnerabilities relating to hardware are not further taken into account. Another thing to note beforehand is that some features of the three security vulnerabilities overlap. For example, transport

[129] See: Chapter 2.2.2 (application layer, network and data communications layer and device layer).

[130] For an elaborate threat taxonomy related to the various assets in the IoT, see ENISA, 'Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures' (ENISA, November 2017) 32.

[131] OWASP, 'Top IoT vulnerabilities'<https://www.owasp.org/index.php/Top_IoT_Vulnerabilities> accessed 5 December 2017.

[132] OWASP, 'Top IoT vulnerabilities'(no 131) .

[133] OWASP, 'Top 10 2014-I 10 Poor Physical Security' < https://www.owasp.org/index.php/Top_10_2014-I10_Poor_Physical_Security> accessed 21 February 2018.

encryption also plays a big role in having a secure software update mechanism which is important for patching *software vulnerabilities*.

3.2.1 Soft/firmware vulnerabilities

A smart home device consists of two main components: hardware and soft/firmware. The former refers to the physical elements that make up the device. As mentioned, physical security issues relating to IoT devices will not be explored further here. Software, in general terms, is a set of instructions or programs instructing a computer to do specific tasks; it is a name for all the computer programs that run on the hardware.[134] Firmware is a type of software that is semi-permanently written on the hardware and that is critical for the functioning of the device or the particular part of hardware.

It is generally recognised that it is not possible to create software that is 100% secure or completely bug-free. Known software vulnerabilities ("bugs") can be exploited and unknown vulnerabilities can be discovered. A software vulnerability can often be repaired ("patched") via a software update. Having secure software is therefore an ongoing process which runs throughout the lifecycle of the software. First, it is important to equip devices with up-to-date software from the start, i.e. at the moment that the device leaves the factory. Second, it is important to have a secure update mechanism.[135]

Having such an update mechanism ensures that security updates are enabled. Securing such a mechanism involves encryption of both the connection via which the update is downloaded and encryption of the update files themselves, so that unauthorized persons are prevented from intercepting and modifying these files or performing their own updates (e.g. installing malware on the device).[136] Other security measures include ensuring that the update server is secure, that it does not expose sensitive data, that the update file is authenticated before it is applied, and possibly implementing a secure boot (a safe restart of the device).[137]

We should note that software updates and update mechanisms are no panacea. Not all software vulnerabilities can be repaired via a software update, even with an update mechanism in place. Some software vulnerabilities require a replacement of hardware, which is a much more cumbersome task than issuing a software patch. Moreover, software updates may have a negative on the performance of the device. This became apparent in the recent aftermath of the Spectre and Meltdown security flaws involving computer chips, in which a Microsoft executive stated that in some circumstances the security

[134] Techopedia Dictionary, 'Software' <https://www.techopedia.com/definition/4356/software> accessed 7 December 2017.

[135] OWASP, 'Top 10 2014-I9 Insecure Software/Firmware' <https://www.owasp.org/index.php/Top_10_2014-I9_Insecure_Software/Firmware> accessed 7 December 2017.

[136] Ibid.

[137] Ibid.

gains would not outweigh the performance losses resulting from the software patch.[138] Another side effect is that security updates are often bundled with feature updates (changes in functionality) in so-called service packs, whilst these changes in functionality may be undesired by the consumer.[139]

Regardless of the exact solution to the problem of software vulnerabilities and updates, software in IoT devices is often lacking in all the areas mentioned above. For one, IoT devices often ship from the factory with software that is already outdated. This means that the software contains many known vulnerabilities that can be exploited as soon as the device is first connected to the internet.[140] For this reason, it is important that a security update is implemented during the first configuration of the device in the user's home. Second, IoT devices may not have an appropriate update mechanism to patch vulnerabilities.[141] There may not be an update mechanism at all, or the update mechanism is insecure. This is problematic in the IoT especially for devices with a long lifecycle, i.e. devices that are not often replaced. A finding of the HP research study into security of popular IoT devices was that 60% of the devices did not use a secure connection to download updates or and did not encrypt update files.[142]

Insecure software in smart devices creates threats to cybersecurity. A distinction can be made between internal and external threats. Internal threats are software vulnerabilities that can cause a security incident on their own. For example, a software bug in a smart thermostat can cause the battery to drain and shut the device off completely, sending the house it was supposed to warm in a chill. [143] This security incident does not occur from an external attacker exploiting a soft/firmware vulnerability, rather, there was an internal mistake in the software of the thermostat that caused this incident. External threats involve third parties that exploit a software vulnerability. For example, a thief hacking a smart lock to gain access to a residence, which is shown to be possible.[144] The exact threats that follow from a software vulnerability depend on the circumstances of the case. Generally, insecure soft/firmware can lead to a

[138] Richard Waters and Hannah Kuchler, 'Intel and Microsoft sow confusion over security flaw' *The Financial Times* (San Francisco, 11 January 2018) <https://www.ft.com/content/f31e0b2a-f6f6-11e7-88f7-5465a6ce1a00> accessed 12 January 2018.

[139] Mark Ciampa, *Security Awareness: Applying Practical Security in Your World* (fifth edition, Cengage Learning 2017) 92.

[140] BITAG, 'Internet of Things (IoT) Security and Privacy Recommendations' (BITAG, November 2016) 7 <https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf> accessed 22 November 2017.

[141] Ibid.

[142] Hewlett Packard Enterprise, *Internet of things research study* (HP, November 2015) 5 <http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf> accessed 5 December 2017.

[143] Nick Bilton, 'Nest Thermostat Glitch Leaves Users in the Cold' *The New York Times* (New York City, 13 January 2016) < https://www.nytimes.com/2016/01/14/fashion/nest-thermostat-glitch-battery-dies-software-freeze.html> accessed 12 December 2017.

[144] Megan Wollerton, 'Here's what happened when someone hacked the August Smart Lock' (*cnet*, 25 August 2016) <https://www.cnet.com/news/august-smart-lock-hacked/> accessed 12 December 2017.

unauthorized access or misuse of (personal) data, unauthorized control of the device or attacking other systems (e.g. through DDos attacks).[145]

3.2.2 Insufficient authentication/authorisation

The second cybersecurity flaw is insufficient authentication and/or authorisation. Authentication in the context of computing means "the process or action of verifying the identity of a user or a process".[146] In other words, it is the process of *identifying* a user, usually by a username and password.[147] It seeks to ensure that the exchanged information is from the source it claims it to be from.[148] On the other hand, the action of authorising means to "give official permission for or approval to (an undertaking or agent)".[149] In the context of computing, authorization refers to the process of *giving access* to a user based on their identity.[150] In sum, insufficient authentication or authorization as a security flaw means that the processes of (1) identifying a user and (2) allowing access to a system are insecure.

In practice, an important and easily achievable security solution is to have secure password management. This includes ensuring that strong passwords are technically possible and required. It also means having unique usernames and passwords as default or requiring users to change them when setting up the device, and not having backdoor admin accounts that can easily be exploited. Furthermore, it includes other features like ensuring secure password recovery mechanisms (for when you forget your password), protected storage of credentials, ensuring granular access control where necessary, implementing two-factor authentication where possible, and more.[151] A strong password policy may also include prompts to periodically renew passwords, though this practice is debated. According to research, forcing people to regularly change passwords results in predictable patterns and variations of the same passwords.[152] It has been mathematically demonstrated that the inconvenience to users for periodically

[145] OWASP, 'Top 10 2014-I9 Insecure Software/Firmware' (no 135).
[146] Oxford Dictionaries, 'Authentication' <https://en.oxforddictionaries.com/definition/authentication> accessed 5 December 2017.
[147] Techopedia Dictionary, 'Authentication, Authorization and Accounting (AAA)' <https://www.techopedia.com/definition/24130/authentication-authorization-and-accounting-aaa> accessed 7 December 2017.
[148] Samaila et al. (n 123) 59.
[149] Oxford Dictionaries, 'Authorise' <https://en.oxforddictionaries.com/definition/authorize> accessed 5 December 2017.
[150] Webopedia, 'Authentication' <https://www.webopedia.com/TERM/A/authentication.html> accessed 5 December 2017.
[151] OWASP, 'Top 10 2014-I2 Insufficient Authentication/Authorization' <https://www.owasp.org/index.php/Top_10_2014-I2_Insufficient_Authentication/Authorization> accessed 5 December 2017.
[152] Brian Barrett, 'Want safer passwords? Don't change them so often' (*Wired*, 3 October 2016) < https://www.wired.com/2016/03/want-safer-passwords-dont-change-often/> accessed 21 February 2018.

changing their passwords does not outweigh the security gains.[153] This debate shows the dynamic nature of cybersecurity good practices.

IoT devices, including smart home devices, are notorious for having weak (default) passwords like "1234" or "password". Several reports confirm that weak passwords constitute a serious security flaw in the IoT. In a 2015 study reviewing the most popular IoT devices, including smart thermostats and smart locks, computer company HP found that 80% of devices (along with their cloud and mobile application components) failed to require passwords of a sufficient complexity and length.[154] In their words: "A strong password policy is Security 101 and most solutions failed."[155] Another 2015 study that looked specifically into the security of baby monitors also identified weak default passwords of local accounts as a common security flaw.[156] This is still a current issue; according to a June 2017 report of Semantic, default passwords remain the biggest security weakness for IoT devices.[157]

A notable example of a security incident involving the exploitation of weak passwords is the Mirai botnet. It accessed and used ("herded") 400,000 IoT devices through the use of 61 common username-password combinations, like admin-admin or admin-1234.[158] The Mirai botnet was used to launch various distributed denial of service (DDoS) attacks against websites, either by directly attacking the website or by targeting a DNS or hosting provider.[159] The attacks resulted in temporary unavailability of these websites, including Spotify, Twitter and Paypal.[160] Other notable security incidents that were likely caused by weak (default) passwords include the hacking of baby monitors whereby the video feeds were put online[161] or where unauthorized persons used the speakers to yell to a baby.[162] Other reported

[153] Ibid.
[154] Hewlett Packard Enterprise (n 142) 5.
[155] Ibid.
[156] Mark Stanislav and Tod Beardsley, 'HACKING IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities' (Rapid7, 2015) <https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf> accessed 5 December 2017.
[157] Symantec, 'Internet Security Threat Report' (Symantec, 2017) 66 <https://www.symantec.com/content/dam/symantec/docs/reports/gistr22-government-report.pdf> accessed 5 December 2017.
[158] Steve Ragan, 'Here are the 61 passwords that powered the Mirai IoT botnet' (*CSO*, 3 October 2016) <https://www.csoonline.com/Article/3126924/security/here-are-the-61-passwords-that-powered-the-mirai-iot-botnet.html> accessed 5 December 2017.
[159] See for a timeline of the Mirai botnet attacks: ENISA, 'Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures' (ENISA, November 2017) 30.
[160] Symantec, 'Mirai: what you need to know about the botnet behind recent major DDoS attacks' (*Symantec Official Blog*, 27 October 2016) <https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks> accessed 5 December 2017.
[161] Conor Gaffey, 'Web of Insecurity: Hacked Baby Monitors Highlight Perils of Internet of Things' (*Newsweek*, 9 april 2015) <http://www.newsweek.com/baby-monitors-hackhack-baby-monitorsbaby-monitorsinternet-thingsinternet-600746> accessed 5 December 2017.
[162] NBC News, 'Man Hacks Monitor, Screams at Baby Girl' (*NBC News*, 28 April 2014) <https://www.nbcnews.com/tech/security/man-hacks-monitor-screams-baby-girl-n91546> accessed 5 December 2014.

incidents include obtaining access control to an entire smart home by complete lack of password protection of the home automation system.[163]

These examples show some of the possible consequences of weak password management or insufficient authentication/authorization more broadly. According to OWASP, insufficient authentication and authorization can result in "data loss or corruption of data, a lack of accountability, or denial of access and can lead to complete compromise of the device and/or user accounts."[164]

3.2.3 Lack of transport encryption

A third cybersecurity vulnerability in smart devices is a lack of transport encryption. According to the Oxford English Dictionary, to encrypt means "[t]o convert (data, a message, etc.) into cipher or code, esp. in order to prevent unauthorized access; to conceal *in* something by this means".[165] In other words, it is the process of making information illegible for unintended recipients. In electronic communications, one of the main functions of encryption is to preserve the confidentiality of information.[166] Another is the authentication of information; establishing the source of the information and ensuring the information has not been tampered with.[167] In this subsection we will focus on encryption for the purposes of confidentiality, as the importance of authentication has been discussed in paragraph 2.3.1. The focus will furthermore be on a lack of *transport* encryption, which means the topic of encryption of data in storage (on the device or in the cloud) will not be discussed.

Encryption of information is achieved by translating an understandable (*plaintext*) phrase into an unintelligible one (*ciphertext*) that can be decrypted through use of the encryption key that has been shared between the trusted (authenticated) sender and recipient. This can be done by various cryptographic methods like symmetric cryptography or public key cryptography.[168] When an IoT device transmits unencrypted data it can be intercepted in plain text as it travels over the local network or the internet, meaning that the information is clear for all to see. This is especially problematic if it concerns sensitive (personal) information or, for example, username and password combinations.

According to OWASP, in IoT devices there is often a lack of transport encryption when data is transmitted to the local network. This makes the information vulnerable for interception by anyone within

[163] Kashmir Hill, 'When 'Smart Homes' Get Hacked: I Haunted A Complete Stranger's House Via The Internet' (*Forbes*, 26 Juli 2013) <https://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/#1e25032fe426> accessed 7 December 2017.

[164] OWASP, 'Top 10 2014-I2 Insufficient Authentication/Authorization' (no 151).

[165] Oxford English Dictionary, 'Encrypt' <http://www.oed.com> accessed 10 December 2017.

[166] Seda Gürses and Bart Preneel, 'Cryptology and Privacy in the Context of Big Data' in Bart van der Sloot et al. (eds) *Exploring the boundaries of big data* (Amsterdam, Amsterdam University Press 2016) 53.

[167] Ibid.

[168] Ibid.

the range of the local network.[169] In a study of IoT devices conducted by HP in 2015, one of the main findings was that a majority of the devices – 70 percent – did not encrypt data that was transmitted to the local network or the internet.[170] A complicating factor in the realization of transport encryption in IoT devices is that some devices are resource-constrained, meaning they have limited processing power and memory.[171] Depending on the exact features of the device, some cryptographic solutions will be impossible. Lightweight encryption mechanisms are therefore of paramount importance for securing IT devices.[172] For example, BITAG calls upon device manufacturers to use Transport Layer Security (TLS) or Lightweight Cryptography (LWC) to ensure transport encryption.[173]

A lack of transport encryption is obviously a threat to confidentiality of (personal) information in transit. The data may be intercepted and fall into the hands of unauthorized persons (e.g. man-in-the-middle attack), and if critical information like usernames and passwords are intercepted the complete device or account may be compromised.[174]

3.2.4 Reasons why cybersecurity is lacking in smart devices

A question that has not yet been dealt with so far relates to the causes of a lack of cybersecurity in smart home devices. Why is cybersecurity lacking? Why are not even basic cybersecurity practices adhered to by smart device manufacturers? Whilst not attempting to exhaustively answer this question, this subsection aims to hint at some of the reasons why the current landscape of cybersecurity in the IoT and the smart home is rather gloomy.

There are three often mentioned reasons that each attribute fault or responsibility to different actors. First, the inherent limitations of some smart devices in terms of resources and interfaces. Smart devices are designed with trade-offs between size, weight power, memory and processing power and price.[175] As a result, certain smart devices are equipped with limited hardware which means they have little processing power and memory, thus not enabling certain security solutions.[176] According to ENISA, the majority of smart devices have such limited capabilities.[177] An example would be that a smart lock

[169] OWASP, ‘Top 10 2014-I4 Lack of Transport Encryption’ <https://www.owasp.org/index.php/Top_10_2014-I4_Lack_of_Transport_Encryption> accessed 7 December 2017.
[170] Hewlett Packard Enterprise (n 142) 5.
[171] Samaila et al. (n 123) 69-70.
[172] Tragos et al., ‘Securing the Internet of Things - Security and Privacy in a Hyperconnected World’ in Ovidiu Vermesan and Peter Friess (eds.) *Building the Hyperconnected Society* (River Publishers 2015) 198-199.
[173] BITAG (n 142) 19-20. See also: Tragos et al. (n 170) 198-199.
[174] OWASP, ‘Top 10 2014-I4 Lack of Transport Encryption’ (n 169).
[175] Cloud Service Alliance, ‘Future-Proofing the Connected World: 13 Steps to Developing Secure IoT Products’ (CSA, 2016) 17, <https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf> accessed 22 November 2017.
[176] BITAG (n 142) 5.
[177] ENISA, ‘Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures’ (n 159) 23.

does not have the capacity to use encryption mechanisms. Restricted or non-existent interfaces in smart devices limit its functionality and make it difficult to e.g. change a password or disable remote services.[178]

A second reason for a lack of cybersecurity in smart devices is a lack of technical knowledge and interest in cybersecurity on the side of the consumer.[179] End-users are often not aware of the cybersecurity risks. If they are, they are likely to lack technical knowledge to protect themselves or possibly do not even care. The impact of the consumer on the level of cybersecurity depends on the design of the smart device. Where a smart device (partially) relies on the end-user to ensure a level of cybersecurity, this may prove to be a weak spot. For example, entrusting consumers with the task of changing weak default passwords (such as 0000 or 1234) or downloading and installing software updates. It is also possible to design a smart device can with less reliance on the consumer, e.g. by using strong default passwords and using automated update mechanisms. One could say that the less influence a user has on the level of cybersecurity, the more responsibility the smart device manufacturer has for cybersecurity in the smart device.

The third reason for a lack of cybersecurity is a lack of technical knowledge and incentives to increase cybersecurity on the side of the device manufacturer. First, many smart device manufacturers are new to the domain of cybersecurity.[180] Often, traditional product developers add software and connectivity to their existing product portfolio without much attention for cybersecurity.[181] They do not have prior experience with privacy or security issues, and therefore lack expertise in these fields that are critical for designing and maintaining secure smart devices.[182] Second, smart device manufacturers lack incentives to increase cybersecurity in their devices. In essence, the market prioritizes features and low costs over security.[183]

The field of cybersecurity economics provides an insight into this problem. This research area studies the incentives that market players have to implement good, bad or no cybersecurity at all.[184] A lack of cybersecurity indicates a market failure (e.g. information asymmetry, negative externalities and moral hazard), meaning that the market does not punish manufacturers for putting products on the market

[178] BITAG (n 142) 5.
[179] Ibid, 3.
[180] ENISA, ‘Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures’ (n 159) 23.
[181] Cloud Service Alliance (n 175) 14.
[182] BITAG (n 142) 5-6.
[183] Bruce Schneier, ‘Testimony before the U.S. House of Representative in the Joint Hearing entitled Understanding the Role of Connected Devices in Recent Cyber Attacks’ (16 November 2016) 3 <https://www.schneier.com/essays/archives/2016/11/testimony_at_the_us_.html> accessed 5 December 2017.
[184] See on this topic: Hadi Asghari, ‘Cybersecurity via Intermediaries’ (PhD dissertation, University of Delft 2016).

with bad cybersecurity.[185] As a result, manufacturers are incentivized to keep costs low, not invest in cybersecurity measures, and push products to the market as quickly as possible to gain a competitive advantage. This market failure could be addressed by various measures, including legal solutions.

3.3 Three incident scenario's

In this section, we will consider three security incident scenario's that can result from each or a combination of the cybersecurity vulnerabilities outlined in the previous section. They are based on incidents that have occurred with these devices, some of which have been mentioned already.[186] For this reason, the incident scenario's may already sound familiar. The intention has been to touch on various types of issues relating to cybersecurity in smart home devices.

3.3.1 Smart thermostat

A software bug in a smart thermostat causes the battery to drain and the device to shut off completely. Its owners are not able to reboot the system and get it back to working. They have to wait for the software update from the manufacturer, who is slow to respond and difficult in communication. On the user forum of the manufacturer's website many people with the same thermostat complain about this issue. Imagine that it's winter. Because the thermostat does not work, the house temperature drops to below zero degrees. The house owners decide to stay at a friend's house until the thermostat functions again. While they are gone, the water pipes in the kitchen and bathroom walls freeze and burst, causing significant water damage to the house.

3.3.2 Smart lock

A budget smart lock was produced without much care for cybersecurity. In particular, it was designed with limited hardware to reduce production costs and compete on the smart lock market with a low purchase price. Because of these design choices, it was not possible to use any encryption mechanisms to encrypt the traffic travelling over the open internet (and to be honest, the manufacturers also lacked the interest and knowledge to even consider this). An IT-savvy thief searches Shodan (a search engine for internet-connected devices), finds a smart lock nearby and intercepts login credentials. In this way, he is able to gain control over the smart lock. This also provides access to personal data about the house owners whereabouts. Waiting until no one is home, the unauthorised access is used to open the door and steal high-value items like jewellery and art. The owner's insurance does not cover the value of the stolen

[185] Benjamin C. Dean, 'An Exploration of Strict Products Liability and the Internet of Things' (Center for Democracy & Technology, April 2018) 3 <https://cdt.org/files/2018/04/2018-04-16-IoT-Strict-Products-Liability-FNL.pdf> accessed 16 April 2018.
[186] See: Chapter 1.1.

items because of a lack of proof of trespassing. Besides suffering property damage in the form of lost items, the owners suffer from anxiety and distress and live in fear of another burglary.

3.3.3 Smart baby monitor

A smart baby monitor is supplied with a weak default password. In the instruction manual, only piecemeal attention is given to the importance of changing the default password. Buyers are not warned of possible cybersecurity risks relating to their privacy and security either. An unsuspecting mother is appalled when she finds out that the video-feed of her baby is accessible on a public website. Even worse, one night she hears an unfamiliar voice shouting in the nursery. Rushing to her crying infant, the mother realises that the unfamiliar voice comes from the baby monitor located in the room. Looking at the baby monitor she took from the living room, she is overcome with the creepy sensation that someone must have been listening in on her conversations all along. The mother suffers from anxiety and distress as a result of this incident.

3.4 Meaningful legal solutions

In the security incident scenarios outlined in the previous section, various types of harm were caused by smart home devices. Put differently; insufficient technical computer security measures resulted in vulnerabilities that materialised in actual incidents that caused harm to consumers. In this section, we will distinguish legal solutions that are meaningful in this context. Our focus is on private law remedies. Rather than approaching this immediately from a legal perspective, i.e. to which extent the Directive offers remedies, the list of meaningful legal solutions is inspired by the information in this factual background. In this way, both the merit and the shortcomings of the remedies offered by the Directive can be examined in the context of cybersecurity vulnerabilities in smart home devices.

Table 1 provides the list of remedies that are considered as meaningful.

	Product Liability Directive
COMPENSATORY MEASURES	
> Recovery of damages	
- personal injury	
- private property	
- other property	
- non-material harm	
PREVENTIVE MEASURES	
> Injunction	
- provision of security updates	
- repair or replacement of the device	
- information at the moment of sale	
- notification at the moment of security incident	

Table 1: Overview of meaningful remedies in private law

The meaningful legal solutions are divided in two categories: compensatory and preventive measures. Compensatory action is aimed at repairing the harm done as a result from the security incident: compensation of damages. This category is divided in four types of damages that might occur: damages caused by personal injury, damage to private property, damage to other property and non-material harm. The extent to which the recovery of these damages is possible under the Directive is discussed extensively in Chapter 7.

Preventive action is focused on preventing harm from occurring; preventing a security incident from happening or reducing the risk that a threat materialises. Such preventive action is possible by obtaining an injunction to compel a device manufacturer to take measures. In the context of cybersecurity vulnerabilities in smart home devices, interesting options would be to require a manufacturer to provide security updates, to otherwise repair or replace the device, or to provide information at the moment of sale or notification of a discovered vulnerability. In Chapter 7 we also consider the extent to which these type of remedies are available under the Directive.

It is important to realize upfront that the legal analysis focuses on a tort law instrument: the Directive. As such, the remedies that it offers are inherently limited. The Directive is mostly aimed at compensating damage caused by personal injury or damage to private property. By contrast, some of the preventive measures listed in table 1 can be characterised as contractual rather than tort law remedies. For example, repairing or replacing a device is typically a remedy under (consumer) contract law.[187] The provision of a security update can be seen as a concrete example of repair. Also information and notification obligations typically belong to (consumer) contract law.

When adhering to a strict distinction between contractual and tort law remedies, it thus makes no sense to look to a tort law regime like the Directive for these remedies. Yet, whilst not expecting that the Directive will provide all the solutions, we also aim to find out whether this unconventional route to preventive remedies might work under certain circumstances. This may seem like a radical approach, but due to the lack of specific rules in this area one has little other option but to rely on more general rules of and claim injunctive relief via this route.[188]

[187] This is a type of specific performance. See e.g. art. 3(2) and (3) of the Sale of Consumer Goods Directive 1999/44/EC.

[188] E.g. Consumentenbond v. Samsung. For the writ of summons (in Dutch) see: https://www.consumentenbond.nl/binaries/content/assets/cbhippowebsite/actie-voeren/updaten/dagvaarding-consumentenbond---samsung-11-nov-2016.pdf . For an English summary of the case so far see: Paul Verbruggen et al., *Towards Harmonised Duties of Care and Diligence in Cybersecurity* (European Foresight Cyber Security Meeting 2016), 78, 83-84 <https://ssrn.com/abstract=2814101> accessed 23 August 2017.

3.5 Chapter conclusion

In this chapter we have considered cybersecurity problems in smart home devices. Cybersecurity is conceptualised as technical computer security (which aims to protect the people who use, own or may be affected by computers and networks). This conception of cybersecurity fits with the research focus on private harm and remedies in private law. Technical computer security is achieved by observing the security attributes of the CIA-triad (Confidentiality, Integrity and Availability). Insufficient technical computer security, i.e. a shortcoming in any of the attributes, creates *vulnerabilities* that pose *threats* to security. Those threats may materialize in *security incidents* and these incidents may create *harm*. We have identified three common security vulnerabilities in smart devices: soft/firmware vulnerabilities, insufficient authentication/authorisation, and a lack of transport encryption. There are various technical solutions to prevent or reduce the threats that flow from them.

We considered three security incident scenario's with smart home devices that can result from each or a combination of the security vulnerabilities. This means that, at least to some degree, the technical solutions were not present in the smart home devices in these scenarios. A list of meaningful legal solutions has been presented, consisting of remedies in private law that would either compensate the damage resulting from these incidents or that allow a consumer to prevent such damage from occurring. The question that is central in Part II is whether the Directive applies to cybersecurity vulnerabilities in smart home devices and to which extent it provides these remedies. It is not expected that all the identified remedies are available under the Directive. The legal analysis aims to show both the merit and the shortcomings of the Directive and tentatively place them in a broader legal context.

PART II: LEGAL ANALYSIS

Chapter 4: Introducing European product liability law

In this chapter, European product liability law will be introduced. In section 4.1 some background information will be given on the Product Liability Directive (Directive), including about its purpose. Section 4.2 will provide an overview of the elements to a claim for product liability under the Directive. Sections 4.3 and 4.4 will cover two elements of such a claim: producer and causality. In the next chapters, the three remaining elements to the claim will be discussed more elaborately.

4.1 Background and purpose of the European Product Liability Directive

Product liability law is an area of law that deals with liability for defective products. It became an autonomous area of law from the moment that mass manufacture of consumer goods started to occur, first in the US and later in Europe also.[189] The European Commission (EC) started working on the Directive in 1968 and it was adopted in 1985.[190] Member States had three years to implement the rules. Though this process was not without troubles and delays, all Member States have implemented the rules of the Directive with only negligible shortcomings.[191] Initially the impact and number of cases decided under the Directive was limited, but it has gained significance from the turn of the century onwards.[192] Since its adoption, the Directive has not been substantially revised.[193] It is currently under review by the European Commission to evaluate whether it remains fit in light of new technological developments like the IoT.[194]

The Directive establishes a regime of strict liability for producers of defective products. This means that a producer is liable, without the need to prove fault or negligence, for defects in his products that cause damage.[195] The Directive aims for full harmonisation, which means that Member States are not at liberty to create more lenient or more stringent rules at the national level within its scope.[196] In other words, Member States cannot maintain a different liability regime for the matters regulated by the Directive. Member States are however at liberty to create liability for defective products on different legal grounds, for example general tort law.[197] Member States are furthermore free to legislate matters that are not within the scope of the Directive, for example liability of service providers or liability for non-

[189] Duncan Fairgrieve et al. ‘Product Liability Directive’ in Piotr Machnikowski (ed), *European Product Liability, an Analysis in the State of the Art in the Era of New Technologies* (Cambridge, Intersentia 2016) 19.

[190] Louise Dommering-van Rongen, *Productaansprakelijkheid: Een rechtsvergelijkend overzicht* (Deventer, Kluwer 2000) 5.

[191] Piotr Machnikowski, ‘Conclusions’ in Piotr Machnikowski (ed), *European Product Liability, an Analysis in the State of the Art in the Era of New Technologies* (Cambridge, Intersentia 2016) 672.

[192] Daily Wuyts, ‘The Product Liability Directive – More than Two Decades of Defective Products in Europe’ (2014) 5 *Journal of European Tort Law* 1, 2-3.

[193] NB. Directive 1999/34/EC extended the scope to include agricultural products and game, which was an optional exclusion under art. 2 and art. 15(1) of Directive 85/374.

[194] See Chapter 1.2.3.

[195] Article 1 and 4 Product Liability Directive.

[196] Article 13 Product Liability Directive. See: Duncan Fairgrieve et al. (no 189) 27-31.

[197] Article 13 Product Liability Directive.

material damage caused by a defective product. From this perspective, product liability law in a particular Member States may encompass more than just the rules provided by the Directive.

The Directive can be seen against the backdrop of European harmonisation of private law. In this context, various Directives have been formed in the field of consumer contract law and to a lesser degree in the context of tort and property law also.[198] The Directive was based on Article 100 of the Treaty of Rome (now Article 115 TFEU) which creates legislative competence for the European Union to regulate elements of private law that create obstacles to trade in the internal market.[199] The internal market considerations of the Directive can be found in the first recital thereto, which states that harmonisation of product liability law is necessary "because the existing divergences may distort competition and affect the movement of goods within the common market and entail a differing degree of protection of the consumer against damage caused by a defective product to his health or property".

Some authors contend that the internal market considerations were the primary driving force behind the Directive.[200] At the same time, the legislative basis was criticised because there were doubts whether competition was in fact disturbed by the differing national laws in the area of product liability.[201] According to Dommering-van Rongen, it is not unthinkable that the actual intention of the European legislator was to prevent further development in this field at the national level. She writes that these types of considerations were also the background of product liability law reforms in the US.[202] The limited legal basis available to the European legislator for harmonisation of private law remains to be a limiting factor at the present moment also.[203]

Besides internal market considerations, the Directive aims to protect consumers. This is reflected in recital 2 to the Directive, which states that "[…] liability without fault on the part of the producer is the sole means of adequately solving the problem, peculiar to our age of increasing technicality, of a fair apportionment of the risks inherent in modern technological production." Although consumer protection is not expressly mentioned, the Directive clearly indicates that strict liability for the producer is the only way to fairly distribute the risks for product defects. From a historical perspective, the adoption of the Directive had political momentum because of product tragedies at the time that harmed consumers.[204] Both products and their production and distribution processes became (and still become) more

[198] Arthur S. Hartkamp, *Asser 3-I Europees recht en Nederlands vermogensrecht* (Wolters Kluwer 2015) 147.

[199] Rafal Manko, *EU Competence in private law: The Treaty framework for a European private law and challenges for coherence* (European Parliamentary Research Service, 2015) 1, 8-9.

[200] Fairgrieve et al. (n 189) 26.

[201] Dommering-van Rongen (n 190) 5; Fairgrieve et al. (n 189) 26;

[202] Dommering-van Rongen (n 190) 5.

[203] Fairgrieve et al. (n 189) 26.

[204] Ibid, 19-20 and 26.

complicated and technical, which makes it difficult for consumers to have a clear view of the risks that the product poses to their safety.[205]

Hartkamp has noted that all directives in the field of private law predominantly have the purpose of consumer protection, including the Directive.[206] In this context it should be noted that, although not yet expressed as a fundamental right at the time that the Directive was adopted, consumer protection currently has the status of a fundamental right in the European Union. Article 38 of the Charter of the European Union states that "Union policies shall ensure a high level of consumer protection." As for all the rights in the Charter, Article 47 of the Charter provides the fundamental right to an effective remedy. These fundamental rights can have an indirect effect on the Directive via interpretation of the provisions in accordance with the fundamental rights and/or the review of provisions of the Directive against fundamental rights.[207]

4.2 Elements of a product liability claim

A claim for product liability under the Directive can be brought by an injured person. The injured person is not defined by the Directive. Considering the consumer protection aim of the Directive, it follows that the liability regime is created for consumers. According to legal scholars, the term was avoided because in EU law it generally indicates a natural person that enters into an agreement with a professional actor, which is something that product liability law does not require.[208] From a technical perspective, any injured party can claim under the European product liability regime. The merit of this legislative route for parties that are not consumers is however limited because the types of damage that are recoverable are aimed at consumers in the economic sense of the word.[209]

A claim under the European product liability regime has five elements: product, producer, defect, damage and causal link. First, there needs to be a product within the meaning of the Directive.[210] This requires there to be a movable and tangible good. Second, this product needs to be manufactured by a producer within the meaning of the Directive.[211] The concept of producer is broadly defined to ensure that the consumer will practically always find a liable person. Third, the product needs to be defective within

[205] Willem H van Boom en Karlijn J M van Doorn, 'Productaansprakelijkheid en productveiligheid' in Karlijn J M van Doorn en Sanne Pape (eds), *Handboek consumentenrecht* (Zutphen: Uitgeverij Parijs 2015) 261.

[206] Hartkamp (n 198) 147.

[207] Ibid, 210. See also: Chantal Mak, 'Rights and Remedies: Article 47 EUCFR and Effective Judicial Protection in European Private Law Matters' (2012) Amsterdam Law School Legal Studies Research Paper no. 2012-88; Centre for the Study of European Contract Law Working Paper No. 2012-11 < https://ssrn.com/abstract=2126551> accessed 25 January 2018.

[208] Fairgrieve et al. (n 189) 79.

[209] Ibid, 80.

[210] Article 1 and 2 Product Liability Directive. See: Chapter 5.

[211] Article 1 and 3 Product Liability Directive. See: Chapter 4.3.

the meaning of the Directive.[212] This is to be determined on the basis of the so-called consumer expectation test, whereby the safety that the average consumer is entitled to expect is the leading criterion. Fourth, the defect must have resulted in a type of damage that is recognised by the Directive.[213] Fifth, the injured person bears the onus of showing a causal link between the defect and the damage.[214]

Although the Directive aims for full harmonisation, this does not mean that it exhaustively regulates all facets of the liability regime that it establishes.[215] The first three elements, product, producer and defectiveness, are defined by the Directive and as such interpreted autonomously by EU law. For the last two elements, damage and causality, the Directive relies on national law to a great extent. This is especially the case for the element of causality, which is only dealt with very minimally in the Directive. Also the concept of damage is left to be interpreted by national law to a great extent, as the Directive only indicates two heads of damage that it covers. National rules on causality and damages apply where the Directive does not provide guidance.

In the next three chapters, we will more closely examine three elements: product, defectiveness and damage. The remaining two elements (producer and causality) will be discussed less elaborately in the sections below. This approach is chosen for the following reasons. The concept of producer is defined very broadly, so that there is no interpretative difficulty when applying it to manufacturers of smart home devices. The causality element is left to the laws of the Member States to such a degree that an elaborate discussion on the European level is not possible. Despite the fact that the same difficulties arise with the concept of damages, this element is discussed more elaborately in chapter 7. The reason for this is that the available remedies under the Directive is one of the main points of focus of this research.

4.3 Producer

The producer is the liable person under the Directive. Article 1 states that “the producer shall be liable for damage caused by a defect in his product.” The definition of producer can be found in Article 3 of the Directive. It has been confirmed by the Court of Justice of the European Union (CJEU) that this Article exhaustively regulates the class of liable persons under the Directive, meaning that it determines not only liability but also which of the operators who have taken part in the production and marketing processes will have to assume this liability for a defective product.[216] In other words, the system of the Directive does not apply to actors that are not defined by the Directive.[217]

[212] Article 1 and 6 Product Liability Directive. See: Chapter 6.

[213] Article 1 and 9 Product Liability Directive. See: Chapter 7.

[214] Article 1 and 4 Product Liability Directive. See: Chapter 4.4.

[215] See: Chapter 1.3.1.

[216] Case C-402/03 *Skov v Bilka* [2006] ECR I-199, para 30; Case C-495/10 *Centre hospitalier universitaire de Besançon v Thomas Dutreux and Causse primaire d’assurance maladie du Jura* [2011] ECR I-14155, para 26.

[217] Dimitri Verhoeven, ‘Productveiligheid en productaansprakelijkheid’ (PhD dissertation, University of Antwerp 2016) 50.

Article 3 includes all producers that are involved in the production process (provided the end-result meets the definition of a "product" in the Directive).[218] This broad definition fits the consumer protection aim of the Directive; the legislators intended to ensure that a victim of a defective product will always find a liable person.[219] It is first and foremost the manufacturer of a finished product that is held liable in Article 3(1) of the Directive.[220] Also liable are producers of raw material or component parts of a finished product where these elements are the cause of the defect.[221] Article 3 exhaustively lists other persons that can be held liable under the Directive.[222] Also liable is any person who presents himself as the producer of the product, by putting his name, trademark or other distinguishing feature on the product.[223] Furthermore, in case of imported goods, the Directive holds the importer of the product liable.[224] As a last resort, only in case there is no (easily) identifiable manufacturer or importer, the injured person can turn to the supplier of the product.[225] The supplier will only be liable in case he does not provide the identity of the producer, importer or any other person who supplied him the product.

With regard to smart home devices, it is thus primarily the manufacturer of the finished product that is liable for damage caused by a defect in the product. This is the company that manufactures and circulates the product on the market. For example, home automation producer Nest Labs fits this definition. Also liable are manufacturers of component parts and raw materials. For example, IBM would be liable for damage caused by defective chips that are used in smart devices. Sometimes it is less clear which role a company takes in the production process, but chances are that they are still covered by the broad definition of Article 3. For example, Nuki Home Solutions GmbH provides smart locks in Europe. They describe themselves as a supplier of smart locks,[226] but they affix their tradename and trademark to the product. Article 3 therefore captures them as a producer, namely as a person who presents itself as the producer of a product.

From a consumer protection perspective, the broad class of liable persons argues in favour of applying product liability rules to smart home devices. The injured person will practically always find a potentially liable person for a defective product within the meaning of the Directive. Another benefit is that the injured person can address the manufacturer of the finished product for *any* defect in the product, regardless of whether it produced the component that caused the defect or not. Considering the fact that

[218] Recital 4 Product Liability Directive ("*protection of the consumers requires that all producers involved in the production process should be made liable*").
[219] Fairgrieve et al (n 189) 61.
[220] Case C-127/04 *Declan O'Byrne v Sanofi Pasteur MSD Ltd and Sanofi Pasteur SA* [2006] ECR I-01313, para 36.
[221] Article 3(1) Product Liability Directive.
[222] *Declan O'Byrne* (n 220) para 37.
[223] Article 3(1) Product Liability Directive.
[224] Ibid.
[225] Article 3(2) Product Liability Directive.
[226] Nuki Home Solutions GmbH, 'About Us' (*LinkedIn*) <https://www.linkedin.com/company/nuki-home-solutions-gmbh> accessed 27 February 2018.

smart home devices are made up of various hardware and software component, some most likely produced by third parties, it is advantageous for the injured person that it is not necessary to figure out who exactly was responsible for the defect. In case there is more than one producer that is liable, an injured person may claim full compensation from any one of them.[227] This is another advantage for the consumer, as it is not required to sue several parties for a proportion of the damage. Also, the injured person can turn to the liable person that is in the best economic position to pay compensation.[228] The joint liability rule expressed in Article 5 of the Directive does not prejudice national rules relating to the rights of contribution or recourse between the liable producers.

There are limits to the broad class of liable persons defined in Article 3. Because Article 3 exhaustively regulates the liable persons, other actors cannot be held liable under the Directive.[229] Interesting exclusions in the context of smart home devices are the original designer of a product and service providers. The exclusions have effect only where these persons do not also act as producers within the meaning of the Directive.[230] We will consider both in more detail.

First, the original designer of a product. This actor is excluded from the definition of producer because he is traditionally not involved in the production process.[231] Thus, where this person does not also fall within the definition of Article 3 of the Directive, he is insulated from liability. This rationale only partially fits with the production processes of smart home devices. An important distinction in this context is the distinction between the hardware and software components of smart home devices. The just described rationale fits with the former, as hardware components, e.g. the physical shape of the device, generally follow a linear production process whereby the design and manufacturing phase follow each other. Where the original designer is not involved in the manufacturing process also, he is not liable under the Directive. Instead, liability is channelled to the producer as defined under the Directive.[232]

The rationale makes less sense in the context of the software components, because software follows a different production process. Modern software production is an ongoing process whereby changes (updates) are made throughout the lifecycle of the software. The end-result is a dynamic rather than a static product. Software is never truly finished, but in a "perpetual beta" phase.[233] The term agile

[227] Article 5 Product Liability Directive; Recital 5 Product Liability Directive.

[228] Fairgrieve et al (n 189) 72.

[229] *Skov v Bilka* (n 216) para 30; *Centre hospitalier universitaire de Besançon* (n 213) para 26.

[230] Fairgrieve et al (n 189) 71.

[231] Geraint Howells et al., 'Product Liability and Digital Products' in Tatiani-Eleni Synodinou et al. (eds) *EU Internet Law* (Springer International Publishing AG 2017) 184.

[232] Ibid.

[233] Tim O'Reilly, 'Design Patterns and Business Models for the Next Generation of Software (*O'Reilly*, 30 September 2005) < http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=4> accessed 27 February 2018.

software development indicates this iterative and incremental software production process.[234] Because most software is today produced in this manner, the production of software components in smart home devices is comparable to constantly developing a design further whilst it is already in the hands of the customer. In the words of Howells et al.: writing a software programme "blurs the line between design and final product".[235] Therefore, excluding a designer of software (a software developer) from the class of liable persons makes little sense. To solve this issue, it is recommended to hold the software developer liable as the manufacturer of the (component part of the) product.[236]

The second exclusion is that of service providers. This has a double implication. First, because product liability only covers goods and not services,[237] the Directive does not create liability for defective services. We will more fully elaborate these issues in chapter 5 on the product definition, where we will discuss the increasingly problematic distinction between goods and services in digital products like smart home devices. Second, providers of services are not liable under the Directive for defective products that they use in the context of providing this service except where they are also the producer of these defective products.[238]

The exclusion for liability of service providers for the products they use in the context of their service was made clear by the CJEU in a case concerning a defect heating mattress in a hospital that caused burns to the patient's body during surgery.[239] The hospital was not liable for the defective product they used, because they did not fall within the class of liable persons established by Article 3 of the Directive. They were not involved in the production process of the mattress and therefore not a producer.[240] They were also not a supplier of the product, because it could not be said that they intended to supply the patient with a product for his use.[241]

A return to the main rule occurs in the circumstance that the service provider is also the producer of the product. This was the case in *Henning Veedfald*, where a donated kidney was used with a defective fluid which made it unusable for transplant.[242] Because the defective fluid was made by the hospital that

[234] Seda Gürses and Joris van Hoboken, 'Privacy After the Agile Turn' in Evan Selinger (eds), *Cambridge Handbook of Consumer Privacy* (Cambridge University Press, 2017) <https://osf.io/ufdvb/> accessed 14 October 2017 (Draft Version 2).
[235] Howells et al. (n 231) 184.
[236] This conclusion depends on the question of whether software is a product or a component part of a product within the meaning of the Directive. For this, see: Chapter 5.
[237] Article 2 Product Liability Directive.
[238] Case C-203/99 *Henning Veedfald* [2001] ECR I-03569; *Centre hospitalier universitaire de Besançon* (n 213).
[239] Case C-495/10 *Centre hospitalier universitaire de Besançon* (n 216).
[240] Ibid, para 26-27.
[241] Ibid, para 28.
[242] *Henning Veedfald* (n 238).

used it in the course of the procedure, they were a producer also. The question of whether a service provider is liable for defective products of which it is not the producer was thus not raised in this case.[243]

4.4 Causality

Another element to a product liability claim under the Directive is causality. According to Article 4 of the Directive, "[t]he injured person shall be required to prove the damage, the defect and the causal relationship between defect and damage." It is thus the person injured by a cybersecurity vulnerability in a smart home device that needs to prove the causal relationship between the security vulnerability and the damage (which he also needs to prove). Furthermore, Article 8 of the Directive provides a rule for two instances of multiple causation.[244] The Directive does not give any further guidance on causality. One needs to look at the national laws of the Member States in order to know what the causal link should consist in, when there is a presumption of causality, etc.

According to Fairgrieve et al, the piecemeal regulation of causality in the Directive is a significant restriction on the harmonisation that it pursues.[245] At the same time, they recognise that causality is a fundamental concept of tort law which is embedded in traditions of national law and that should not lightly be interfered with.[246] Dommering-van Rongen also concludes that there is no reason to adopt European rules on causality in this context, because it is generally undesirable that a national legal system has to deal with various systems of liability.[247] For the reason that in this thesis a European perspective is adopted (focusing on the text of the Directive rather than its implementations in national law)[248] we will not further explore the topic of causality.

4.5 Chapter conclusion

This chapter has introduced European product liability law, more specifically the Product Liability Directive. Information was given on the background and purpose of the Directive. Any injured person can claim under the Directive, but the practical use of the Directive is limited to consumers (in the economic sense of the word, i.e. not requiring a contractual relationship with the defendant). A claim for product liability consists of five elements: product, producer, defect, damage and causal link. This chapter covered two of the elements: producer and causality.

The broad definition of producer in Article 3 of the Directive argues in favour of applying the Directive to smart home devices, because an injured person will practically always find a liable person. The exclusion of the original designer from the scope of liable persons makes less sense in the context of

[243] *Centre hospitalier universitaire de Besançon* (n 216) para 37.
[244] See further: Chapter 7.1.
[245] Fairgrieve et al. (n 189) 86.
[246] Ibid
[247] Dommering-van Rongen (n 190) 154.
[248] See: Chapter 1.3.1.

agile software production, where design and production are an ongoing process and products are in a "perpetual beta" phase. Therefore, it is recommended to hold software developers liable as manufacturers of (a component part of) the product within the meaning of the Directive. Service providers are also excluded from the scope of the Directive, which will be considered more elaborately in the next chapter.

The Directive leaves the element of causality to be regulated primarily by the national laws of the Member States. Because of the European focus that this thesis has adopted, this element is not further explored. The next chapter three chapters will discuss the remaining three elements in more detail, starting with the product definition.

Chapter 5: Product analysis of smart home devices

In this chapter, we will consider whether smart home devices can be considered to be products within the meaning of the Product Liability Directive (Directive). The definition of a product can be found in Article 2 of the Directive. According to this definition, products are “all movables [...] even though incorporated into another movable or into an immovable [...]”. The following three criteria can be deduced from this: products are (1) movable and (2) tangible (3) goods. In the following paragraphs, we will consider the three requirements in more detail.

Before we start, it is important to draw attention to the distinction between the hardware and software components in smart home devices. As we will see throughout the product analysis, the interpretative difficulties lie with the software components. It is important to know whether the product definition includes software, because cybersecurity vulnerabilities often present themselves in the software components of a smart home device.

5.1 Only movables

The first requirement is that the Directive only applies to movable goods, thereby excluding immovable goods. A movable incorporated into an immovable also falls within the scope of the rules. For example: a house does not fall within the scope of the product liability rules as it is an immovable, but the bricks used to build the house are products even after they have been incorporated in the house.[249] By analogy, we can easily conclude that smart home devices satisfy this element of the definition. First, many smart home devices are not incorporated into the house itself, e.g. a smart baby monitor. Second, even if they are incorporated into the house, arguably a smart thermostat or a smart lock, they will remain subject to the product liability rules as movables incorporated into an immovable. A relevant indicator is that they are movable goods at the moment of sale.[250]

5.2 Tangible goods

The second limitation is that the Directive only applies to tangible goods. This limitation has been and remains the subject of debate in the context of software. We will first consider the origin of the tangibility requirement. Following this, we will discuss its implications for the hardware and the software components in smart home devices. Some of these difficulties also relate to the distinction between goods and services, which is the topic of discussion in section 5.3.

[249] Duncan Fairgrieve et al. ‘Product Liability Directive’ in Piotr Machnikowski (ed), *European Product Liability, an Analysis in the State of the Art in the Era of New Technologies* (Cambridge, Intersentia 2016) 41.
[250] Dimitri Verhoeven, ‘Productveiligheid en productaansprakelijkheid’ (PhD dissertation, University of Antwerp 2016) 36-37.

The requirement of intangibility is not expressly stated in the directive, but is derived *a contrario* from the express statement that electricity is included in the product definition.[251] As electricity is intangible, the reasoning goes, it follows that other intangible goods are excluded. Otherwise why include electricity in the definition to begin with? Council statements show that the legislative intention was to include defects that are due to a failure in the production process of electricity.[252] Because the status of electricity was divided in the Member States, it was explicitly mentioned to achieve the desired level of harmonisation.[253] According to some authors, the inclusion of other types of intangible products therefore requires legislative intervention.[254] At the same time, the interpretation and the existence of the tangibility requirement have been criticised also.[255]

The tangibility requirement is not problematic for the hardware components of a smart home devices. Hardware components are clearly tangible: the materials that make up a smart thermostat, smart lock or smart baby monitor. Not only the material form or shell, but also other physical components in these devices are covered. This includes chips, processors etc. In the event that hardware elements cause harm, product liability rules will apply as they do in traditional “offline” product liability scenarios. For example, where a baby monitor has sharp edges that can cause physical injury or where a processor heats and causes the device to explode.

By contrast, the tangibility requirement causes various interpretative difficulties for the software components of a smart home device and for software in general. This is not a new discussion. Around the time that the Directive was implemented in the national laws of the Member States, there was disagreement amongst scholars on whether software was included in the product definition. Opponents argued that software was intangible because it was mere information; a series of instructions to be performed on a computer.[256] In response to this, it was argued that the tangibility requirement did not exist. Other proponents argued that software is tangible as it is practically always stored on a physical carrier. We will consider both responses in more detail.

[251] Fairgrieve et al. (n 249) 41; Daily Wuyts, ‘The Product Liability Directive – More than Two Decades of Defective Products in Europe’ (2014) 5 *Journal of European Tort Law* 1, 4-5.

[252] Louise Dommering-van Rongen, *Productaansprakelijkheid: Een rechtsvergelijkend overzicht* (Deventer, Kluwer 2000) 123.

[253] Kees Stuurman en Guy P.V. Vandenberghe, ‘Softwarefouten: een ‘zaak’ van leven of dood?’ (1988) 24(45/46) *Nederlands Juristenblad* 1667, 1670-1671.

[254] Clarisse Girot, *User protection in IT contracts: a comparative study of the protection of the user against defective performance in information technology* (The Hague, Kluwer Law International 2001) 330, footnote 88.

[255] Stuurman and Vandenberghe (n 253) 1671; Piotr Machnikowski, ‘Conclusions’ in Piotr Machnikowski (ed), *European Product Liability, an Analysis in the State of the Art in the Era of New Technologies* (Cambridge, Intersentia 2016) 700-701.

[256] J.J. Borking, ‘Risico’s voortvloeiend uit produktaansprakelijkheid voor programmatuurmakers’ [1987] Informatie 928-935.

In an article dating from 1988, Stuurman and Vandenberghe argue that the European legislator did not intend to exclude all intangibles by expressly including electricity in the scope.[257] The intention underlying the inclusion was very specific: including defects that are due to a failure in the production process of electricity. The fact that the legislator did not include other disputed subject matter does not automatically mean it is excluded. Moreover, based on an analysis of the translations of the Directive and the implementations of the Member States, it is not clear whether a tangibility requirement exists. They conclude that, in absence of guidance from the CJEU, the purposes of the Directive are leading. On the basis of the consumer protection aim of the Directive, which they deem to be important or the most important, they conclude that software should be included.[258] However, despite the criticism of Stuurman and Vandenberghe, the tangibility requirement has survived the test of time and is still included as a requirement in recent scholarly work on the Directive.[259]

Another argument for treating software as a product under the Directive was not to attack the requirement itself, but to argue that software is in fact a tangible good. In an article dating from 1988, Dommering-van Rongen states: "[i]n my opinion software is a tangible good. Software is fixed on a [physical] carrier almost without exception."[260] This is most likely also the argument that the European Commission had in mind in its 1989 response to the question of a member of the European Parliament whether "computer software" was covered by the Directive, to which it answered that the Directive applied to software "in the same way […] that it applies to handicraft and artistic products".[261] In accordance with this, in older literature one can find the general statement that "software" is a product under the Directive.[262]

It is important to place this answer of the European Commission in a historical perspective. Around that time, Personal Computers (PCs) were the dominant form of computing.[263] Consumers bought a mainframe PC which was "all hardware, no software" and separately bought software programs that were supplied on a physical carrier like a CD-ROM or floppy disk.[264] This type of software is called "shrink-wrap software". The consumer would install the software on his or her PC and new versions were

[257] Stuurman and Vandenberghe (n 253) 1670-1671.
[258] Ibid, 1672.
[259] See e.g. Wuyts (n 251) 4-5; Verhoeven (n 250) 38; Fairgrieve et al. (n 249) 41.
[260] Louise Dommering-van Rongen, 'Produktenaansprakelijkheid en software' (1988) 5 *Computerrecht* 227, 228 (own translation).
[261] Written Question No 706/88 by Gijs de Vries to the Commission: Product liability for computer programs, Official Journal (OJ) C 114/42.
[262] Dommering-van Rongen, *Productaansprakelijkheid: Een rechtsvergelijkend overzicht* (n 252) 126; Dommering-van Rongen, 'Produktenaansprakelijkheid en software' (n 261) 228.
[263] See on this topic: Jonathan L Zittrain, *Future of the Internet and How to Stop it* (New Haven and London, Yale University Press 2008) 11-18.
[264] Ibid, 13.

released every now and then. Because of the fact that practically all software was supplied on a physical carrier, it is easy to see how the tangibility requirement was satisfied.

Since that time, the ways in which software is supplied and produced have changed significantly. This is reflected in more recent literature on the product definition, where scholars make a distinction between software that is provided on a physical carrier and software that is supplied without such a physical dimension, i.e. where it is downloaded or otherwise accessed online.[265] In relation to the former, there is a general consensus that the software is a product within the meaning of the Directive. This finding corresponds with the conclusion from the older debate and is based on the physical carrier reasoning. In relation to the latter, it is often said that online downloads are intangible and therefore cannot fall within the product definition.[266] Applying this to software components in smart home devices, we are presented with a scattered legal field.

First, let us consider software stored on a physical carrier. This traditionally includes the situation that a software program is stored on a separate carrier like a CD-ROM, floppy disk or a USB stick.[267] It is immediately clear that this is not the means by which software in smart home devices is supplied. It is furthermore recognised that the physical carrier reasoning can be extended to the situation that software is directly incorporated into a tangible good to such an extent that it becomes a part of the good. [268] In this context, Verhoeven mentions two criteria: (1) the software must be necessary for the full or partial functioning of the good; and (2) the software must be an indistinguishable element of the good.[269] As an example he names software that is necessary for aircraft control.[270]

To which extent is software incorporated in a smart home device? This reasoning is at least also convincing for some software components in such a device. To start, it fits with the firmware of a smart home device, which is the semi-permanent software that is critical for the functioning of the device and other software components on it. Without such software the device would not function (criterion 1) and the software is not separable from the device but is one of its fundamentals; it cannot be removed at will like a computer game can be removed from a PC (criterion 2). Presumably this is the rationale that Leverett et al. have in mind when they state that firmware in a IoT device is very likely covered by the Directive.[271] This reasoning can also be applied to other software that is installed on the device at the moment of sale, but the matter is complicated by the issue of updates.

[265] Fairgrieve et al. (n 249) 41; Wuyts (n 251) 5.

[266] Verhoeven (n 250) 46-47; Fairgrieve et al. (n 249) 46.

[267] Ibid.

[268] Verhoeven (n 250) 46.

[269] Ibid.

[270] Ibid.

[271] Éireann Leverett, Richard Clayton and Ross Anderson, 'Standardisation and Certification of the 'Internet of Things' (WEISS Conference, 2017) 9 <http://www.cl.cam.ac.uk/~rja14/Papers/weis2017.pdf> accessed 15 December 2018.

This brings us to the second category that we identified above: software that is supplied without any physical dimension, e.g. online downloads. According to current literature, this is where the limit of the tangibility requirement is reached.[272] Software that is supplied without a physical carrier is generally considered to be intangible by nature, and as such cannot be within the scope of the definition. This outcome is problematic for software in general, as more and more software is supplied online as a download rather than on a CD-ROM in a store. Moreover, increasingly software is not even fully downloaded on the user's device but stored on a remote server which is accessible via a thin user client on the device.[273]

The distinction between software supplied on a physical carrier and software supplied otherwise leads to inconsistencies and undesirable outcomes. For example, if one were to buy Microsoft Word on a CD-ROM in a store, the software would fall within the product definition, but if it were downloaded online and stored on the computer or otherwise accessed online via a user client, it would not. For this reason, reliance on a physical carrier has been called "not very rational"[274] and "outdated".[275] This is already recognised at the European level in the proposal for a directive on digital content, which defines digital content independently of the medium used for transmission.[276] As such, the directive applies regardless of whether the digital content is supplied on a durable medium, as a download or otherwise accessible online. According to recital 11 of the proposal, this approach is taken to make the definition future-proof and to prevent arbitrary discriminations between different suppliers in a technologically fast changing market.

Not only is software currently often available as download or otherwise accessible online, it is also in a state of constant flux. Unlike shrink-wrap software, which is a finished and static software programme and whereby new versions are released on a new CD-ROM, updates that change the software in terms of both functionality and security are downloaded and installed throughout the lifecycle of the device. Updates are downloaded online after the moment of sale and therefore provided in a non-physical manner; intangible. Upon installation, they make alterations to the software that was previously installed

[272] Verhoeven (n 250) 46-47; Fairgrieve et al. (n 249) 46.

[273] This is generally known as Software as a Service (SaaS) and touches on the goods and services distinction that will be discussed in Chapter 5.3.

[274] Wuyts (n 151) 6.

[275] Geraint Howells et al., 'Product Liability and Digital Products' in Tatiani-Eleni Synodinou et al. (eds) *EU Internet Law* (Springer International Publishing AG 2017) 190.

[276] Article 2 proposal for a directive on digital content. See also: Explanatory Memorandum page 11 *("[Some] definitions reflect the specificity of digital content and reflect the rapid technological and commercial evolution. For example, the definition of digital content is deliberately broad and encompasses all types of digital content, including for example, downloaded or web streamed movies, cloud storage, social media or visual modelling files for 3D printing, in order to be future-proof and to avoid distortions of competition and to create a level playing field.*").

on the device. In this sense, software is a "moving target".[277] These developments indicate a transformation from so-called waterfall to agile software production processes.[278]

What does this mean for the status of software as a product in the Directive? More specifically, what does it mean for the software components in smart devices? A smart device is delivered with firm/software on it. As explained earlier, it can be said to be incorporated into the tangible good so that it falls within the definition of a product in the Directive. What is the effect of updates? These are supplied without a physical dimension and as such are intangible. Do updates have the effect of excluding the software components from the scope of the Directive that were initially considered tangible due to the incorporation in a tangible good at the moment of sale? Or conversely, do updates become part of the incorporated software in the device as soon as they are installed, meaning the software components are covered by the product definition?

It is not clear how one should answer these questions. The discussed legal literature does not include the agile software production process and the issue of updates in their discussion of the tangibility requirement. There is also little attention for normative aspects of the analysis, i.e. whether it is desirable to include software in the product definition.[279] Often, the argument is advanced that strict liability is inappropriate for a product that will never be without flaws, i.e. 100% bug-free, so that it is inappropriate to make the manufacturers strictly liable.[280] Mostly, however, legal scholars focus on a grammatical interpretation of the product definition in the Directive. When one does take into account modern software production processes, the strain caused by the definitional limitation that products must be tangible is evident. To solve the tangibility issue, some arguments can be forwarded.

First, we can extend the physical carrier reasoning to include updates and/or updated software. For this we should again consider the two criteria for incorporation of software in a tangible good. First, the software is necessary for the full or partial functioning of the good. Second, the software forms an indistinguishable part of the tangible good. With regard to the first criterion, it is clear that software is necessary for the functioning of the good in its smart capacity or at all. A secure update mechanism and updates play an important role in this. Second, a secure update mechanism and the downloading and installation of updates form an essential part of the software. Moreover, the software remains an indistinguishable part of the device even when updated. The software cannot be removed at will, but is

[277] Leverett, Clayton and Anderson (n 271) 12.

[278] Seda Gürses and Joris van Hoboken, 'Privacy After the Agile Turn' in Evan Selinger (eds), *Cambridge Handbook of Consumer Privacy* (Cambridge University Press, 2017) 5 <https://osf.io/ufdvb/> accessed 14 October 2017 (Draft Version 2).

[279] To an extent, this question is covered by the defectiveness analysis (see Chapter 6) as this introduces elements of fault based liability.

[280] See e.g. Scott L. Wenzel, 'Not Even Remotely Liable: Smart Car Hacking Liability' (2017) University of Illinois Journal of Law, Technology and Policy 49.

merely altered by the updates. Neither of the two criteria require that the software remains static and unchanged throughout its lifetime. As updates become a part of the incorporated software in the device, we can say that the software components in a smart home device satisfy the tangibility requirement. In a similar vein, it has been suggested that the physical manifestation of the software on the host mainframe after it has been downloaded can be considered to be a product.[281] Also the parts of the software which are not present on the device itself but stored "in the cloud" ultimately also reside on a tangible server.

Second, some scholars simply call for change. Recently, Machnikowski has called the distinction between software supplied in a physical carrier and software supplied in a non-physical manner arbitrary.[282] More generally, he attacks the existence of the tangibility requirement overall. Not unlike Stuurman and Vandenberghe concluded in 1988, he argues that there is no convincing reason for limiting products to tangible goods only.[283] He therefore calls for a determination by either legislative intervention or by the CJEU that data, like software and digital contents, can be products within the meaning of the Directive.[284] His view has the support of the European Consumer Organisation in their response to the European Commission's evaluation of the product liability rules.[285] The determination that "data" can be a product within the meaning of the Directive will however have wider implications than bringing software into the scope of the Directive and therefore should be approached with caution. Instead, it is recommended to abandon the physical carrier reasoning in favour of a product definition that defines software as products independently of their means of transmission. For this, inspiration can be drawn from the proposal for a directive on digital content.[286]

Third and last, an alternative approach would be to circumvent the tangibility requirement. Theoretically, it is possible to regard the software as a component part of a product. According to Article 3 of the Directive, a producer of a component part is liable for defects caused by its product. The term "component part" is however not defined in the Directive. This means that it is not required that a component part is tangible. This lacuna opens up the possibility of applying product liability rules to an intangible component part of a product, e.g. software updates or software components in general. On the one hand this seems plausible, because the role that software plays in a smart home device is not significantly different from the role that material components play in a traditional product.[287] On the other

[281] Wuyts (n 251) 6.
[282] Machnikowski, 'Conclusions' (n 255) 700-701.
[283] Ibid, 701.
[284] Ibid.
[285] Christoph Schmon, *Review of the Product Liability Rules, BEUC Position Paper* (The European Consumer Organisation 2017), 3.
[286] Article 2 and Recital 11 proposal for a directive on digital content,
[287] Machnikowski, 'Conclusions' (n 255) 701.

hand, this approach creates legal inconsistency without the simultaneous recognition of intangible goods as products.[288]

More specifically, this approach has the effect that a producer of software would not be subject to product liability rules, except where the software is a component part of a product. There is no liability for the product, but only for the component part. This is unlikely to have been the intended result of the legislators. More likely is that the problem of intangibles like software and digital content being components of physical products was not foreseen back in 1985.[289] With products of technology nowadays often being based on data that originates from other people than the manufacturer of the product, it has been recognised in literature that the understanding of the term "component part" becomes more important to clarify.[290] In the meantime, in practice it is theoretically be possible and perhaps desirable to hold the producer of the component liable despite these systematic inconsistencies.

5.3 Goods, not services

The third limitation of the product definition is that it covers goods only, not services. This exclusion can be approached in two ways. First, Article 3 does not include service providers in the scope of liable persons.[291] Therefore, liability for the provision of services as such is excluded from the scope of the Directive.[292] Also, service providers are not liable for defective products that they use in the provision of their service under the Directive except where they also produced the product.[293] Second, services do not fall within the product definition of Article 2 of the Directive. An argument advanced in this context is that services are intangible and as such excluded from the scope. Moreover, from the traditional dichotomy between goods and services it follows that it is a *contradictio in terminis* to include a service under the definition of a product where this is defined as a good.

Whilst not an issue for hardware components of a smart device (clearly goods), the exclusion of services from the scope of the Directive is problematic for the software components in a smart device. This has been observed by various legal scholars, some with more attention for the technical workings of software than others. We will first consider the more general observations before we turn to a more technical discussion of why software is increasingly seen as a service rather than a good.

[288] Ibid.
[289] Ibid.
[290] Ibid.
[291] See also: Chapter 4.3.
[292] Verhoeven (n 250) 40.
[293] Case C-495/10 *Centre hospitalier universitaire de Besançon v Thomas Dutreux and Causse primaire d'assurance maladie du Jura* [2011] ECR I-14155; Case C-203/99 *Henning Veedfald* [2001] ECR I-03569.

In general, scholars are recognising a so-called "servitisation" of products; a term used to indicate that products are combined with services and vice versa.[294] Put differently, it is becoming more commonplace to combine elements of product sales and service provision into one business relationship.[295] Writing specifically on the implications of the Internet of Things for consumer law, Helberger observes that the very way in which consumers buy and use products is revolutionised – including the relationship between consumers and traders – due to complementary services that are combined with such a good.[296] With the purchase of e.g. a smart watch, a consumer does not only acquire a watch, but also an entire "service universe" relating to this watch.[297] Many of these services are made possible through the collection of data by the smart device, which enables the provision of highly individualised services and products.[298] For example, the provision of health advice based on how many steps are taken and how many calories are burned.

All this has a profound effect on the relationship between the consumer and the trader.[299] Where this relationship was traditionally limited to the moment of sale and a possible repair or replacement when a defect occurred, it now potentially becomes a continuous, dynamic and personal relationship throughout the lifecycle of the product. According to Kokx, Director of Product Security at Philips, this requires a change of mentality on the side of manufacturers. What was once a 'design-manufacture-forget' attitude now has to evolve into a mind-set in which there is continuous review of the product, including product security.[300] From a legal perspective, it is relevant to classify the role that the device manufacturer takes in this context and the responsibility that he has. Further adding to the complexity is that it is likely that the consumer is drawn into relationships with various third party service providers that are involved in the smart device service universe. Therefore, Helberger notes, smart devices need to be assessed not so much as things but as "platforms for value added services".[301] In this context, Machnikowski notes that the effectiveness of attributing liability to the product manufacturer needs to be reconsidered.[302]

[294] Janja Hojnik, 'Technology Neutral EU law: digital goods within the traditional goods/services distinction' (2017) 25 International Journal of Law and Information Technology 63, 66.

[295] Piotr Machnikowski, 'Introduction' in Piotr Machnikowski (ed), *European Product Liability, an Analysis in the State of the Art in the Era of New Technologies* (Cambridge, Intersentia 2016) 10.

[296] Natali Helberger, 'Profiling and Targeting Consumers in the Internet of Thigns - A New Challenge for Consumer Law' in Reiner Schulze and Dirk Staudemeyer (eds) *Digital Revolution: Challenges for Contract Law in Practice*' (Hart Publishing 2016), 136.

[297] Ibid. See also: Jenna Lindqvist, 'New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?' (2017) 25 International Journal of Law and Information Technology 1, 5-6 ("*When consumers buy smart home devices, they do not just buy the object, but also by implication they acquire many services and data from multiple stakeholders.*")

[298] Helberger (n 297) 137-138.

[299] Ibid, 136.

[300] Ben Kokx, 'De cybersecurity uitdaging' (2017) 3 Tijdschrift voor Compliance 171.

[301] Helberger (n 297) 141.

[302] Machnikowski, 'Introduction' (n 296) 10.

Approaching the topic from a more technical perspective, Gürses and Van Hoboken discuss three paradigmatic transformations in the production of software (digital functionality) that they call "the agile turn".[303] We have already touched upon some aspects in the previous parts of this analysis.[304] The first transformation is the move from waterfall to agile software production processes, meaning that software development continues until after deployment. In other words, software is in "perpetual beta" and is updated throughout its lifecycle. The second transformation is the move from shrink-wrap software to a service-oriented architecture model (SOA). This means that software is no longer supplied on a tangible carrier like a CD-rom (so-called shrink-wrap software), but supplied electronically via an user interface that connects to a remote server which runs most of the software. The third is the move from the PC to cloud computing, which indicates a relocation of computing resources on remotely located servers instead of on the physical consumer device. The developments in cloud computing make the increasing reliance on SOA's possible, realizing *inter alia* Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platforms as a Service (PaaS).

According to Gürses and van Hoboken, one of the consequences of these changes in the production process of software is the increasing modularity of digital functionality.[305] This means that software products are made up of various independent service components that are offered by a host of service providers. Examples include user analytics, advertisement, authentication and payment. Thus, a website, application or software program incorporates other software components provided by third party service providers. As a result, these service providers have the ability to collect and pool end-user data across the applications that use them.[306] Another result is that the end-user is pulled in a host of relationships with the various service providers, as also observed by Helberger, which may not at all be clear from their perspective.[307] Furthermore, the responsibility for privacy in this complex network of service blocks is obscure.[308] In the same vein, we can see how responsibility for cybersecurity in this context is obscure also.

For the applicability of the Directive to software components in a smart home device, these transformations in the production of software have a profound effect. If software components can no longer be seen as goods, but have to be characterised as services, this has the effect of excluding software from the scope of the Directive. In response, Leverett at al. have made the recommendation to extend the applicability of the Directive to encompass services and hybrid systems that are a mix of products and

[303] Gürses and Van Hoboken (n 279) 5-9.
[304] See: Chapter 4.3 and Chapter 5.2.
[305] Gürses and Van Hoboken (n 279) 10.
[306] Ibid, 13.
[307] Ibid, 14.
[308] Ibid, 15-16.

services.[309] In a recent study for the European Commission on the future of product safety regulation, they write "[a]s we move to a world in which physical devices routinely interact with online services, this needs to be tackled, or vendors will just put safety-critical functionality in the cloud to escape liability."[310] The inclusion of liability for services in the Directive would have the effect of harmonising a field of law that has so far been left to the national laws of the Member States, save in some specific cases (e.g. the package travel directive). Although the European Commission introduced a Directive concerning liability of service providers in 1990, it was never adopted, leaving service provider liability to be regulated by the national laws of the Member States.[311]

Relevant in this context are the difficulties that legal scholars are having with the traditional goods/services distinction. Writing on this topic in the context of digital goods, Hojnik realises that although this distinction may seem straightforward at first sight, explicit definitions of the terms have long troubled scholars from different domains.[312] Some generally accepted attributes of goods are that they are physical objects for which ownership can be established, that exist independently of the owner, and that are exchangeable and tradable.[313] Services are more difficult to define. Since the 1980s, the IHIP-characteristics were dominant.[314] They stand for intangibility, heterogeneity, inseparability and perishability.[315] With new advances in technology, some of these characteristics have lost their distinguishing power. For example, the perishability of services and the interconnection between production and consumption are overcome by technology-based solutions, e.g. a lecture can be recorded and watched on demand at the desired moment.[316] The IHIP paradigm is as such criticised for focusing mostly on low-tech personal services (e.g. getting a haircut).[317] The lack of suitable characteristics to define services leaves the term undefined, also making it more difficult to draw the line between goods and services.

Taking into account the difficulty in defining services and distinguishing them from goods, it may not be such a radical idea of Leverett et al. to extend the scope of the Directive. At the same time, extending it to services in general might be too coarse a measure. It is not desirable to include the traditional services, i.e. personal services (like getting a haircut) in the scope of the Directive. However, for the service-like aspects of smart devices as described by Helberger this might be desirable. These are a

[309] Leverett, Clayton and Anderson (n 271) 10.
[310] Ibid.
[311] Verhoeven (n 250) 40.
[312] Hojnik (n 295) 64.
[313] Ibid.
[314] Ibid, 65.
[315] For an explanation, see: Sabine Moeller, 'Characteristics of Services – a new approach uncovers their value' (2010) 25(5) Journal of Services Marketing 359.
[316] Ibid, 359.
[317] Ibid.

different type of services, namely information services that are provided by software and algorithms. For example the smart watch which provides health advice, or a smart thermostat which provides real time information about heating in a house. These can also be considered as feature of the good rather than a service. We would not say that a calculator is providing a service by giving the answer of a calculation; it is simply the way that the good works. The technical insights on the transformations in the production of these digital functionalities given by Gürses and Hoboken however show the amalgam of parties that may be involved in this besides the device manufacturer, which very much complicates the notions of producer and product under the Directive.

5.5 Chapter conclusion

In this chapter we have considered whether we can define smart home devices as "products" under the Directive. The discussion was structured around three requirements deduced from the definition in Article 2 of the Directive: a product is a (1) movable (2) tangible (3) good. Assuming that a smart home device is a tangible good, we first concluded that they are (currently) movable goods. In the analysis of the latter two requirements we encountered various interpretative difficulties, especially in relation to the software components of a smart home device. Hardware components more closely resemble traditional products and can generally be considered as products within the meaning of the Directive.

Based on the reasoning that software is tangible when it is stored on a physical carrier, including where it is incorporated into a tangible good (provided that the software is necessary for the full or partial functioning of the good and forms an indistinguishable part of the good), we conclude that firmware and software installed on the smart home device at the moment of sale is tangible. The issue of updates complicates this conclusion, because they are downloaded after the moment of sale and supplied online. This problem can be solved by extending the physical carrier reasoning to include software updates also; they are considered as incorporated into the smart home device from the moment of installation. Another solution would be to abandon the physical carrier reasoning in favour of a product definition which defines software as products independently of their means of transmission. For this, inspiration can be drawn from the proposal for a directive on digital content. Lastly, because the Directive does not define a "component part" of a product, it is theoretically possible to keep the producer liable under the Directive.

The requirement that products are goods rather than services is increasingly problematic in the context of smart home devices. The reasons for this are twofold. First, smart devices are equipped with service-like aspects (for example, real-time information on the status of heating in the home). Second, the software in smart home devices is organised as a service rather than a good via service-oriented architecture models. This means that software is increasingly modular, i.e. complemented by offerings from other third party service providers. By taking into account these technological underpinnings of software production, i.e. how consumer software is produced today, it becomes clear that the characterisation of software as a good rather than a service is flawed. Whilst it has been recommended by other to simply extend the scope of the Directive to cover services also, this is likely to be too coarse a measure and will result in unintended side-effects. Whilst the inclusion of the service-like aspects of smart home devices in the product definition of the Directive would be a desirable development (also because these aspects can be seen as features of the tangible good rather than as a service), the developments in the production of software pose a more fundamental problem to the traditional goods/services distinction on which the Directive relies. This is an area that would merit from more legal research that takes the production of software into account.

Chapter 6: Defectiveness analysis of security vulnerabilities

In this chapter, we aim to answer the question of whether software vulnerabilities in smart home devices constitute a defect within the meaning of the Directive. Defectiveness is a central concept in the Directive: it is the criterion for determining whether a producer is liable or not. The producer is liable for a defective product, regardless of whether the defect was his fault or due to his negligence. For this reason, the Directive is said to establish a system of strict liability. At the same time, the defectiveness test introduces elements of fault-based liability by looking at the reasonable expectations that one may have about the safety of a product and whether the producer acted reasonably in light of these expectations.

The structure of this chapter is as follows. First, we will consider whether software vulnerabilities are in fact a safety problem. This is a relevant question because the Directive only covers defects related to the safety of a product. Second, we will explain the defectiveness test and types of defects and apply this to the three incident scenario's. Third and last, we will bring our attention the risk development defence and its implications for cybersecurity vulnerabilities in smart home devices.

6.1 Safety and security

First, the question of whether the problem of security vulnerabilities in a smart home device is in fact a safety problem. This is a relevant question because the Directive only covers defects that are related to the safety of a product. In this section, we will first look into the defectiveness criterion of the Directive and the role that safety plays therein. Secondly, we will consider whether cybersecurity vulnerabilities can be seen as a safety issue as covered by the Directive. It will be argued that the inclusion of cybersecurity vulnerabilities requires a transformation in thinking about product safety. In particular, traditional safety regulators must start thinking about security as well as safety.

Article 6 of the Directive reads: “a product is defective where it does not provide *the safety* which a person is entitled to expect” (emphasis added). The Directive does not give a legal definition of safety. Some more guidance can be found in recital 7 of the Directive: “[...] the defectiveness of the product should be determined by reference not to its fitness for use but to the lack of the safety which the public at large is entitled to expect.” Moreover, from recital 1 it follows that the Directive seeks to protect the consumer from damage caused by defective products to his “health or property.” The Directive is thus concerned with defects that cause harm to the health or property of consumers and not with questions of whether a product is unfit for its purpose or unmerchantable.[318] Issues of non-conformity belong to the rules concerning the sale of goods. To illustrate the difference, Fairgrieve et al. mention that a blunt

[318] Duncan Fairgrieve et al. ‘Product Liability Directive’ in Piotr Machnikowski (ed), *European Product Liability, an Analysis in the State of the Art in the Era of New Technologies* (Cambridge, Intersentia 2016) 50-51.

kitchen knife is not defective, though it is obviously not fit for its intended purpose. By contrast, when the cutting blades of an electronic kitchen knife become detached, the product is defective within the meaning of the Product Liability Directive.[319]

Product liability law traditionally deals with “offline” defects. It protects the safety and property of a person against unsafe products like the detached kitchen knife or an exploding coca cola bottle. Cybersecurity problems are new to the field of product liability. Writing on the future of product safety law, Leverett et al. therefore come to the conclusion that safety regulators must start taking security concerns into account also.[320] Society is becoming more software driven as computers and connected devices are embedded everywhere. Therefore, safety and security are merging. To achieve safety of people and products, computer security concerns must be taken into account. This will change the field of product safety regulation profoundly.[321] Currently, it is a static field of law which consists mostly of pre-market testing according to standards that slowly change. Product recall is an ultimate remedy and a rarity, and feedback from post-market surveillance is slow. By contrast, safety which takes into account computer safety is expected to become much more dynamic in nature.[322]

Helen Nissenbaum has examined this topic from another academic discipline: whether the concerns raised by technical computer security are actually security concerns.[323] She defines security as “safety, freedom from the unwanted effects of another’s actions.”[324] It is “the condition of being protected from danger, injury, attack (physical and non-physical) and other harms, and protection against threats of all kinds.” [325] This definition is in accordance with the definition of security in the Oxford English Dictionary, where security is defined as “the state or condition of being protected from or not exposed to danger; safety”.[326] The Oxford English Dictionary defines safety as “[t]he state of being protected from or guarded against hurt or injury; freedom from danger.”[327] From these definitions, it follows that an important goal of security is to provide safety. It can be seen as a means to prevent unsafe situations from happening or as a prerequisite for safety. In this sense, involving security concerns in product liability law

[319] Ibid.
[320] Éireann Leverett, Richard Clayton and Ross Anderson, ‘Standardisation and Certification of the ‘Internet of Things’ (WEISS Conference, 2017) 21-22 <http://www.cl.cam.ac.uk/~rja14/Papers/weis2017.pdf> accessed 15 December 2018.
[321] Ibid.
[322] Ibid.
[323] Helen Nissenbaum, ‘Where Computer Security Meets National Security’ *Ethics and Information Technology* 7 (2005) 64.
[324] Ibid.
[325] Ibid.
[326] Oxford English Dictionary, ‘Security’ <http://www.oed.com> accessed 5 January 2018.
[327] Oxford English Dictionary, ‘Safety’ <http://www.oed.com> accessed 5 January 2018.

places more emphasis on the preventive function of the Directive rather than the compensatory function.[328]

Nissenbaum further examines whether the activities against which security measures aim to guard warrant the label of "threat of harm."[329] She finds that the promise of technical computer security is that individuals are protected against attacks that negatively impact the confidentiality, integrity or availability of the device and its functionalities. These are safety concerns to the extent that we find that these attacks constitute *harm* to individuals.[330] In part I, we have discussed various scenario's in which a lack of technical computer security resulted in a threat of harm or actual harm for users of smart home devices. These harms ranged from personal injury to a violation of someone's fundamental right to privacy or the protection of personal data. In this sense, cybersecurity vulnerabilities in smart home devices can indeed be said to constitute safety issues.

In sum, we have considered that product liability law is traditionally concerned with offline defects, e.g. a detached kitchen knife or an exploding coca cola bottle. Extending this conception of safety to include threats and harms flowing from cybersecurity vulnerabilities, requires a transformation in thinking in the fields of product liability and also product safety law. The recommendation of Leverett et al. in this context that safety regulators must start thinking about security also as society becomes more software-driven is supported here. An analysis of what technical computer security aims to protect shows that it is in fact the safety of users that is threatened as a result of cybersecurity vulnerabilities.

6.2 Security vulnerabilities as product defects

The next question is whether security vulnerabilities constitute a defect within the meaning of the Directive. For this, we need to consider in which way defectiveness is assessed under the Directive. First, the defectiveness test will be explained. Second, we will consider the traditional classification of product defects in manufacturing, design and instruction defects. Third and lastly, we will apply the defectiveness test to the three incident scenario's. This approach is chosen because the outcome of the defectiveness analysis very much depends on the particular circumstances of the case, which makes it difficult to make any conclusive remarks about whether cybersecurity vulnerabilities constitute a defect in general. Applying the test in this way will however approximate real cases as best as possible and provide some insights on possible outcomes.

[328] Joined Cases C-503 and 504/13, *Boston Scientific Medizintechnik v. OAK Sachsen-Anhalt,* Opinion of Advocate General Bot, para 38.
[329] Nissenbaum (n 323) 64.
[330] Ibid.

6.2.1 Elements of the defectiveness analysis

Article 6(1) of the Directive reads: “a product is defective when it does not provide the safety *which a person is entitled to expect* (...)” (emphasis added). In other words, whether a product is defective must be determined on the basis of what a normal person is entitled to expect with regard to a product’s safety.[331] This is called the average consumer expectation test. It is an objective and normative test.[332] It is objective because one needs to look at the legitimate expectations of *general public* rather than the subjective expectations of a particular person. The test is normative because it looks at the *legitimate* expectations of the general public. The court may decide what the general public was allowed to expect, regardless of the actual expectations of the general public or standards promulgated by the government or industry. Taking into account these elements, the standard for defectiveness is the safety that the *general public* is *entitled to expect* from a product.[333]

To gain more insight into the defectiveness test, one can also look to the adjacent field of product safety law. According to Verhoeven,[334] the definition of defectiveness in the Directive should be interpreted in the same vein as the definition of a “safe product” in the Product Safety Directive.[335] Article 2(b) of this Directive defines a safe product as “any product which [...] does not present any risk or *only the minimum risks compatible with the product’s use* [...]”. As it is practically impossible to create a product that is completely risk-free (or software that is bug-free), the key insight is that a product is regarded as unsafe where it creates *unacceptable risks*.[336] Combining the two articles, the question in the defectiveness analysis becomes whether there is an unacceptable safety risk which an average person does not need to expect.

The focus on risk rather than harm is consistent with the preventive function of the Directive.[337] In a case before the CJEU involving medical devices implanted in patients, the Court held that *potential* defectiveness of these products was enough to render the entire series defective.[338] The injured persons

[331] Fairgrieve et al. (n 318) 51.
[332] Ibid, 52.
[333] Ibid.
[334] Dimitri Verhoeven, ‘Productveiligheid en productaansprakelijkheid’ (PhD dissertation, University of Antwerp 2016), 80 (Author’s note: Verhoeven’s reasoning is somewhat circular, concluding that defectiveness must be interpreted by looking at the safety concept and vice versa, referring to each other in infinity. My view is that on the basis of his analysis we can conclude that the two definitions influence each other, which is why I included it here).
[335] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety [2001] OJ L11/4 (Product Safety Directive).
[336] Verhoeven (n 334) 79-80.
[337] Bot (Advocate General) (n 328) para 38 (“*Making proof of a lack of safety subject to the actual occurrence of damage would disregard the preventive function assigned to EU legislation on the safety of products offered on the market and to the specific liability regime established by Directive 85/374, which manifestly pursues a preventive function by imputing liability to the person who, having created the risk most directly by manufacturing a defective product, is in the best position to minimise it and to prevent damage at the lowest cost.*”)
[338] Joined Cases C-503/13 and C-504/13 *Boston Scientific Medizintechnik* [2015] ECLI:EU:C:2015:148, para 41.

were not required to prove that the defect was present in the medical device in question.[339] This case clearly demonstrates that defectiveness must be assessed by having regard to the safety that someone can expect and whether there are any unacceptable risks, whilst it does not necessarily require proof that the defect has presented itself. In particular, where a defect has occurred in another product of the same series, the probability that it will also materialize in another product must be taken into account.

Article 6(1) of the Directive further makes clear that "*all circumstances*" should be taken into account. By making reference to all the circumstances of the case, it is said that the article introduces an element of reasonableness into the assessment of defectiveness or elements of fault liability.[340] In particular, three circumstances are given which a court can include in their assessment:[341]

a. the presentation of the product;

b. the use to which the product could reasonably be expected to be put;

c. the time when the product was put into circulation.

We will look into these three circumstances in more detail below. In general, they are merely suggestions and not mandatory elements of a defectiveness assessment nor meant as an exhaustive list.[342] Other circumstances that can be taken into account include the price of the product, the nature of the product and the severity of the danger.[343]

Because of the fact that all circumstances must be taken into account and that the list of circumstances in Article 6(1)(a)-(c) of the Directive is not exhaustive, it is also possible to include elements of other defectiveness tests. In this context, the risk-utility test is an interesting addition. This is a more objective test compared to the average consumer expectation test, because it places less emphasis on the legitimate expectation of the public with regard to the safety of the product.[344] Instead, the utility or benefits of the product are weighed against the risks of the product. If the risks outweigh the benefits, the product is deemed to be defective. Several factors are included in this assessment, like the likelihood that risks will materialize, the availability of other products, knowledge of the consumer, and the desirability of the product.[345]

Overall, the defectiveness assessment must be made on a case-by-case basis, and courts have a wide margin of appreciation in determining whether a product is defective or not in the given

[339] Ibid, para 41.
[340] Simon Whitaker, *Liability for Products* (Oxford University Press 2005) 435; Steven de Schrijver and Marlies Maes, 'Aansprakelijkheid in een ambient-intelligence omgeving: Wie heeft het gedaan?' (2010) 174 Computerrecht 3.
[341] Article 6(1)(a)-(c) Product Liability Directive.
[342] Fairgrieve et al. (n 318) 56.
[343] Verhoeven (n 334) 158, 162, 163.
[344] Ibid, 103.
[345] Ibid.

circumstances.[346] Because of this, the average consumer expectation test is quite vague and unpredictable in outcome. Yet, this approach is said to provide the necessary flexibility, meaning that it reflects how our expectancy of product safety evolves over time together with science and technology.[347] Advocate General Bot explains it as follows: "the concept of safety which a person is entitled to expect (…) is relatively imprecise and of indeterminate content [and] leaves scope for interpretation which must nevertheless be exercised having regard to the objectives of [the Directive]."[348] The flexibility provided is thus limited by the objectives of the Directive.

The figure of the hypothetical average consumer is an important benchmark in other fields of law also, including consumer contract law.[349] The average consumer is generally conceived as "reasonably well-informed and reasonably observant and circumspect."[350] The exact characteristics of the average consumer depend on the particular (product) market.[351] On the average consumer in the IoT, Helberger writes that "[a]rguably, the requirements for the average consumer in a digital environment must reflect in some way or other the greater technical and organisational complexity but also the changed nature of digital or digitally enhanced products, and hence her ability to deal with that complexity."[352] At the moment it is unclear whether the average consumer of smart home devices is a technically sophisticated and media literate consumer, or whether he or she is increasingly vulnerable and defenceless against the privacy and security implications in this complex technological landscape.[353]

In this and the following paragraphs, we will consider the three circumstances provided in Article 6(1) of the Directive in more detail and give some general remarks about their functioning in the context of cybersecurity vulnerabilities. The first circumstance is the presentation of the product.[354] The product must be assessed as a whole and in its entirety, thus including marketing, advertisements, packaging,

[346] Fairgrieve et al. (n 318) 52.
[347] Verhoeven (n 334) 81.
[348] Bot (Advocate General) (n 328) para 30.
[349] Also important in trade mark law. See e.g. Jennifer Davis, 'Locating the average consumer: his judicial origins, intellectual influences and current role in European trade mark law' (2005) 2 Intellectual Property Quarterly 183; Jennifer Davis, 'Revisiting the average consumer: an uncertain presence in European trade mark law' (2015) 1 Intellectual Property Quarterly 15.
[350] Case C-210/96 *Gut Springenheide* [1998] ECR I-4657; Recital 18 Unfair Commercial Practices Directive. See on the origins of the average consumer: Jennifer Davis, 'Locating the average consumer: his judicial origins, intellectual influences and current role in European trade mark law' (n 349) 183; Rossella Incardona and Cristina Poncibò, 'The average consumer, the unfair commercial practices directive, and the cognitive revolution' (2007) 30(1) Journal of Consumer Policy 21.
[351] E.g. a consumer in a supermarket can be seen as less attentive in comparison with a consumer buying an expensive watch or speaker set.
[352] Natali Helberger, 'Profiling and Targeting Consumers in the Internet of Things - A New Challenge for Consumer Law' in Reiner Schulze and Dirk Staudemeyer (eds) *Digital Revolution: Challenges for Contract Law in Practice*' (Hart Publishing 2016) 159.
[353] Ibid, 160.
[354] Article 6(1)(a) Product Liability Directive.

instruction, warnings etc.[355] It is generally accepted that wrong, incomplete or missing information may cause a product to be defective under the Directive.[356] Adequate information, instruction and possibly warnings are especially relevant with regard to an inherently dangerous product, including complicated high tech goods.[357] It is important that a producer of these type of products provides information about the risks related to their product and which steps consumers can take to avoid or reduce them.

If done properly, information, instruction and warnings can make an unsafe product safe, because it lowers the safety expectations that the public may have about this product.[358] If on the other hand no such information or warnings are given, this is a circumstance pointing into the direction of defectiveness.[359] In the context of smart home devices, a producer would be wise to include information about the cybersecurity risks that a product poses to the consumer and instructions about the measures someone can take to mitigate these risks, e.g. choosing a strong password.

Second, the use to which the product is reasonably put.[360] The producer needs to anticipate the expected conduct of the user, including some degree of misconduct.[361] This means that the producer cannot assume that the product will always be used in the safest way, and that this should be anticipated in the design.[362] This approach is favourable to the consumer.[363] Within the context of cybersecurity, it is known that consumers are often not capable of fully understanding the implications of the smart products that they use because of the (technical) complexity of these products and their production chain.[364] As such they are generally unfit to secure themselves against cyber threats, lacking technical knowledge, interest, or both.[365] Users are for example also unlikely to update their devices out of own accord.[366] Given these characteristics of the average consumer of smart home products, the producer of a smart home device should try to design the product in such a way that there is only the minimally necessary reliance on user activity for security matters. With regard to *un*reasonable misuse of the device, i.e. conduct which the producer need not anticipate or take into account during the design, a suggestion is to

[355] Fairgrieve et al. (n 318) 56-57.
[356] Ibid, 57.
[357] Ibid.
[358] Ibid.
[359] Cf. Article 6(1)(c) proposal for a directive on digital content (the non-conformity assessment of a contract for the supply of digital content includes the correct instruction for integration of the digital content).
[360] Article 6(1)(b) Product Liability Directive.
[361] Fairgrieve et al. (n 318) 58-59.
[362] Ibid.
[363] Fairgrieve et al. (n 318) 59.
[364] Helberger (n 352) 150.
[365] BITAG, 'Internet of Things (IoT) Security and Privacy Recommendations' (BITAG, 2016) 3 <https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf> accessed 22 November 2017.
[366] Ibid, 15.

(at least) include the scenario when a user himself modifies ("cracks") the smart home device in such a way that the provided security is affected.

Third, the time when the product was put into circulation.[367] What is meant here is that only the safety expectations at the time when the product was put into circulations may be taken into account.[368] This circumstance also resonates with Article 6(2) of the Directive, which states that a product cannot be defective "for the sole reason that a better product is subsequently put into circulation." A better product here means a safer product.[369] It also relates to the development risk defence which exempts a producer from liability where he proves that the state of scientific and technical knowledge at the time when the product was put into circulation was not such as to enable the existence of the defect to be discovered.[370] In the context of cybersecurity vulnerabilities, what a person can expect depends on the generally acknowledged good practices in technical computer security. In part I we discussed some basic security considerations about which we can say these are (increasingly) expected from smart device manufacturers, for example having a secure update mechanism.

An important realization is that this is a very static approach to product safety. It is a characteristic of current product safety law, which is focused on pre-market testing and where product recall is a rarity.[371] In product liability law, the product is seen as an unchanging object, whereby the level of safety provided at the moment of sale is the reference point. This does not reflect the dynamic nature of software components in a smart home device. As discussed elaborately in chapter 5, the production of software has changed after the so-called "agile turn". Software is updated throughout its lifecycle, changing both functionalities and (ideally) increasing security.

These technological developments create new opportunities for product safety, as a higher level of security and safety can be achieved in products that are already in the hands of consumers. Presumably, a high level of cybersecurity will be expected from manufacturers more and more. When considering whether a cybersecurity vulnerability in a smart home device constitutes a defect, these technological developments should be taken into account. In the event that a new software vulnerability is discovered for instance, it would not be reasonable for the manufacturer to hide behind the fact that this was unknown at the moment that the product was put into circulation. A better approach would be to say that at the moment that the product was put into circulation, it is known that cybersecurity vulnerabilities can occur and that best practice is to quickly provide an update patch.

[367] Article 6(1)(c) Product Liability Directive.
[368] Fairgrieve et al. (n 318) 60.
[369] Verhoeven (n 334) 156.
[370] Article 7(e) Product Liability Directive. See further: Chapter 6.4.
[371] Leverett, Clayton and Anderson (n 320) 22.

6.2.2 Types of defects

Before we apply the defectiveness test to the incident scenarios, it is helpful to first consider three generally accepted types of product defects. This is derived from the US system of product liability, which categorises product defects in three types: manufacturing, design and instruction defects. [372] In the US, there are different approaches (tests) to defectiveness for all of the categories.[373]Although European product liability law officially does not have such a tripartite categorisation of defects, in practice courts and scholars are influenced by this categorisation.[374] It is considered to be the traditional classification of product defects,[375] and as such is covered by literature on product liability in Europe also.[376] Here, it is a useful tool to translate our incident scenario's in recognised types of defects. In our discussion of the types of defects, we will include some examples related to the production of software and cybersecurity vulnerabilities.

The first type of defect, a manufacturing defect, is a technical defect. According to §2(a) of the Restatement of Torts (3th): "a product contains a manufacturing defect when the product departs from its intended design even though all possible care was exercised in the preparation and marketing of the product." It covers mistakes made during the production phase of the product, including the manufacture, assembly or the control test of the product.[377] Typically, manufacturing defects only affect one or several products in a series to deviate from the design.[378] The general approach in assessing these defects is the consumer-expectation test, as a consumer can generally expect the product to be in accordance with the design. A classic example of a manufacturing defect is the situation where small lacerations in returned bottles go unnoticed and cause the refilled bottle to explode.[379] In the context of software, some argue that the distinction between design and manufacture becomes blurred.[380] This implies that manufacturing

[372] §2 Restatement (3th) of Torts: Products Liability ("*A product is defective when, at the time of sale or distribution, it contains a manufacturing defect, is defective in design, or is defective because of inadequate instructions of warnings*").

[373] Verhoeven (n 334) 105.

[374] Fairgrieve et al. (n 318) 53.

[375] Louise Dommering-van Rongen, *Productaansprakelijkheid: Een rechtsvergelijkend overzicht* (Deventer, Kluwer 2000) 50.

[376] E.g. Louise Dommering-van Rongen, 'Produktenaansprakelijkheid: Een nieuwe Europese privaatrechtelijke regeling vergeleken met de produktenaansprakelijkheid in de Verenigde Staten' (PhD thesis, University of Utrecht 1991) 143-145; Dommering-van Rongen, *Productaansprakelijkheid: Een rechtsvergelijkend overzicht (n 375)* 50-53; De Schrijver and Maes (n 340) 3; Willem H van Boom en Karlijn J M van Doorn, 'Productaansprakelijkheid en productveiligheid' in Karlijn J M van Doorn en Sanne Pape (eds), *Handboek consumentenrecht* (Zutphen: Uitgeverij Parijs 2015) 264; Fairgrieve et al. (n 318) 53; Verhoeven (n 334) 112-113.

[377] Dommering-van Rongen, 'Produktenaansprakelijkheid: Een nieuwe Europese privaatrechtelijke regeling vergeleken met de produktenaansprakelijkheid in de Verenigde Staten' (n 376) 143.

[378] Ibid. See also: Verhoeven (n 334) 112.

[379] Louise Dommering-van Rongen, *Productaansprakelijkheid: Een rechtsvergelijkend overzicht* (n 375) 51.

[380] Geraint Howells et al., 'Product Liability and Digital Products' in Tatiani-Eleni Synodinou et al. (eds) *EU Internet Law* (Springer International Publishing AG 2017) 184.

mistakes do not occur for software. However, one can imagine programming bugs or deployment mistakes that can be recognised as manufacturing defects rather than design defects.

The second type of defects are design defects. According to §2(b) of the Restatement of Torts (3th), a product is "defective in design when the foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design by the seller or other distributor, or a predecessor in the commercial chain of distribution, and the omission of the alternative design renders the product not reasonably safe." Thus, a safer design of the product was possible and also reasonable given the circumstances, e.g. price and severity of the damage.[381] Design defects affect all products in a series.[382] In terms of assessing such a defect, one cannot refer to the product's own specifications or quality criteria as these are what make the product unsafe.[383] The risk-utility test is therefore considered to be more appropriate, whereby the pros and cons of the existing design must be weighed against the possible alternatives.[384]

An example of a design defect from case law is a sleeping pill which caused severe side effects because of its active substance.[385] In the context of software production, more specifically cybersecurity in smart home devices, we can easily recognise this type of defect. In part I of this thesis we mentioned studies that show that producers of smart devices do not take care of cybersecurity in their devices, i.e. they make a design choice by implementing no or limited cybersecurity. The question becomes whether the choices made by the producers are reasonable or not in the circumstances of the case. As mentioned above, the distinction between manufacturing defects and design defects may be difficult to draw in the context of software. For example, a software bug in a security update is likely to affect all products in a series (like a design defect) whilst at the same time such a flaw cannot be said to have been part of the design of the product (so that it is more like a manufacturing defect).

The third type of defects are instruction defects. These types of defects find their origin in wrong or incomplete information provided by the producer. Like design defects, instruction defects typically affect all products in a series.[386] According to §2(c) of the US Restatement of Torts (3th) a product is defective because of: "inadequate instructions or warnings when the foreseeable risks of harm posed by the product could have been reduced or avoided by the provision of reasonable instructions or warnings [...]." Inaccurate, incomplete or missing information can also render a product defective in the European

[381] Verhoeven (n 334) 112.
[382] Ibid.
[383] Dommering-van Rongen, *Productaansprakelijkheid: Een rechtsvergelijkend overzicht* (n 375) 52.
[384] Ibid (NB. She also considers the 'prudent manufacturer test' in this context, whereby the criterion is that a reasonable person would not have marketed the product knowing of its harmful capacity').
[385] Hoge Raad 30 juni 1989, NJ 1990, 652 (*Halcion*).
[386] Verhoeven (n 334) 112.

system of product liability law.[387] The presentation of the product is one of the circumstances to be taken into account in the assessment of defectiveness.[388] Especially for inherently dangerous products such as medical products or complicated high-tech goods, accurate and complete information is considered to be essential to this assessment.[389] It is not the case that inherently dangerous products render them defective, but the producer of such products must take into account that the public does not always recognise what specific dangers to expect.[390] If done properly, information, instruction and warnings can make an unsafe product safe, because it lowers the safety expectations that the public may have about this product.[391] At the same time, one can wonder about the effectiveness of such instructions and warnings in reality. Research has shown that users routinely disregard such security warnings.[392]

Examples of instruction defects in case law include the omission of information about side effects of medicines.[393] In the context of cybersecurity vulnerabilities in smart home devices, instruction defects can occur where producers do not provide information about the involved risks and instructions about how to limit them. As covered in Part I, where they rely on the end-user of the product for cybersecurity, they would do well by emphasising the importance of strong passwords and installing updates, and other measures that could prevent or reduce the risk of harm posed by the product.

A fourth type of product defect, which is not reflected in the US tripartite system, are mistakes in product monitoring. Dommering-van Rongen calls them product monitoring defects.[394] This refers to the obligation of producers to take appropriate measures when product defects are discovered after they have been put on the market. This is not a separate category of defects, but covers the other three types of defects.[395] In other words, a product monitoring defect always occurs in combination with one of the other types of defects. In the context of software production and cybersecurity vulnerabilities, one immediately thinks of the provision of warnings and software patches in case that a critical vulnerability is discovered after the initial moment of sale.

6.2.3 Application to the incident scenario's

In this section, we have so far described the elements of the defectiveness test and the traditional categorisation of defects. Some remarks have already been made about their application in the context of

[387] Fairgrieve et al. (n 318) 57.
[388] Article 6(1)(a) Product Liability Directive.
[389] Fairgrieve et al. (n 318) 57.
[390] Daily Wuyts, 'The Product Liability Directive – More than Two Decades of Defective Products in Europe' (2014) 5 *Journal of European Tort Law* 16.
[391] Fairgrieve et al. (n 318) 57.
[392] E.g. Bonnie Brinton Anderson et al., 'Your memory is working against you: How eye tracking and memory explain habituation to security warnings' (2016) 92 Decision Support Systems 3.
[393] Wuyts (n 390) 17.
[394] Louise Dommering-van Rongen, *Productaansprakelijkheid: Een rechtsvergelijkend overzicht* (n 375) 50.
[395] Ibid.

cybersecurity vulnerabilities and software production. Because of the case-by-case approach that needs to be taken, in this section we will more closely analyse three incident scenario's that may occur with smart home devices. The overall question is whether the cybersecurity vulnerability in the smart home device constitutes an unacceptable safety risk which an average person does not need to expect.

The structure in these analyses will be as follows. First, as a preliminary inquiry we will consider what type of (possible) defects we might be dealing with. Second, we will consider whether these product defects are likely to render the product defective within the meaning of the Directive. A note upfront is that, despite the fact that we are applying the tests to specific incident scenario's, we still do not have all the exact circumstances as would have been in a real case. Moreover, we can only indicate possible results without any certainty that a similar case will in fact have this outcome. Applying the test in this way will however approximate a real case as best as possible and provide some insights on possible outcomes. For all scenario's it is furthermore assumed that the end-user did not put the device to unreasonable use.[396]

The first incident scenario concerned a smart thermostat. The relevant information for the defectiveness analysis is that the smart thermostat ceased to work as a result of an internal software bug. Furthermore, the manufacturer was slow to respond with an update patch and difficult in his communication. The internal software bug can be classified as a manufacturing defect, because it cannot be said to be a part of the intended design of the software. The fact that many other people on the website's user forum complain about the same issue does indicate that all products in the series are affected, as is common for design defects, but this is inherent to the software production process. The slow response of the manufacturer qualifies as a product monitoring defect.

The appropriate test for assessing manufacturing defects is the average consumer expectation test. Is it reasonable for the average consumer to expect that this defect does not occur? On the one hand, it could be argued that software bugs will always occur. On the other hand, manufacturing defects of all sorts will always occur, so this should not have the effect of exonerating the manufacturer immediately. One could argue that this particular software bug is of a severity that the consumer is not required to expect. Circumstances that support this is that the owners tried to get the thermostat working again but that nothing helped, whereas a safe reboot on an older version of software might have been expected to be possible. Furthermore, the slow response of the manufacturer and difficult communication can be seen as an additional product defect or as a type of aggravating circumstance.

The second incident scenario concerned a smart lock. The manufacturer designed the lock with a connection to the open internet (rather than low-range technology) and with limited hardware capacity, which made it impossible to encrypt the internet traffic. As a result, the lock was easily hacked by

[396] Article 6(1)(b) Product Liability Directive.

intercepting usernames and passwords. The manufacturer made these choices to be able to produce the device cheaply and sell it for a competing price. In terms of the type of defect, this can be classified as a design defect. The manufacturer could have made different design choices that would have made the product safer in terms of cybersecurity.

The appropriate approach for design defects is to include elements of the risk-utility test into the average consumer expectation test. As mentioned above, it does not make sense to look at the specifications and quality standard of the product in comparison with the consumer expectation, because it is the design that is the problem. The risk-utility test involves criteria such as the likelihood that the risks will materialize, the availability of other products, knowledge of the consumer and the desirability of the product. In this context, there are other smart locks for sale and the consumer chose a cheap one for which you should have a lower expectation of safety. As with normal locks, a cheaper one will provide you with less security than an expensive one and there are always tricks to break a lock. On the other hand, the likelihood that the risk resulting from this design will materialize is considerate giving how easy it is to intercept unencrypted traffic. Moreover, the fact that the manufacturer chose to use long-range technology (WiFi connection) rather than low-range technology (e.g. BlueTooth) further increases the risk of misuse. The manufacturer could have implemented light weight encryption mechanisms to ensure that at least usernames and passwords are not transmitted unencrypted. In this sense, it can be said that there was a reasonable alternative design possible that would have increased the safety of the product.

The third scenario involved a smart baby monitor. It was supplied with a weak default password and the instruction manual only provided piecemeal information on the importance of changing the default password. No information was given about the cybersecurity risks either. This scenario involves a design defect and/or instruction defect. A design defect because the manufacturer decided to use weak default passwords, whilst it is good practice to provide strong default passwords. An instruction defect because the manufacturer could have foreseen this risk and could have prevented (or at least reduced) the unsafe situation by providing clear instructions on how to mitigate this cybersecurity risk.

Much the same as the second scenario, the design defect is best assessed on the basis of the risk-utility test. Because this involves mostly the same considerations, we will only look into the instruction defect. This involves the application of the average consumer test with an emphasis on the presentation of the product. As mentioned, especially for inherently dangerous products like complicated high-tech goods, a producer should provide adequate information about the risks and instructions on how to mitigate them. This is arguably even more so for a smart baby monitor that is connected to the internet, because users may not easily recognise these dangers when buying the product. Moreover, it is not very difficult or costly for the manufacturer to provide this information. A lack of information on basic cybersecurity measures is therefore quite likely to constitute an instruction defect.

6.3 Exemptions

The Directive provides the producer of a defective product with various defences. Where the producer proves any of the circumstances listed in Article 7 of the Directive, he will be exempted from liability. For example, in case the defect is the result of compliance with mandatory regulations issued by public authorities.[397] Here, we will consider only one of the exemptions that is often discussed in the context of innovative areas like high-tech products: the risk development defence. First, we will consider the background of the defence and how it is interpreted by the CJEU. Second, we will consider in what way it makes an impact on product liability for smart home devices.

Article 7(e) of the Directive provides that the producer shall not be liable if he proves "that the state of scientific and technical knowledge at the time when he put the product into circulation was not such to enable the existence of the defect to be discovered". This means that a producer is not liable for defects that are the result of so-called 'development risks', i.e. risks that could not have been known at the time that the product was put on the market. The development risk defence is based on the idea of foreseeability; where a risk was not foreseeable for the producer at the time he put the product in circulation, he should not be held liable for it. In other words, the producer can free himself of liability in the situation that the defect could not have been avoided even though the producer was in possession of all relevant available information at the time.[398] The effect is that the Directive shifts the risk of injury resulting from a new technology from the producer to the injured person.[399]

With regard to the functioning of the development risk defence, the CJEU has clarified its scope in *Commission v. United Kingdom*. According to the CJEU, the development risk defence "relates to the state of scientific and technical knowledge, including the most advanced level or such knowledge, at the time when the product in question was put into circulation".[400] It has been said that this introduces elements of a negligence standard, but where a producer must demonstrate the highest level of diligence.[401] Moreover, it is not a subjective test. Instead, one must take into account the "objective state of scientific and technical knowledge of which the producer *is presumed to have been informed*" (emphasis added).[402]

The risk development defence was controversial during the implementation of the Directive,[403] and remains a topic of debate in more recent studies.[404] In the initial proposal of the Directive, producers

[397] Article 7(1)(d) Product Liability Directive.
[398] Fairgrieve et al. (n 318) 78.
[399] Ibid.
[400] C-300/95 *Commission v. United Kingdom* [1997] ECR I-02649, para 26.
[401] Fairgrieve et al. (n 318) 78.
[402] *Commission v. United Kingdom* (n 400) para 27-28.
[403] Dommering-van Rongen, 'Produktenaansprakelijkheid: Een nieuwe Europese privaatrechtelijke regeling vergeleken met de produktenaansprakelijkheid in de Verenigde Staten' (n 376) 223. See e.g. Lori M. Linger, 'The

were liable for development risks because it was seen as undesirable to place the cost of safety risks for new and innovative products on the side of the consumer.[405] Because of concerns that strict liability in this context would stifle innovation and increase insurance costs, the development risk defence was included in the Directive as a compromise. For example the pharmaceutical industry, where experimental and innovative products may in the future cause unknown and undesirable side effects, voiced concerns about the burden of being liable for development risks.[406]

The risk development defence is optional: Member States could choose whether or not to implement it.[407] Most of the countries decided to implement the risk development defence.[408] Finland and Luxembourg are amongst the countries that did not implement the defence into national law, so that producers are liable for development risks in those countries.[409] In some countries the development risk defence only applies to particular products and in particular circumstances (including France, Germany and Spain) and in others it applies to all products (including Austria, Belgium, Denmark, the Netherlands and more).[410] Studies have shown that the risk development defence serves it purpose and there is no proof that it results in socially or economically unacceptable results.[411] It is however also said to be of limited practical relevance so that empirical evidence is scarce.[412]

In the context of smart home devices, we are dealing with an innovative area of production. This means that products are "under development", which brings about certain risks. However, because of the high standard that the defence requires it is unlikely that the producers of the smart home devices under consideration in this thesis are exempted from liability. As described in Part I, a reason for the lack of cybersecurity is that manufacturers do not have the required knowledge and expertise in this field. For example, an established baby monitor manufacturer might decide to start offering smart baby monitors without having an appropriate sense of the cybersecurity risks it is exposing its customers to. Because the risk development defence involves an objective test, whereby it is presumed that the producer was aware

Products Liability Directive: A Mandatory Development Risk Defense' (1990) 14(2) *Fordham International Law Journal* 478 (NB. Author argues that the defense should become mandatory rather than optional).

[404] Piotr Machnikowski, 'Introduction' in Piotr Machnikowski (ed), *European Product Liability, an Analysis in the State of the Art in the Era of New Technologies* (Cambridge, Intersentia 2016) 13.

[405] Verhoeven (336) 248; Dommering-van Rongen, 'Produktenaansprakelijkheid: Een nieuwe Europese privaatrechtelijke regeling vergeleken met de produktenaansprakelijkheid in de Verenigde Staten' (n 376) 221.

[406] Linger (n 403) 506, footnote 178.

[407] Article 15(1)(b) Product Liability Directive.

[408] Alessandra Alaimo et al., 'Study for the European Commission: Analysis of the Economic Impact of the Development Risk Clause as provided by Directive 85/374/EEC on Liability for Defective Products' (Fondazione Rosselli 2002) 28.

[409] Ibid.

[410] Ibid, 29-32.

[411] Piotr Machnikowski, 'Conclusions' in Piotr Machnikowski (ed), *European Product Liability, an Analysis in the State of the Art in the Era of New Technologies* (Cambridge, Intersentia 2016) 704; Alaimo et al. (n 408) 135.

[412] Alaimo et al. (408) 130 and 132.

of all the available knowledge in the field, these manufacturers cannot hide behind the development risk defence.

The relevance of the risk development defence is limited to “true” development risks, i.e. risks that could not have been known at the time of development. Similar to other aspects of the Directive, this is quite a static approach to product safety and product liability. It does not take into account the technological developments that make it possible to increase the level of cybersecurity (and thus safety) of a software-based product after the moment of sale. When taking this into account, the implications of the development risk defence decrease even further. In relation to the common cybersecurity vulnerabilities that are the subject of discussion in this thesis, we can say that these are known risks at this moment in time and would not fall under this exemption. E.g. a software bug or a hack resulting from a lack of transport encryption or use of default passwords can be considered as a foreseeable risk.

6.4 Chapter conclusion

In this chapter, we have aimed to answer the question of whether cybersecurity vulnerabilities in smart home devices constitute a defect within the meaning of the Directive. We have observed that the Directive traditionally deals with offline product defects, so that the inclusion of threats and harms flowing from cybersecurity vulnerabilities requires a transformation in thinking in the field of product liability and also product safety law. Because cybersecurity vulnerabilities in smart home devices do threaten the safety of users, it is concluded that inclusion of these issues in the defectiveness assessment of products would be a desirable development. Because the defectiveness assessment is performed on the basis of open norms, i.e. the legitimate expectations of the average consumer, the inclusion of cybersecurity concerns can be achieved within the current wording of the Directive.

Under the defectiveness test of article 6 of the Directive, one must assess the legitimate expectations of the general public with regard to the safety of a product and consider whether the product creates unacceptable safety risks. At the moment it is unclear whether the average consumer of smart home devices is a technically sophisticated and media literate consumer, or whether he or she is increasingly vulnerable and defenceless against the privacy and security implications in such a complex technological ecosystem. As suggested by Helberger, one must take into account this complexity, the nature of digital products and the ability of the consumer to deal with this complexity when assessing defectiveness in this context. In particular, one should take into account that smart device manufacturers have the ability to perform software updates, thereby increasing cybersecurity throughout the product’s lifecycle. This means that the level of safety at the moment of sale, which is currently a relevant circumstance to take into account, loses significance in the context of software-based products.

Although it is hard to provide conclusive remarks on the outcome of the defectiveness assessment because it is imprecise and indeterminate in content, the relevant circumstances of the three security incidents have been weighed against each other in search for an outcome. At this time, in which concerns about security, privacy and personal data are ubiquitous, it is reasonable to say that the general public is entitled to some degree of technical computer security in smart home devices. It is anticipated that this expectancy is likely to grow as these products become more pervasive in the future. Therefore, where a smart device manufacturer fails to take basic cybersecurity measures, such as the manufacturers in the incident scenarios, the resulting vulnerabilities should be considered as defects under the Directive. Where they cause harm, the smart home device manufacturer should be held responsible. The risk development defence is unlikely to be of help; although smart home devices are an innovative product area, the cybersecurity vulnerabilities that are the object of inquiry in this thesis cannot be said to be unforeseeable at this moment in time.

Chapter 7: Compensation of damages and other remedies

In this chapter, we will consider the last element of a claim under the Product Liability Directive (Directive) in more detail: damage. Rather than focusing on the concept of damage only, however, this chapter is more broadly aimed at meaningful remedies for cybersecurity vulnerabilities in smart home devices. This chapter functions as the connecting link between the list of meaningful remedies provided in Part I and the legal analysis.[413] To the extent that the Directive does not allow these remedies, we look to other fields of law that might help. By taking this perspective, both the merit and the shortcomings involved with using the Directive in this context are examined and placed in a broader legal perspective.

The structure is as follows. First, we will consider the available remedies under the Directive and apply this knowledge to the incident scenarios provided in part I.[414] We will see that the Directive only allows recovery for two particular types of damage and that the details are left mostly to the national laws of the Member States. Second, we consider the limits of the Directive's system of remedies in light of the meaningful remedies. Third, we examine alternative legal approaches with the aim of placing the Directive in a broader legal context.

7.1 Available remedies under the Product Liability Directive

From the wording of the Directive it follows that the producer is liable for damage caused by a defect in his product and that the injured person bears the burden of proving these elements.[415] Article 9 of the Directive provides two categories of recoverable damages. It states as follows:

> For the purpose of [the Directive], 'damage' means:
>
> (a) damage caused by death and personal injuries;
>
> (b) damage to, or destruction of, any type of property other than the defective product itself, with a lower threshold of 500 EUR, provided that the item of property:
>
> (i) is of a type ordinarily intended for private use or consumption, and
>
> (ii) was used by the injured person mostly for his own private use or consumption.
>
> This Article shall be without prejudice to national provisions relating to non-material damage.

In short, this means that the Directive provides for the recovery of two types of damages caused by a defective product: (a) damage caused by death or personal injury; and (b) damage to private

[413] Chapter 3.4.
[414] Chapter 3.3.
[415] Article 1 and 4 Product Liability Directive.

property.[416] As such, the Directive only covers consequential loss, which is economic loss following a personal injury or private property damage as defined in article 9(b) and excludes damages for pure economic loss.[417] With regard to the last sentence on non-material damage, the explanatory memorandum to the Directive makes clear that this type of damage is *not* within the regulatory scope of the Directive.[418] It is however possible to award such damages caused by a defective product where this is possible on the basis of *other legal grounds* in the national legal systems.[419]

The Directive does not further define the concept of damage. In *Henning Veedfald*, the CJEU has made clear that, therefore, it is left to the national legislatures to determine the precise contents of the two heads of damage stated in Article 9 of the Directive.[420] However, Member States are required to provide for the 'full and proper" compensation; they may not restrict the types of material damages that are to be made good.[421] This is an invocation of the principle of effectiveness: [422] the application of national rules may not impair the effectiveness of the Directive.[423] Although it is for the Member States to establish the characteristics and conditions for the categories of loss identified in Article 9 of the Directive, they may not do so in a way that negatively impacts the full compensation that was intended by the European legislator.[424]

The Directive also does not specify which remedies are available for repairing the two types of damage identified in Article 9, so that the types of claims that a person can pursue are a matter of domestic law.[425] The harmonisation that the Directive achieves in the context of remedies for product defects is thus very limited. In a 1999 Green Paper, the European Commission asked questions about whether special measures were required to improve victim's access to justice when claiming under the Directive.[426] Specifically, whether the Directive should introduce the possibility of injunctions and/or

[416] NB. Private property is used as a shorthand to indicate the type of damage described in article 9(b) of the Directive.

[417] Martin Ueffing, 'Directive 85/374 – European Victory or a Defective Product Itself?' (2013) Maastricht University MaRBLe Research Papers Vol 4 (2013) *Europeanisation of Private Law* 373, 391 <http://openjournals.maastrichtuniversity.nl/Marble/Article/view/167> accessed 8 March 2018.

[418] European Commission, 'Explanatory Memorandum' in 'Proposal for a Council Directive relating to the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products' COM (76) 372 (proposal for a directive on digital content) para 17.

[419] Ibid.

[420] Case C–203/99 *Henning Veedfald v Århus Ambtskommune* [2001] ECR I–3586, para 25-27.

[421] Ibid.

[422] Article 19(1) TFEU. See on this topic: Koen Lenaerts, *Effective judicial protection in the EU* (2013) 2 <http://ec.europa.eu/justice/events/assises-justice-2013/files/interventions/koenlenarts.pdf> accessed 28 January 2017.

[423] *Henning Veedfald* (n 420) para 27.

[424] Simon Whittaker, *Liability for Products* (Oxford University Press 2005) 504-505.

[425] Duncan Fairgrieve et al. 'Product Liability Directive' in Piotr Machnikowski (ed), *European Product Liability, an Analysis in the State of the Art in the Era of New Technologies* (Cambridge, Intersentia 2016) 81.

[426] Commission of the European Communities, 'Green paper on Liability for defective products' COM (1999) 369 final, 32.

group actions.[427] Based on the results of the consultation, the EC did not see reason to take action.[428] Various received contributions saw no need for an individual's right to an injunction because of the existing possibilities in national law.[429] Therefore, these matters have remained to be decided at the national level which results in divergences across Member States. To illustrate: Keirse reports that, in the Netherlands, an injunction is available for product liability claims on the basis of Article 3:296 of the Dutch Civil Code.[430] By contrast, this remedy is not available in the UK.[431]

Further relevant to note here is that the Directive includes a provision on the effects of multiple causation to the recovery of damage. Article 8(1) provides that the liability of the producer will not be reduced when the damage is caused by the defect and by the act or omission of a third party. This provision only affects the relationship between the injured person and the producer; it does not prejudice the national provisions concerning the law of the right of contribution or recourse under which the producer can recover compensation from the third party. Article 8(2) deals with contributory negligence. It provides that the liability of a producer may be reduced or disallowed when damage is caused by the defect and by the fault of the injured person (or someone for whom he is responsible). The exact meaning of fault and workings of this provision are left to be decided in accordance with the national provisions on contributory negligence.[432] In any case, it is possible that the amount of compensation is reduced or that compensation disallowed where the injured person did not exercise a proper level of care in response to the defect.

In the subsections that follow, more information will be given on the two heads of damages provided for in article 9 of the Directive. In this discussion we also consider the merit of these remedies in the context of cybersecurity vulnerabilities in smart home devices. Thereafter, we apply this knowledge to the incident scenarios to see not only the merits but also the shortcomings of the Directive's system of remedies.

[427] Ibid.

[428] Report from the Commission on the Application of Directive 85/374 on Liability for Defective Products, COM/2000/0893 final, para 3.2.10.

[429] Ibid. Also see: Rod Hunter and Lucas Bergkamp, 'Should Europe's Product Liability Regime be Expanded? Comments on the European Commission's Green Paper on Product Liability' (2001) 29 Product Safety and Liability Reporter 17, 403, 410.

[430] Anne Lucienne Maria Keirse, 'Product Liability in the Netherlands' in Piotr Machnikowski (ed), *European Product Liability, an Analysis in the State of the Art in the Era of New Technologies* (Cambridge, Intersentia 2016) 311, 342.

[431] Ken Oliphant and Vanessa Wilcox, 'Product Liability in England and Wales' in Piotr Machnikowski (ed), *European Product Liability, an Analysis in the State of the Art in the Era of New Technologies* (Cambridge, Intersentia 2016) 173, 196.

[432] Fairgrieve et al. (n 425) 87.

7.1.1 Damage caused by death and personal injuries

The recovery of damage caused by death and personal injury is seen as the primary purpose of product liability law.[433] It is therefore unsurprising that the Directive covers this type of damage. Article 16(1) of the Directive however also provides the regulatory option to place a financial cap on the amount of recoverable damages of this type, with a minimum of 70 million EUR, to meet the concerns of industry that massive claims would be brought under the Directive.[434] The majority of the Member States have not opted for this.[435] Besides this, Member States must provide for the full and proper compensation of this type of damages as provided by the CJEU in *Henning Veedfald*.

The meaning of "personal injury" is left to be decided by the laws of the Member States. Some guidance can be found in the explanatory memorandum to the Directive, which states that "[t]he term 'personal injuries' comprises the cost of [...] all expenditure incurred in restoring the injured person to health [...]."[436] Beyond this, the exact meaning of 'personal injury' is left to be decided by the national laws of the Member States. As a result, there are divergences at the national level. For example, in Germany and Austria, the concept of "personal injury" includes recovery of psychological damage.[437] By contrast, in the Netherlands psychological damage is only recoverable under product liability law where it is caused by physical personal injury or death. Recovery of mere psychological damage is seen as immaterial damage which is recoverable only under the fault-based general tort liability regime.[438] To limit such divergences at the national level, the European Parliament has proposed in the past to make explicit in Article 9(a) that personal injury covers damage caused by "physical and/or mental injuries".[439] This amendment has not been accepted,[440] which means that national divergences remain in relation to recovery of damage caused by death or personal injury.

[433] Joined Cases C-503/13 and C-504/13 *Boston Scientific Medizintechnik* [2015] ECLI:EU:C:2015:148, Opinion of AG Bot, para 65.

[434] Countries that have made use of this option include Germany (§10(1) Produkthaftungsgesetz sets a limit of 85 million EUR) and Spain (Article 141 Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias sets a limit of €63.106.270,96 EUR - originally established in pesetas before the conversion to the Euro).

[435] Piotr Machnikowski, 'Conclusions' in Piotr Machnikowski (ed), *European Product Liability, an Analysis in the State of the Art in the Era of New Technologies* (Cambridge, Intersentia 2016), 674.

[436] European Commission, 'Explanatory Memorandum' (n 418) para 16.

[437] Ilona van der Zalm, '*Hof 's Hertogenbosch 1 September 2009, LJN BJ7299*' [2010] 7(1) Jurisprudentie Aansprakelijkheid 1, para 4 (note).

[438] See e.g.: Hof 's Hertogenbosch 1 September 2009, ECLI:NL:GHSHE:2009:BJ7299.

[439] European Parliament, Committee on the Environment, Public Health and Food Safety, 'Legislative resolution embodying Parliament's opinion on the proposal for a European Parliament and Council Directive amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products' (COM(97)0478 C4-0503/97 97/0244(COD)).

[440] Dagmar Roth-Behrendt, 'Report on the proposal for a European Parliament and Council Directive amending 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 (COM(97)0478 - C4-0503/97 - 97/0244(COD))' (European Parliament, Committee on the Environment, Public Health and Consumer Protection, 28

In any event, where cybersecurity vulnerabilities cause death or personal injury the Directive covers the recovery of damage. One could think of a smart baby monitor heating and even exploding as the result of a software vulnerability, thereby causing physical injuries to those in its vicinity. These instances are like traditional “offline” product liability cases like a coca bottle exploding and causing personal injury.[441] In the online or virtual context, it seems rather unlikely that software vulnerabilities cause this type of damage. An exception would be smart assisted living devices, which are a blend of medical and smart home devices.[442] In the non-medical consumer smart home market however, instances of defects causing physical injury or death are likely to be rare and to the knowledge of the author have not been reported yet.

Another possible incident would be the remote access of a smart baby monitor, listening in on private conversations in the home or even using the speaker function to harass people. This may cause mental injury in various forms. Whether this type of damage is recoverable depends on the implementation of the Directive in the national laws of the Member States. As we saw above, Germany and Austria allow for the recovery of mental injury under the heading of ‘personal injury’ in their product liability laws. In the Netherlands, this type of damage is only recoverable under the general fault-based tort regime, which includes recovery of non-material damage caused by mental injury.[443]

7.1.2 Damage to private property

The second type of damage that the Directive covers is damage to, or destruction of a certain type of private property. The ruling in *Henning Veedfald* also covers Article 9(b) of the Directive, which means that full and proper compensation must be provided for by the Member States. This head of damage is however only of limited significance because of its restricted scope. There are three limitations to take into account, namely that the damage must concern:

1. other items of property than the defective product itself;
2. a sum higher than 500 EUR; and
3. is intended for private use or consumption and used as such by the injured person.

We will consider these limitations in more detail in the following paragraphs.

September 1998) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A4-1998-0326+0+DOC+XML+V0//EN> accessed 11 April 2018.

[441] Escola v. Coca Cola Bottling Co., 150 P.2d 436, 24 Cal. 2d 453, 1944 Cal (absolute liability for producer of exploding coca cola bottle); Hoge Raad 24 december 1993, *Leebeek / Vrumona*, ECLI:NL:HR:1993:ZC1197 (cola bottleneck breaking whilst used normally; defective unless producer proves otherwise).

[442] European Commission, ‘Advancing the Internet of Things in Europe’ SWD(2016) 110 final, 32. See also, e.g. European Commission, ‘Smart technology tested in Germany allows older people to live independently’ (*European Commission Projects*, 23 August 2017) <http://ec.europa.eu/regional_policy/en/projects/germany/smart-technology-tested-in-germany-allows-older-people-to-live-independently> accessed 12 April 2018.

[443] Article 6:106(1)(b) Burgerlijk Wetboek (Dutch Civil Code).

First, only damages that are *caused by* the defective product are covered. The Directive does not cover damage to the defective product itself. This means that claims relating to the replacement or repair of the defective product are generally not covered. These types of (contractual) claims typically belong to the national law on the sale of goods, which remains unaffected by the Directive.[444] In particular, the proposal for a directive on digital content provides interesting opportunities, which we will discuss in more detail below.[445]

Second, the damage must concern a sum higher than 500 EUR. This franchise is intended to prevent excessive litigation for product liability.[446] There are various divergences at the national level. Some countries have a lower threshold as a result of the currency conversion now or when the euro was introduced, for example the UK and Italy.[447] Furthermore, because of ambiguity in the different language versions of the Directive, it can be interpreted as a deductible or as a threshold which, once met, allows for the recovery of the full amount of damages.[448] Regardless of these differences at the Member State level, this second limitation will in many cases prevent consumers from bringing a successful claim under the product liability regime, "as it may be assumed that in many cases damage to consumer goods due to a defect in the product does not exceed this value".[449]

Third, the damage must concern property that is intended for private use and be used in such a manner by the injured person. Therefore, under the Directive only damage to private property is recoverable. In *Société Moteurs Leroy Somer* the CJEU confirmed that damage to property intended for and used in the professional context is not within the scope of the Directive.[450] This limitation effectively restricts the recovery of property damage under the Directive to consumers, whereas the class of injured persons that can claim for damage caused by death or personal injury is not limited in such a way. Because this research focuses on meaningful remedies from the perspective of the consumer, this limitation to a claim for property damage under the Directive is of little relevance to us.

In the context of smart home devices we can conclude that, where cybersecurity vulnerabilities result in property damage to other private property in the home this is recoverable insofar it exceeds an amount of 500 EUR. For the reasons mentioned above, it is questionable whether this will incentivise many consumers to pursue a claim under the Directive. Especially the fact that the Directive does not cover damage to the smart home itself means that it cannot be used to repair or replace the smart home

[444] European Commission, 'Explanatory Memorandum' (n 418) para 20.
[445] See: Chapter 7.3.3.
[446] Recital 9 Product Liability Directive.
[447] UK: Section 5(4) Consumer Protection Act 1987 (limit of £275). Italy: Article 123 of the Consumer Code, Legislative Decree 6 September 2005 no.206 (limit of €387).
[448] Fairgrieve et al. (n 425) 84.
[449] Machnikowski, 'Conclusions' (n 435) 685.
[450] Case C‑285/08 *Société Moteurs Leroy Somer v Société Dalkia France and Société Ace Europe* [2009] ECR I-04733, para 17.

device. At first glance, this seems to exclude the possibility to use the Directive to compel security updates in case that e.g. a software vulnerability is discovered, regardless of whether an injunction is even available as a remedy in the national implementation of the Directive that is applicable to the case.

7.1.3 Other types of damages

A question that comes to mind when discussing the two heads of damages listed in the Directive is how this system relates to the recovery of other types of damages caused by defective products. For example, property damage of a type that does not meet the requirements of Article 9(b) of the Directive. There are two approaches that can be taken. First (the more convincing approach): anything that is not regulated by the Directive remains to be governed by the national legislatures. Second (and less convincing): Article 9 encompasses all possible types of damage so that all damage resulting from a defective product must be categorised as such.

The first approach is founded in the general logic of EU law: Member States retain their full legislative powers over any subject matter that does not fall within the scope of the Directive.[451] Although the Directive aims for full harmonisation, Article 13 makes clear that it does not preclude a (similar or equivalent) system of liability for subject matter that is not covered by the Directive.[452] In this vein, the CJEU ruled in *Société Moteurs Leroy Somer* that the Directive did not preclude a French provision of strict liability for a defective product which allowed recovery for damages intended for and used for professional purposes.[453] Although such damage is not recoverable under the Directive, which only covers damage to private property, this did not mean that the Directive precluded a rule at the national level allowing for recovery of this type of damage under the same conditions as those provided by the Directive.[454]

The second approach can be found in *Henning Veedfald*. Here, the CJEU seems to indicate that Article 9 is exhaustive in the sense that it encompasses all possible types of damage.[455] The CJEU instructed the referring national court to categorise the damage that resulted from the defective product under one of the three categories provided by Article 9 of the Directive.[456] In this examination, the national court was not allowed “to decline to award any damage at all under the Directive on the ground that, where the other conditions of liability are fulfilled, the damage incurred is not such as to fall under

[451] Dorota Leczykiewicz, ‘Compensatory Remedies in EU Law: The Relationship Between EU Law and National Law” in Paula Giliker (ed) *Research Handbook on EU Tort Law* (Edward Elgar 2017); Oxford Legal Studies Research Paper No. 18/2017, 11.

[452] Case C-402/03 *Skov and Bilka* [2006] ECR I-00199.

[453] *Société Moteurs Leroy Somer* (n 450).

[454] Ibid, para 17 and 32.

[455] Fairgrieve et al. (n 425) 83.

[456] *Henning Veedfald* (n 420) para 33.

any of the foregoing heads."[457] On the basis of this finding of the Court one might conclude that all damages must fit in either of the two heads of damage listed in Article 9 of the Directive.

It is however likely that this reading of the last part of the judgment is unintended. It contradicts the CJEU's position taken earlier in the case that the interpretation of the heads of damage is left to the Member States; by saying that all damage must fall within one of the categories, not much room is left for Member States to interpret the meaning of the categories.[458] Therefore, the first approach discussed above should be accepted. This means that damages which do not fall within the scope of Article 9 are not recoverable under the Directive (or its implementations in national law), but may be recoverable on another legal ground available to the claimant at the national level. Considering the fact that the Directive merely creates a complementary system of product liability, this includes other product liability rules.

7.1.4 Application to the incident scenario's

Having discussed the Directive's system of remedies, we will now consider whether the harms in the incident scenarios are covered by the Directive.[459] A note upfront is that it is difficult to answer this question based solely on the Directive, because the exact meaning of the two categories of damages and the available remedies very much depend on the implementations of the Directive in the Member States. Furthermore, despite the fact that we are looking at specific incident scenario's, this does not reflect all the intricacies that a real case would have. It will however give some indication of the meaningfulness of the Directive in the context of cybersecurity vulnerabilities in smart home devices.

The first incident scenario concerned a smart thermostat which turned off as a result of an internal software bug. Because of the cold, the owners decide to stay at a friend's house. While they are gone, the water pipes freeze and burst, causing significant water damage to the house. The owners therefore clearly incur costs relating to damage to their private property. Where this damage exceeds the amount of 500 EUR, it is covered by Article 9(b) of the Directive and as such should be recoverable in the national law applicable to the case. It is important to note that contributory negligence of the owners, as they simply left the house unattended, might affect the amount of recoverable damages.

The second incident scenario involved the hack of a smart lock which resulted in burglary. The house owners also suffer from anxiety and distress and live in fear of another burglary. With regard to the incurred losses as a result of the stolen items, it is not entirely clear whether they are covered by the Directive as it only refers to "damage to, or destruction of" an item of property. Ordinarily, this type of damage is considered to be property damage. Therefore, where defectiveness and causation is established also, the producer will be liable for the damage to private property that the owners incurred. Because

[457] Ibid.
[458] Fairgrieve et al. (n 425) 82.
[459] See: Chapter 3.3.

Article 8(1) provides that the producer's liability shall not be reduced where the damage is caused by a third party also, the producer is not able to point towards the hacker as the primary culprit.

Depending on the applicable national law, the anxiety, distress and fear that the house owners suffer as a result of the burglary can be classified as mental personal injury or immaterial damage. Recovery of the former is possible under the Directive (provided the national law covers this in its conception of personal injury) and the latter is to be determined solely the basis of Member State laws and as such does not fall within the scope of the Directive. For example, in the Netherlands recovery of non-material damages under product liability law is only possible insofar this damage is caused by physical personal injury or death.[460] Immaterial damage, including 'fear and loss of enjoyment of life' can be recovered under the general system of fault-based tort law.[461]

The third scenario involved a baby monitor hack. It causes anxiety and distress, for which the same can be said as in in scenario 2 discussed above. Furthermore, it involves a violation of the fundamental right to privacy (and protection of personal data). Recovery of damages for this would classify as non-material damages, regulation of which is left to the national laws of the Member States. The outcome hereof thus very much depends on the availability of immaterial damages at the national level. This shows that in the context of privacy concerns, the Directive does not offer a harmonised solution for cybersecurity vulnerabilities in smart home devices.

For example, in the Netherlands it is possible to claim non-material damages where the victim is personally harmed,[462] which includes a serious violation of a fundamental right. [463] To a limited degree, the Dutch judiciary has also accepted the recovery of non-material damage for a violation of a fundamental right without further injury.[464] This reflects a tendency of the Dutch judiciary to take compensation for violations of fundamental rights seriously.[465] In the literature this is called "integrity damage": damage resulting from a violation of a fundamental right that does not create material damage nor mental injury, but which does affect the integrity of a person.[466] This type of damage is almost

[460] Van der Zalm (n 437) para 4.

[461] Marijke Malsch, 'Compensation of Non-Material Damage in Civil and Criminal Law in the Netherlands' (2002) 9 International Review of Victimology 31, 33-34.

[462] Article 6:106 Burgerlijk Wetboek (Dutch Civil Code).

[463] Albert J. Verheij, 'Vergoedbaarheid van angstschade' (2018) 3 Nederlands Tijdschrift voor Burgerlijk Recht, para 2.3.

[464] Siewert D. Lindenbergh, 'Schending en schade. Over aantasting van fundamentele rechten en eenheid in het schadevergoedingsrecht' *Rechtseenheid en vermogensrecht* (BW-krant Jaarboek 2005) 305-327.

[465] Ibid.

[466] Ivo Giesen, 'Herstel als er (juridisch) geen schade is: "integriteitsschade"' E.C. Huijsmans en M. van der Weij (eds) *Schade en herstel* (Wolf Legal Publishers 2014) 44; Tim F. Walree, 'De vergoedbare schade bij de onrechtmatige verwerking van persoonsgegevens' (2017) 7172 Weekblad voor Privaatrecht, Notariaat en Registratie 921, 926.

punitive by nature. It can be imposed on another party than those who violated the fundamental right, which is important in this scenario as it is not the manufacturer who violates the right to privacy.[467]

To conclude this overview of possibilities in the incident scenarios, we very clearly see only limited possibilities in the context of cybersecurity vulnerabilities in smart home devices. Not all the types of damages are recoverable under the Directive. In particular, non-material harm is not covered by the Directive, but depends fully on available legal grounds in the national laws of the Member States. The same goes for damage to other property, but this is less relevant in the context of remedies from the perspective of the consumer. Moreover, the Directive does not harmonise remedies for repairing possible damages, so that it is not clear whether some form of injunction is available to consumers of smart home devices across Europe.

This outcome is not necessarily surprising, because we have stated from the outset that the Directive is unlikely to be a panacea in solving the issue of cybersecurity vulnerabilities in smart home devices.[468] An express aim of this study was also to highlight the shortcomings of the Directive's system of remedies in the context of cybersecurity vulnerabilities in smart home devices. Table 2 provides an overview of the results. MSL indicates that the availability of the remedy depends on the national laws of the Member State that are applicable to the case (Member State Law, MSL).

	Product Liability Directive
COMPENSATORY MEASURES	
> Recovery of damages	
- personal injury	Yes
- private property	Yes
- other property	No
- non-material harm	No
PREVENTIVE MEASURES	
> Injunction	MSL*
- provision of security updates	
- repair or replacement of the device	
- information at the moment of sale	
- notification at the moment of security incident	

Table 2: overview of meaningful remedies provided by the Directive

7.2 Pushing the limits of the Directive's system of remedies

The discussion of whether the harms in the incident scenarios are covered by the Directive has shown various shortcomings of the Directive's system of remedies. In the following paragraphs, we highlight two reasons why the Directive's system of remedies is limited. First, the fact that the Directive mostly

[467] Hoge Raad 9 juli 2004, *Groningen / Lammerts*, NJ 2005, 391 (claim for damages against the municipality for riots in a private home).

[468] See: Chapter 3.4.

pursues a compensatory rather than a preventive aim. Second, the limited harmonisation that the Directive achieves in the context of remedies. In both discussions, we will consider how these limitations may be overcome.

7.2.1 Compensation rather than prevention

The Directive mainly pursues a compensatory function by providing for the compensation of certain types of damages. This focus fits well with the traditional compensatory function of liability law in general.[469] The list of meaningful remedies however also included preventive measures, i.e. injunctions of various kinds to move the device manufacturer to increase cybersecurity. To which extent does the Directive also allow such preventive measures, if at all? In short, recent developments in the CJEU's case law have highlighted the preventive function of the Directive. We will discuss this in the following paragraphs and consider whether these results can be extended to cybersecurity vulnerabilities in smart home devices.

The CJEU recognised a type of preventive action in *Boston Scientific*.[470] This case concerned medical devices implanted in patients which were potentially defective. Besides the question relating to defectiveness,[471] the Court also considered whether the costs of the preventive surgery to replace the devices were covered by the Directive as damages caused by personal injury under Article 9(a). In response to the discovery of the product defect, the producer of these devices advised physicians to replace the devices. They provided the replacement product free of charge, but refused to pay the costs of the surgeries. Both the Court and the AG concluded that these costs were damages caused by personal injury within the meaning of the Directive. According to the Court, compensation for damage "(…) relates to all that is necessary to eliminate harmful consequences and to restore the level of safety which a person is entitled to expect".[472] This includes the costs relating to the replacement of the defective product.[473]

In his opinion, AG Bot emphasised the preventive function of the Directive. He stated that the Directive "manifestly pursues a preventive aim, by imputing liability to the person who, having created the risk most directly by manufacturing a defective product, is in the best position to minimise it and prevent damage at the lowest cost."[474] This preventive aim would be disregarded by requiring the occurrence of actual damage to demonstrate defectiveness.[475] The recognition that compensation for costs preventing a more serious harm can be rewarded is likely to prompt producers to improve the safety of

[469] A. Franken, 'Het voorzorgsbeginsel in het aansprakelijkheidsrecht - een verkenning' (2010) 5 Aansprakelijkheid, Verzekering en Schade, 25.
[470] Joined Cases C-503/13 and C-504/13 *Boston Scientific Medizintechnik* [2015] ECLI:EU:C:2015:148.
[471] See: Chapter 6.2.1.
[472] *Boston Scientific* (n 470), para 49.
[473] Ibid, para 50.
[474] Bot (Advocate General) (n 433) para 38.
[475] Ibid.

their products, because it is not only the actually incurred damage that is recoverable under the Directive.[476]

It is difficult to extend the findings of the CJEU in *Boston Scientific* to other types of products, because this case involved the extraordinary case of potentially defective medical devices implanted in human bodies which posed life-threatening risks. It is difficult to imagine a cybersecurity vulnerability in a smart home device which poses a serious risk of the right type of damage. An exception hereto is the area of smart assisted living. Smart assisted living devices are a blend of medical and smart home devices and assist (senior) citizens in their homes. Cybersecurity vulnerabilities in these type of smart devices clearly involve greater risks to a person's physical safety and have the potential to create life-threatening risks not unlike the defective pacemakers in *Boston Scientific.* For example, imagine that cybersecurity vulnerabilities cause a smart stairlift to malfunction and harm its user.

One could therefore argue, in the context of smart home living or smart home devices more generally, that a security update or another preventive measure is necessary in order to prevent serious damage from occurring. Depending on the law of the Member State in which the claim is pursued, it might be possible to claim an injunction rather than compensation of costs to prevent the damage from occurring. In this way, one could imagine that the producer would have to patch the security vulnerability (or cover the costs hereof) similar to the way the manufacturer in *Boston Scientific* had to pay for the replacement surgeries. The fact that information, warnings and instructions have been proven to be ineffective makes it less likely that these types of injunctions are allowed on the basis of this argument. Moreover, where serious harm is likely to materialize it makes little sense to obtain an injunction to provide information or warning (except where no other option is available).

At the same time, it must be admitted that this approach is quite a stretch and would only be a possibility in very limited circumstances. First, it will only be an available route of litigation in countries that provide injunctions as a remedy in the context of the implementation of the Directive. Second, this would only be possible where the impending damage falls within either of the two heads of damage identified by Article 9 of the Directive. Arguably, only a risk of serious personal harm will suffice as this was the case in *Boston Scientific*. It is difficult to imagine a cybersecurity vulnerability in a smart home device which poses a serious risk of the right type of damage. After all, increasing cybersecurity in a smart home device is very unlike surgically replacing a pacemaker in a patient's body to avert a life-threatening risk.

[476] Ibid, para 74.

7.2.2 Limited scope of harmonisation

The Directive provides only minimal guidance in respect of the concept of damage and the types of remedies that are available for consumers. This means that many details are left to be decided by the national laws of the Member States, which leads to legal divergences across Member States. In this respect, the harmonising power of the Directive is quite limited. Notable is the fact that the availability of an injunction depends on the laws of the Member States. In general, divergences in the Member States procedural law will create divergences in remedial possibilities for consumers throughout the EU.

In theory, it might be possible to complain about the lack of remedies in the Directive and/or at the national level on the basis of fundamental rights.[477] In particular, one can think about invoking the rights to privacy and the protection of personal data and/or the right to consumer protection in combination with the right to an effective remedy as enshrined in Article 7, 8, 38 and 47 of the Charter of Fundamental Rights of the European Union (CFREU).[478]

A successful invocation of the aforementioned fundamental rights would be a type of indirect horizontal effect of fundamental rights, whereby the Directive or a national law is interpreted and/or assessed in light of these fundamental rights.[479] Norbert Reich has described how remedies under national law can be upgraded by appealing to the principle of effectiveness under EU law, which is codified in article 47 of the CFREU, leading to a hybrid remedy based in both national and EU law.[480] The Court has been particularly activist in relation to the right to the protection of personal data,[481] which means there may also be a role to play for this right in the context of the Directive.

A full discussion of this complex interaction between fundamental rights and provisions of national law goes beyond the scope of this thesis, but it should be noted that an appeal to these fundamental rights may have a positive effect on the remedies available for consumers under the Directive. Fundamental rights could be invoked to overcome obstacles in national procedural law, for example provisions related to the burden of proof.

7.3 Alternative approaches

Having examined both the merits and the shortcomings of the Directive's system of remedies, we will now consider some alternative legal routes. The aim of this section is to tentatively place the Directive in

[477] See on general principles of EU law: Norbert Reich, *General Principles of EU Civil Law* (Cambridge, Intersentia 2014).

[478] See also: Article 6, 8 and 13 of the European Convention of Human Rights. The right to an effective remedy is furthermore also recognized as a general principle of EU law, i.e. the effectiveness principle (which includes the principle of equivalence). See on this topic: Reich, *General Principles of EU Civil Law* (n 477) 89 and onwards.

[479] Article 52(5) CFREU. See: Arthur S. Hartkamp, *Asser 3-I Europees recht en Nederlands vermogensrecht* (Wolters Kluwer 2015) 207-215, para 231d.

[480] Reich, *General Principles of EU Civil Law* (n 477) 98-99.

[481] Takis Tridimas, 'Fundamental Rights, General Principles of EU Law, and the Charter' (2014) 16 Cambridge Yearbook of European Legal Studies 361.

a broader legal context. We merely explore these other fields of law without aiming to be exhaustive. The results of this quick comparison with the Directive are given in table 3 at the end of this section.

We will consider three alternative legal routes. First, using civil litigation to enforce the producer's obligations in product safety law that relate to information, notification, control and recall of products. Second, a claim based on the obligation to take adequate security measures in the context of data protection law. Third, a claim based on consumer contract law. At the end of this chapter, an overview table of the remedies provided by the Directive in relation to these alternative routes is provided.[482]

7.3.1 Product safety law

The general Product Safety Directive harmonises producers' obligations with regard to the safety of products.[483] The main obligation is to only place safe product on the market.[484] Furthermore, the Product Safety Directive places various information and monitoring obligations on producers and provides measures that can be taken when risks materialize.[485] Similar to the Directive, the Product Safety Directive has been created with traditional, offline product safety in mind. For example, where it is discovered that a product contains lead or that its reaction to fire is higher than was declared.[486] In the near future, a desirable development would be to include cybersecurity concerns in this area of law also, making it a more dynamic area of law.[487] In particular, it would be interesting to explore the possibility of a "digital product recall". This could e.g. take the form of providing a security update that averts the discovered safety risk, which is a possibility that does not exist for offline products.

If the Product Safety Directive were to include cybersecurity risks also, what is its value for consumers in civil litigation? Product safety law is a public area of law, and the Product Safety Directive does not create standing to sue for a consumer who feels that a producer does not meet its obligations. Where a safety risk occurs, producers can opt to voluntarily take measures (e.g. warning consumers or a product recall) or they can be forced by the public regulator.[488] The question of whether it is possible for consumers to enforce the obligations in the Product Safety Directive via a civil lawsuit depend on the national laws of the Member States. To illustrate, let's consider the Netherlands. In literature it has been

[482] See: Table 3, page 101.

[483] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety [2001] OJ L11/4 (Product Safety Directive).

[484] Article 3(1) Product Safety Directive.

[485] Article 5(1) Product Safety Directive.

[486] Examples derived from rapid alert numbers A12/0350/18 and A12/0353/18.

[487] Éireann Leverett, Richard Clayton and Ross Anderson, 'Standardisation and Certification of the 'Internet of Things' (WEISS Conference, 2017) 22 <http://www.cl.cam.ac.uk/~rja14/Papers/weis2017.pdf> accessed 15 December 2018.

[488] Article 5(1)(b) and Article 8 Product Safety Directive.

argued that it is possible to obtain an injunction to force a product recall.[489] The producer's infringement of the Product Safety Directive constitutes unlawful behaviour, which opens up the route for a claim based on general tort law. One could imagine a similar claim for enforcing other obligations of the producers, e.g. the information obligation.

7.3.2 Data protection law

In Europe, the protection of personal data is regulated via the upcoming General Data Protection Regulation ("GDPR").[490] The GDPR is likely to apply in the context of smart home devices, as they collect personal data about their surroundings. Depending on the circumstances, the device manufacturer could be the "controller" of this personal data and as such the primary responsible person under the GDPR. Of particular interest is Article 32 of the GDPR, which requires entities that are responsible for the processing of personal data to implement appropriate security measures. The CIA-triad is the conceptual framework for this. In the event that a personal data breach occurs, affected individuals must be informed thereof and instructed how they can mitigate the risks that flow from the breach.[491]

Enforcement of the GDPR is possible by public regulators, but also individuals. Where someone feels that his or her rights under the GDPR are infringed, they have the right to an effective judicial remedy.[492] Furthermore, the GDPR allows recovery of material and non-material damage suffered as a result of an infringement.[493] This opens up the possibility to claim non-material damage caused by a lack of cybersecurity in a smart home device, whereas this is not harmonised in the Directive. Injunctions are not mentioned in the GDPR, which means that their availability depends on the national laws of the Member States also.

7.3.3 Consumer contract law

Consumer contract law aims to protect consumers in their dealings with traders, because they are considered as the weaker party. It regulates sales contracts between traders and consumers, which also includes (software) licenses. In the event that the device manufacturer of a smart home device is the licensor of the software in the smart home device, this agreement is subject to consumer contract law. Illustrative in this context is the Dutch case of the Consumentenbond v. Samsung, in which a consumer rights association is trying to compel software updates from Samsung and the provision of information

[489] Frank Kroes, 'Product recall. Enkele vermogensrechtelijke gezichtspunten' (2005) 3 Vermogensrechtelijke Analyses, 32.

[490] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 (General Data Protection Regulation, GDPR).

[491] Article 33 and 34 GDPR.

[492] Article 79 GDPR.

[493] Article 82 GDPR; Recital 85 GDPR.

thereof on the basis of national and European consumer contract law.[494] Some other interesting areas to explore are the following.

The Consumer Rights Directive provides information obligations for traders.[495] Article 6(1)(r) of this Directive requires the trader to provide information on the functionality of digital content, including about the technical protection measures.[496] This is an obligation to provide information about cybersecurity measures at the moment of sale. Under the Unfair Commercial Practice Directive, it is considered an unfair commercial practice to omit material information about the transaction.[497] Arguably, this includes the provision of information about cybersecurity. In the proposal for a directive on digital content, rules on conformity of a digital content contract also relate to the security features of the digital content.[498]

These Directives vary in the level of harmonisation in respect of remedies. The Consumer Rights Directive states that Member States must ensure that adequate and effective means exist to enforce compliance, leaving the particulars to be decided by the Member States.[499] Enforcement of the obligations in the Unfair Commercial Practices Directive is more harmonised. In particular, it provides for the availability of an injunction to stop the unfair commercial practice.[500] Also the proposal for a directive on digital content provides various remedies for non-conformity, ranging from specific performance to compensation of damages to the digital environment of the consumer.[501]

[494] For the writ of summons (in Dutch) see: https://www.consumentenbond.nl/binaries/content/assets/cbhippowebsite/actie-voeren/updaten/dagvaarding-consumentenbond---samsung-11-nov-2016.pdf . For an English summary of the case so far see: Paul Verbruggen et al., *Towards Harmonised Duties of Care and Diligence in Cybersecurity* (European Foresight Cyber Security Meeting 2016) 78, 83-84 <https://ssrn.com/abstract=2814101> accessed 23 August 2017.

[495] Consumer Rights Directive 2011/83/EU.

[496] This article relates to distance contract, which are defined as contract whereby there is no simultaneous physical presence of the trader and the consumer, which is the case when a consumer accepts a software license when initially setting up the smart home device (and possible renewals).

[497] Article 7 Unfair Commercial Practices Directive 2005/29/EC.

[498] Article 6(1)(a) and Article 6(2) proposal for a directive on digital content.

[499] Article 23 Consumer Rights Directive.

[500] Article 11(2) of the Unfair Commercial Practices Directive states that it must be possible to order the cessation or prohibition of an unfair commercial practice, without there being a requirement of actual loss or damage, or intention of negligence on the side of the trader.

[501] Article 14 and 2(8) of the proposal for a directive on digital content.

	Product Liability Directive	*Product Safety Directive**	*GDPR*	*Consumer contract law*
COMPENSATORY MEASURES				
> Recovery of damages		No	Yes**	Yes / MSL***
- personal injury	Yes			
- private property	Yes			
- other property	No			
- Non-material harm	No			
PREVENTIVE MEASURES				
> Injunction	MSL	MSL	MSL	Yes / MSL
- provision of security updates				
- repair or replacement of the device				
- information at the moment of sale				
- notification at the moment of security incident				

* possibilities depend on development in this area of law to include cybersecurity concerns.
** any material or non-material damage resulting from an infringement of the GDPR.
*** contractual damages.

Table 3: Overview of meaningful remedies provided by the Directive placed in broader legal context

7.4 Chapter conclusion

In this chapter, we have considered to which extent the Directive provides meaningful legal solutions in the context of cybersecurity vulnerabilities in smart home devices. We have seen that the Directive covers two types of damages: damage caused by death and personal injury and a certain type of private property damage. Where a smart home devices causes damage of these sorts, the Directive provides for the full and proper compensation hereof. Other types of damages, including non-material damages, are not recoverable under the Directive. This does not prejudice the recovery of such damage caused by a defective product on the basis of other legal grounds in the national laws of the Member State. We can conclude that the Directive offers some meaningful legal solutions in the form of compensatory measures when certain types of damage occur. However, the fact that recovery of non-material damage is not included in the scope of the Directive is a great deficit in the context of finding a remedy for privacy harms.

The possibilities under the Directive to obtain a preventive measure are very limited. The Directive pursues a compensatory rather than a preventive aim. In *Boston Scientific* the CJEU allowed a type of preventive action. Its significance for cybersecurity problems in smart home devices is however likely to be limited. Except where cybersecurity vulnerabilities create life-threatening risks similar to those in *Boston Scientific*, e.g. in the context of smart assisted living devices, it is difficult to extend the Court's findings to the problem of cybersecurity vulnerabilities in smart home devices. The Directive furthermore achieves only limited harmonisation with respect to remedies. The availability of certain remedies, most notably injunctions, are left to be decided at the national level. It has been suggested that invoking the fundamental right to privacy and the protection of personal data and/or the right to consumer protection in combination with the right to an effective remedy can have a positive effect on the available remedies for the consumer in national court. In the last section of this chapter, some alternative legal routes have been explored to place the findings about the Directive in a broader legal context. The results hereof can be found in table 3.

Chapter 8: Conclusion

The purpose of this thesis has been to find out whether the European product liability regime as established by the Product Liability Directive (Directive), provides meaningful legal solutions in the context of cybersecurity vulnerabilities in smart home devices that cause private harm. The main legal inquiries were whether the Directive is applicable in this context and, where it does, whether it provides meaningful remedies from the perspective of the consumer. The research question was the following:

> **To which extent does the European product liability regime offer meaningful solutions to the problem of attributing responsibility for cybersecurity vulnerabilities in consumer smart home devices?**

The underlying aim of this research was to find a solution to the problem of allocating responsibility for cybersecurity in smart home devices, as it has been shown that these devices often lack an adequate level of cybersecurity. Considering that the smart home market is expected to grow significantly in the next years, the risk of private harm that flows from badly secured smart home devices is expected to increase also. A reason to look to the Directive is that producers of smart home devices are in a good position to increase the level of cybersecurity, as they have control over the products that they put on the market. The idea is to incentivise them to increase the level of cybersecurity in their products by making them liable for a lack thereof.

The legal analysis is supported by an extensive factual background to the problem of cybersecurity vulnerabilities in smart home devices. This background shows that the excitement about the potential of the smart home market can be offset with concerns about privacy and security, which might harm the further growth of this market. Furthermore, the issue of allocating responsibility for cybersecurity in smart devices is complicated, because of the variety of interdependent actors that are involved in the Internet of Things (IoT) ecosystem. By limiting our focus to cybersecurity in relation to the smart device itself, we identified three common vulnerabilities: soft/firmware vulnerabilities, insufficient authentication/authorisation and a lack of transport encryption. The device manufacturer can implement basic technological security measures to prevent or reduce the threats that stem from these vulnerabilities. Where such technological measures are not taken, threats can materialise in security incidents that cause private harm to consumers.

The first legal inquiry focused on the application of the Directive to the problem of cybersecurity vulnerabilities in smart home devices. We encountered various interpretative difficulties relating to the product definition and the defectiveness assessment under the Directive. Where these difficulties can be overcome, consumers can benefit from the broad class of liable persons that are defined as ‘producer’ under the Directive. However, the exclusion of service providers from the scope of liable persons is problematic in the context of smart home devices, because software is increasingly offered as a service rather than a good. This is an issue that also relates to the product definition under the Directive (see below). In relation to the exclusion of the original designer from the scope of liable persons, it has been observed that this rationale does not make sense for the developer (designer) of software. Therefore, it is recommended that a software developer is seen as a manufacturer rather than a designer for the purposes of the Directive.

The requirement that a product must be a tangible good are difficult to overcome for software components of a smart home device, whilst these parts are often the source of cybersecurity vulnerabilities. For this reason, it is difficult to define smart home devices as products within the meaning of the Directive. Whereas hardware components of smart home devices are clearly tangible goods, software is often seen as intangible where it is supplied without a physical carrier. Moreover, transformations in the production of software indicate a move to a service-oriented architecture model, whereby software products become an amalgam of software components offered by different third party service providers. These developments have a profound effect on the characterisation of software as a good rather than a service.

The tangibility requirement has been discussed at length. Based on the reasoning that software is tangible when it is stored on a physical carrier, including where it is incorporated into a tangible good (provided that the software is necessary for the full or partial functioning of the good and forms an indistinguishable part of the good), we concluded that firmware and software installed on the smart home device at the moment of sale is tangible. Updates can be considered as incorporated into the smart home device from the moment of installation, thereby also satisfying the tangibility criterion. For the parts of the software which are not present on the device itself but stored "in the cloud", it has been suggested that they ultimately also reside on a server and as such are tangible also. The fact that one must engage in this exercise of creative interpretation in order to prevent arbitrary outcomes in the characterisation of software is however undesirable. As an overall solution, it is therefore recommended to abandon the physical carrier reasoning in favour of a product definition which defines software as products independently of their means of transmission. For this, inspiration can be drawn from the proposal for a directive on digital content.

The requirement that products are goods rather than services is increasingly problematic in the context of smart home devices. The reasons for this are twofold. First, smart devices are equipped with service-like aspects (for example, real-time information on the status of heating in the home). Second, the software in smart home devices is organised as a service rather than a good via service-oriented architecture models. This means that software is increasingly modular, i.e. complemented by offerings from other third party service providers. By taking into account these technological underpinnings of software production, i.e. how consumer software is produced today, it becomes clear that the characterisation of software as a good rather than a service is flawed. Whilst it has been recommended by other to simply extend the scope of the Directive to cover services also, this is likely to be too coarse a measure and will result in unintended side-effects. Whilst the inclusion of the service-like aspects of smart home devices in the product definition of the Directive would be a desirable development (also because these aspects can be seen as features of the tangible good rather than as a service), the developments in the production of software pose a more fundamental problem to the traditional goods/services distinction on which the Directive relies. This is an area that would merit from more legal research that takes the production of software into account.

In relation to the assessment of defectiveness under the Directive, it has been observed that the focus has traditionally been on offline product defects. Considering the growth of software based products, a transformation in thinking about product safety to also include (cyber)security would be a desirable development. The defectiveness assessment is performed on the basis of open norms, i.e. the legitimate expectations of the average consumer, which means that the inclusion of cybersecurity concerns can be achieved within the current wording of the Directive. It has been suggested that at this time, in which concerns about security, privacy and personal data are ubiquitous, it is reasonable to say that the general public is entitled to some degree of technical computer security in smart home devices. This expectancy is likely to further increase in the future. Therefore, where a device manufacturer fails to take basic cybersecurity measures, the resulting vulnerabilities should be considered as defects under the Directive.

Whilst acknowledging the difficulties in the application of the Directive in the context of cybersecurity vulnerabilities in smart home devices, the second inquiry focused on whether the Directive offers meaningful legal solutions. This question is answered against the evaluative framework formed on the basis of the factual analysis; a list of meaningful legal solutions. This includes compensation of damage where a security incident has occurred and preventive action in the form of injunctions to move the device manufacturer to increase the level of cybersecurity in smart home devices. Overall, we must conclude that the possibilities under the Directive are limited. This means that the value of applying the Directive to this set of problems is limited from the perspective of the consumer. The Directive would need to be amended in order to ensure that these meaningful legal solutions in the context of cybersecurity vulnerabilities are available throughout the European Union.

The Directive’s system of remedies is limited to compensation of certain types damages. In the event that a consumers suffers damage caused by death or personal injury or damage to private property other than the defective product itself and exceeding an amount of EUR 500, this damage must be fully compensated. The recovery of non-material damages is however not included, which is a great deficit in the context of finding a remedy for privacy harms. Also damage to the defective product itself is not recoverable under the Directive. The availability of injunctions depends fully on the national laws of the Member States. Some form of preventive action can be created by extending the ECJ's findings in *Boston Scientific*. The significance hereof is likely to be limited. Except where cybersecurity vulnerabilities create life-threatening risks, e.g. in the context of smart assisted living devices, such a preventive measure is unlikely to be carried by that case. Another possibility would be to invoke the fundamental right to privacy and the protection of personal data and/or the right to consumer protection in combination with the right to an effective remedy to obtain a procedural advantage before the national court.

The overall conclusion of this thesis is that the Directive is capable of providing some meaningful legal solutions for consumers in the context of cybersecurity vulnerabilities in smart home devices. The applicability of the Directive to this problem is however not self-evident. Various interpretative difficulties need to be overcome in order to be able to define these devices as products within the meaning of the Directive. Moreover, the limitations of the Directive's system of remedies make it a less evident route for preventive measures (e.g. an injunction for the provision of a security update) and the exclusion of non-material damages makes it a less attractive legal route when recovering damages for privacy harms. Without amendment of the Directive, the threat of liability that emanates from the Directive is therefore restricted. Other legal approaches may prove to be more fruitful in this context. However, the fact that the Directive does offer a meaningful solution to consumers in certain circumstances makes it applicability to cybersecurity vulnerabilities in smart home devices worthwhile.

References

Alaimo A et al., ‘Study for the European Commission: Analysis of the Economic Impact of the Development Risk Clause as provided by Directive 85/374/EEC on Liability for Defective Products*’* (Fondazione Rosselli 2002).

Albrecht J P, ‘Hearing, Security in the Internet of Things?’ (*Jan Philipp Albrecht*, 21 June 2017) <https://www.janalbrecht.eu/2017/06/2017-06-21-security-in-the-internet-of-things/> accessed 13 February 2018.

Anderson B et al., ‘Your memory is working against you: How eye tracking and memory explain habituation to security warnings’ (2016) 92 Decision Support Systems 3.

Arnbak A, ‘Securing Private Communications’ (PhD dissertation, University of Amsterdam 2015).

Arthur S. Hartkamp, *Asser 3-I Europees recht en Nederlands vermogensrecht* (Wolters Kluwer 2015).

Article 29 Data Protection Working Party, ‘Opinion 8/2014 on the Recent Developments of the Internet of Things’ 14/EN WP223, 4.

Asghari H, ‘Cybersecurity via Intermediaries’ (PhD dissertation, University of Delft 2016).

Baldwin G, ‘Researcher finds huge security flaws in Bluetooth locks’ (*engadget*, 8 October 2016) < https://www.engadget.com/2016/08/10/researcher-finds-huge-security-flaws-in-bluetooth-locks/> accessed 23 February 2018.

Barrett B, ‘Want safer passwords? Don’t change them so often’ (*Wired*, 3 October 2016) < https://www.wired.com/2016/03/want-safer-passwords-dont-change-often/> accessed 21 February 2018.

Bilton N, ‘Nest Thermostat Glitch Leaves Users in the Cold’ *The New York Times* (New York City, 13 January 2016) <https://www.nytimes.com/2016/01/14/fashion/nest-thermostat-glitch-battery-dies-software-freeze.html> accessed 6 February 2018.

BITAG, ‘Internet of Things (IoT) Security and Privacy Recommendations’ (BITAG, 2016). <https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf> accessed 22 November 2017.

Bix B, ‘Conceptual Questions and Jurisprudence’ (1995) 1 Legal Theory 465.

Borking J J, ‘Risico’s voortvloeiend uit produktaansprakelijkheid voor programmatuurmakers’ [1987] Informatie 928.

Bot (Advocate General), Opinion of 21 October 2014 in Joined Cases C-503 and 504/13, *Boston Scientific Medizintechnik v. OAK Sachsen-Anhalt.*

Bugeja J et al., ‘On Privacy and Security in Smart Connected Homes’ (2016 European Intelligence and Security Informatics Conference, Uppsala, August 2016).

Cakebread C, ‘Consumers are holding off on buying smart-home gadgets thanks to security and privacy fears’ (*Business Insider*, 15 November 2017) <http://www.businessinsider.com/consumers-holding-off-on-smart-home-gadgets-thanks-to-privacy-fears-2017-11?international=true&r=US&IR=T> accessed 22 February 2018.

Cbp, ‘Richtsnoeren voor beveiliging persoonsgegevens’ (Cbp, 2013).

Charles P. Pfleeger, ‘Data Security’ in Anthony Ralston et al. (eds) *Encyclopedia of Computer Science 4th Edition* (Nature Publishing Group 2000) 504.

Ciampa M, *Security Awareness: Applying Practical Security in Your World* (fifth edition, Cengage Learning 2017).

Cloud Service Alliance, ‘Security Guidance for Early Adopters of the Internet of Things (IoT)’ (CSA 2015) <https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf> accessed 17 October 2017.

Cloud Service Alliance, ‘Future-Proofing the Connected World: 13 Steps to Developing Secure IoT Products’ (CSA, 2016) 17, <https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf> accessed 22 November 2017.

Columbus L, ‘2017 Roundup Of Internet Of Things Forecasts’ (*Forbes*, 10 December 2017) <https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#3fb953c1480e> accessed 7 February 2018.

Commission of the European Communities, ‘Green paper on Liability for defective products’ COM (1999) 369 final.

Davis J, ‘Locating the average consumer: his judicial origins, intellectual influences and current role in European trade mark law’ (2005) 2 Intellectual Property Quarterly 183.

Davis J, ‘Revisiting the average consumer: an uncertain presence in European trade mark law’ (2015) 1 Intellectual Property Quarterly 15.

Dean B C, ‘An Exploration of Strict Products Liability and the Internet of Things’ (Center for Democracy & Technology, April 2018) <https://cdt.org/files/2018/04/2018-04-16-IoT-Strict-Products-Liability-FNL.pdf> accessed 16 April 2018.

Deloitte, ‘2017 Global Mobile Consumer Survey: US edition’ (Deloitte, 2017) <www.deloitte.com/us/mobileconsumer> accessed 22 February 2018.

DeNisco Rayome A, ‘DDoS attacks increased 91% in 2017 thanks to IoT’ (*TechRepublic.*, 20 november 2017) <https://www.techrepublic.com/Article/ddos-attacks-increased-91-in-2017-thanks-to-iot/> accessed 6 February 2018.

De Schrijver S and Maes M, 'Aansprakelijkheid in een ambient-intelligence omgeving: Wie heeft het gedaan?' (2010) 174 Computerrecht.

Dommering D and Van Eijk N, 'Convergenties in regulering: reflecties op elektronische communicatie' (Dutch Ministry of Economic Development, 2010).

Dommering-van Rongen L, 'Produktenaansprakelijkheid: Een nieuwe Europese privaatrechtelijke regeling vergeleken met de produktenaansprakelijkheid in de Verenigde Staten' (PhD thesis, University of Utrecht 1991).

Dommering-van Rongen L, *Productaansprakelijkheid: Een rechtsvergelijkend overzicht* (Deventer, Kluwer 2000).

Efthymiou C and Kalogridis G, 'Smart Grid Privacy via Anonymization of Smart Metering Data' (First IEEE International Conference on Smart Grid Communications, October 2010).

ENISA, 'Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures' (ENISA, November 2017).

ENISA, 'Major DDoS Attacks Involving IoT Devices' (ENISA Suggested Reading, 3 November 2016) <https://www.enisa.europa.eu/publications/info-notes/major-ddos-attacks-involving-iot-devices> accessed 6 February 2018.

European Commission, 'A Connected Digital Single Market for All' COM(2017) 228 final, 12.

European Commission, 'Advancing the Internet of Things in Europe' SWD(2016) 110 final, 6.

European Commission, 'Brief factual summary on the results of the public consultation on the rules on producer liability for damage caused by a defective product' (2017) GROW/B1/H1/sc(2017) 3054035.

European Commission, 'Commission's Forward Planning of Evaluation and Studies – 2017 and beyond' (2017) <https://ec.europa.eu/info/sites/info/files/20170504-studies-and-evaluations-2017-planning_en.pdf> accessed 27 March 2018.

European Commission, 'Evaluation of the Directive 85/374/EEC concerning liability for defective products - Roadmap' (2016) <http://ec.europa.eu/DocsRoom/documents/18842/> accessed 2 January 2018.

European Commission, 'Explanatory Memorandum' in 'Proposal for a Council Directive relating to the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products' COM (76) 372.

European Commission, 'Shaping the Digital Single Market' <https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market> accessed 8 February 2018.

European Commission, 'Smart technology tested in Germany allows older people to live independently' (*European Commission Projects*, 23 August 2017)

<http://ec.europa.eu/regional_policy/en/projects/germany/smart-technology-tested-in-germany-allows-older-people-to-live-independently> accessed 12 April 2018.

European Parliament, Committee on the Environment, Public Health and Food Safety, 'Legislative resolution embodying Parliament's opinion on the proposal for a European Parliament and Council Directive amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products' (COM(97)0478 C4-0503/97 97/0244(COD)).

Fairgrieve D et al. 'Product Liability Directive' in Piotr Machnikowski (ed), *European Product Liability, an Analysis in the State of the Art in the Era of New Technologies* (Cambridge, Intersentia 2016).

Franken A, 'Het voorzorgsbeginsel in het aansprakelijkheidsrecht - een verkenning' (2010) 5 Aansprakelijkheid, Verzekering en Schade 25.

FTC Staff Comment, 'Comments on the Benefits, Challenges and potential Roles for the Government in Fostering the Advancement of the Internet of Things' (FTC 2016).

FTC Staff Report, 'Internet of Things: Privacy and Security in a Connected World*'* (FTC 2015) <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf> accessed 22 November 2017.

Gaffey C, 'Web of Insecurity: Hacked Baby Monitors Highlight Perils of Internet of Things' (*Newsweek*, 9 april 2015) <http://www.newsweek.com/baby-monitors-hackhack-baby-monitorsbaby-monitorsinternet-thingsinternet-600746> accessed 5 December 2017.

Giesen I, 'Herstel als er (juridisch) geen schade is: "integriteitsschade" E.C. Huijsmans en M. van der Weij (eds) *Schade en herstel* (Wolf Legal Publishers 2014).

Girot C, *User protection in IT contracts: a comparative study of the protection of the user against defective performance in information technology* (The Hague, Kluwer Law International 2001).

Gürses S and Preneel B, 'Cryptology and Privacy in the Context of Big Data' in Bart van der Sloot et al. (eds) *Exploring the boundaries of big data* (Amsterdam, Amsterdam University Press 2016).

Gürses S and Van Hoboken J, 'Privacy After the Agile Turn' in Evan Selinger (eds), *Cambridge Handbook of Consumer Privacy* (Cambridge University Press, 2017) <https://osf.io/ufdvb/> accessed 14 October 2017 (Draft Version 2).

Hart H L A, 'Positivism and the Separation of Law and Morals' (1958) 71 Harvard Law Review 593.

Helberger N, 'Profiling and Targeting Consumers in the Internet of Thigns - A New Challenge for Consumer Law' in Reiner Schulze and Dirk Staudemeyer (eds) *Digital Revolution: Challenges for Contract Law in Practice*' (Hart Publishing 2016).

Hewlett Packard Enterprise, *Internet of things research study* (HP, November 2015 <http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf> accessed 5 December 2018.

Hill K, 'When 'Smart Homes' Get Hacked: I Haunted A Complete Stranger's House Via The Internet' (*Forbes*, 26 Juli 2013) <https://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/#1e25032fe426> accessed 7 December 2017.

Hojnik J, 'Technology Neutral EU law: digital goods within the traditional goods/services distinction' (2017) 25 International Journal of Law and Information Technology 63.

Howells G et al., 'Product Liability and Digital Products' in Tatiani-Eleni Synodinou et al. (eds) *EU Internet Law* (Springer International Publishing AG 2017).

Hughes M, 'Hacker remotely raises home temperature 12ºC (22ºF) on smart thermostat' (*The Next Web,* 21 July 2017) <https://thenextweb.com/insider/2017/07/21/hacker-remotely-raises-home-temperature-12oc-22of-smart-thermostat/> accessed 6 February 2018.

Hughes M, 'Thermostats can now get infected with ransomware, because 2016' (*The Next Web*, 8 August 2016) <https://thenextweb.com/gadgets/2016/08/08/thermostats-can-now-get-infected-with-ransomware-because-2016/#.tnw_MJak6uyF> accessed 6 February 2018.

Hunter R and Bergkamp L, 'Should Europe's Product Liability Regime be Expanded? Comments on the European Commission's Green Paper on Product Liability' (2001) 29 Product Safety and Liability Reporter 17, 403.

Hutchinson T and Duncan N, 'Defining and Describing What We Do: Doctrinal Legal Research' (2012) 17 Deakin Law Review 83.

Hutchinson T, 'Doctrinal research: researching the jury' in Dawn Watkins and Mandy Burton (eds) *Research Methods in Law* (Taylor & Francis Group 2013).

Incardona R and Poncibò C, 'The average consumer, the unfair commercial practices directive, and the cognitive revolution' (2007) 30(1) Journal of Consumer Policy 21.

Initiatiefnota van het lid Verhoeven: Het Internet der Dingen: maak apparaten veilig!, *Kamerstukken II* 2016/17, 34613, 2.

International Telecommunication Union Recommendation Y.2060, 'Overview of the Internet of Things' (ITU, 2012) <https://www.itu.int/rec/T-REC-Y.2060-201206-I> accessed 17 October 2017.

International Telecommunication Union, World Telecommunication/ICT Development Report and database, 'Individuals Using the Internet (% of population)' (The World Bank, undated) <https://data.worldbank.org/indicator/IT.NET.USER.ZS> accessed 7 February 2018.

Internet Society, *Some Perspectives on Cybersecurity: 2012* (Internet Society 2012).

Keirse A L M, 'Product Liability in the Netherlands' in Piotr Machnikowski (ed), *European Product Liability, an Analysis in the State of the Art in the Era of New Technologies* (Cambridge, Intersentia 2016).

Kite-Powell J, ‘This Company Staged A Hack With Multiple Devices To Show Your Home's Vulnerability’ (*Forbes*, 19 September 2017) <https://www.forbes.com/sites/jenniferhicks/2017/09/19/this-company-staged-a-hack-with-multiple-devices-to-show-your-homes-vulnerablity/#503922895322> accessed 6 February 2018.

Kokx B, ‘De cybersecurity uitdaging’ (2017) 3 Tijdschrift voor Compliance 171.

Kroes F, ‘Product recall. Enkele vermogensrechtelijke gezichtspunten’ (2005) 3 Vermogensrechtelijke Analyses, 32.

Leczykiewics D, ‘The Constitutional Dimension of Private Law Liability Rules in the EU’ in D. Leczykiewics and S. Weatherill (eds) *The Involvement of EU Law in Private Law Relationships* (Hart Publishing, 2013).

Lenaerts K, *Effective judicial protection in the EU* (2013) <http://ec.europa.eu/justice/events/assises-justice-2013/files/interventions/koenlenarts.pdf> accessed 28 January 2017.

Leverett E, Clayton R and Anderson R, ‘Standardisation and Certification of the ‘Internet of Things’ (WEISS Conference, 2017) <http://www.cl.cam.ac.uk/~rja14/Papers/weis2017.pdf> accessed 15 December 2018.

Lindenbergh S D, ‘Schending en schade. Over aantasting van fundamentele rechten en eenheid in het schadevergoedingsrecht’ *Rechtseenheid en vermogensrecht* (BW-krant Jaarboek 2005) 305-327.

Lindqvist J, ‘New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?” (2017) 25 International Journal of Law and Information Technology 1.

Linger L M, ‘The Products Liability Directive: A Mandatory Development Risk Defense’ (1990) 14(2) *Fordham International Law Journal* 478.

Lynch G, ‘Amazon Key smart lock security integrity called into question by hack’ (*Techradar*, 5 February 2018) <http://www.techradar.com/news/amazon-key-smart-lock-security-integrity-called-into-question-by-hack> accessed 6 February 2018.

Machnikowski P, ‘Conclusions’ in Piotr Machnikowski (ed), *European Product Liability, an Analysis in the State of the Art in the Era of New Technologies* (Cambridge, Intersentia 2016).

Machnikowski P, ‘Introduction’ in Piotr Machnikowski (ed), *European Product Liability, an Analysis in the State of the Art in the Era of New Technologies* (Cambridge, Intersentia 2016).

Mak C, ‘Rights and Remedies: Article 47 EUCFR and Effective Judicial Protection in European Private Law Matters’ (2012) Amsterdam Law School Legal Studies Research Paper no. 2012-88; Centre for the Study of European Contract Law Working Paper No. 2012-11 < https://ssrn.com/abstract=2126551> accessed 25 January 2018.

Malsch M, ‘Compensation of Non-Material Damage in Civil and Criminal Law in the Netherlands’ (2002) 9 International Review of Victimology 31.

Manko R, *EU Competence in private law: The Treaty framework for a European private law and challenges for coherence* (European Parliamentary Research Service, 2015).

McDaniel P and Smith S W, 'Security and Privacy Challenges in the Smart Grid' (2009) 7(3) IEEE Security and Privacy, 75.

Minerva R et al., *Towards a Definitions of the Internet of Things (IoT)* (IEEE Internet Initiative 2015).

Mitew T, 'Do objects dream of an internet of things' (2014) 23 The Fibreculture Journal 3.

Moeller S, 'Characteristics of Services – a new approach uncovers their value' (2010) 25(5) Journal of Services Marketing 359.

NBC News, 'Man Hacks Monitor, Screams at Baby Girl' (*NBC News*, 28 April 2014) <https://www.nbcnews.com/tech/security/man-hacks-monitor-screams-baby-girl-n91546> accessed 5 december 2014.

Nissenbaum H, 'Where Computer Security Meets National Security' (2005) 7 Ethics and Information Technology 61.

O'Reilly T, 'Design Patterns and Business Models for the Next Generation of Software (*O'Reilly*, 30 September 2005) <http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=4> accessed 27 February 2018.

OECD Working Party on Communication Infrastructures and Services Policy, 'The Internet of Things: Seizing the Benefits and Addressing the Challenges (OECD 2015).

Olejnik L, 'Highlights of the French cybersecurity strategy' (*Security, Privacy & Tech Inquiries*, 13 February 2018) <https://blog.lukaszolejnik.com/highlights-of-french-cybersecurity-strategy/> accessed 14 February 2018.

Oliphant K and Wilcox V, 'Product Liability in England and Wales' in Piotr Machnikowski (ed), *European Product Liability, an Analysis in the State of the Art in the Era of New Technologies* (Cambridge, Intersentia 2016).

OWASP, 'Top 10 2014-I10 Poor Physical Security' <https://www.owasp.org/index.php/Top_10_2014-I10_Poor_Physical_Security> accessed 21 February 2018.

OWASP, 'Top 10 2014-I2 Insufficient Authentication/Authorization' <https://www.owasp.org/index.php/Top_10_2014-I2_Insufficient_Authentication/Authorization> accessed 5 December 2017.

OWASP, 'Top 10 2014-I4 Lack of Transport Encryption' <https://www.owasp.org/index.php/Top_10_2014-I4_Lack_of_Transport_Encryption> accessed 7 December 2017.

OWASP, ‘Top 10 2014-I9 Insecure Software/Firmware’ <https://www.owasp.org/index.php/Top_10_2014-I9_Insecure_Software/Firmware> accessed 7 December 2017.

OWASP, ‘Top IoT vulnerabilities’ <https://www.owasp.org/index.php/Top_IoT_Vulnerabilities> accessed 5 December 2017.

Oxford Dictionaries, ‘Authentication’ <https://en.oxforddictionaries.com/definition/authentication> accessed 5 December 2017.

Oxford Dictionaries, ‘Authorise’ <https://en.oxforddictionaries.com/definition/authorize> accessed 5 December 2017.

Oxford English Dictionary, ‘Encrypt’ <http://www.oed.com> accessed 10 December 2017.

Paez M and La Marca M, ‘The Internet of Things: Emerging Legal Issues for Businesses’ (2016) 43 North Kentucky Law Review 29.

Poudel S, ‘Internet of Things: Underlying Technologies, Interoperability and Threats to Privacy and Security” (2016) 31 Berkeley Technology Law Journal 997.

Ragan S, ‘Here are the 61 passwords that powered the Mirai IoT botnet’ (*CSO*, 3 October 2016) <https://www.csoonline.com/Article/3126924/security/here-are-the-61-passwords-that-powered-the-mirai-iot-botnet.html> accessed 5 December 2017.

Reich N, *General Principles of EU Civil Law* (Cambridge, Intersentia 2014).

Reich N, ‘Product Liability and Beyond: An Exercise in ‘Gap-Filling’ (2016) 3-4 European Review of Private Law 619.

Report from the Commission on the Application of Directive 85/374 on Liability for Defective Products, COM/2000/0893 final.

Ross E, ‘Baby Monitors ‘Hacked’: Parents Warned to be Vigilant After Voices Heard Coming From Speakers’ (*The Independent*, 30 January 2016) <http://www.independent.co.uk/life-style/gadgets-and-tech/news/baby-monitors-hacked-parents-warned-to-be-vigilant-after-voices-heard-coming-from-speakers-a6843346.html> accessed 6 February 2018.

Roth-Behrendt D, ‘Report on the proposal for a European Parliament and Council Directive amending 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 (COM(97)0478 - C4-0503/97 - 97/0244(COD))’ (European Parliament, Committee on the Environment, Public Health and Consumer Protection, 28 September 1998) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A4-1998-0326+0+DOC+XML+V0//EN> accessed 11 April 2018.

Samaila M G et al., ‘Security Challenges of the Internet of Things’ in Batalla et al. (eds) *Beyond the Internet of Things: Everything Interconnected* (Springer International Publishing AG 2017).

Schmon C, *Review of the Product Liability Rules, BEUC Position Paper* (The European Consumer Organisation 2017).

Schneier B, ‘Testimony before the U.S. House of Representative in the Joint Hearing entitled Understanding the Role of Connected Devices in Recent Cyber Attacks’ (16 November 2016) <https://www.schneier.com/essays/archives/2016/11/testimony_at_the_us_.html> accessed 5 December 2017.

Stanislav M and Beardsley T, ‘HACKING IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities’ (*Rapid7*, 29 September 2015) <https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf> accessed 5 December 2017.

Statista, ‘Smart Home Worldwide’ <https://www.statista.com/outlook/279/100/smart-home/worldwide#> accessed 29 November 2017.

Stuurman C (Kees) and Vandenberghe G P V, ‘Softwarefouten: een ‘zaak’ van leven of dood?’ (1988) 24 *Nederlands Juristenblad* 45/46, 1667.

Symantec, ‘Internet Security Threat Report’ (Symantec, 2017) <https://www.symantec.com/content/dam/symantec/docs/reports/gistr22-government-report.pdf> accessed 5 December 2017.

Symantec, ‘Mirai: what you need to know about the botnet behind recent major DDoS attacks’ (*Symantec Official Blog*, 27 October 2016) <https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks> accessed 5 December 2017.

Techopedia Dictionary, ‘Authentication, Authorization and Accounting (AAA)’ <https://www.techopedia.com/definition/24130/authentication-authorization-and-accounting-aaa> accessed 7 December 2017.

Techopedia Dictionary, ‘Software’ <https://www.techopedia.com/definition/4356/software> accessed 7 December 2017.

The Huffington Post ‘Parental Warning: Your Baby Monitor Can Be Hacked’ (*The Huffington Post*, 23 August 2016) <https://www.huffingtonpost.com/healthline-/parental-warning-your-bab_b_11668882.html> accessed 7 February 2018.

Thielman S and Johnston C, ‘Major cyber attack disrupts internet service across Europe and US’ *The Guardian* (London and New York City, 21 October 2016) <https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service> accessed 6 February 2018.

Thomson I, ‘If you use ‘smart’ Bluetooth locks, you're asking to be burgled’ (*The Register*, 8 August 2016)

<https://www.theregister.co.uk/2016/08/08/using_a_smart_bluetooth_lock_to_protect_your_valuables_youre_an_idiot/> accessed 6 February 2018.

Tridimas T, ‘Fundamental Rights, General Principles of EU Law, and the Charter’ (2014) 16 Cambridge Yearbook of European Legal Studies 361.

Ueffing M, ‘Directive 85/374 – European Victory or a Defective Product Itself?’ (2013) Maastricht University MaRBLe Research Papers Vol 4 (2013) *Europeanisation of Private Law* 373, 391 <http://openjournals.maastrichtuniversity.nl/Marble/Article/view/167> accessed 8 March 2018.

Van Boom WH and Van Doorn C J M, ‘Productaansprakelijkheid en productveiligheid’ in Karlijn van Doorn en Sanne Pape (eds), *Handboek consumentenrecht* (Zutphen, Uitgeverij Parijs 2015).

Van der Zalm I, ‘*Hof ‘s Hertogenbosch 1 September 2009, LJN BJ7299*’ [2010] 7(1) Jurisprudentie Aansprakelijkheid (note).

Van Gestel R and Micklitz H W, ‘Revitalizing Doctrinal Legal Research in Europe: What About Methodology?’ (2011) EUI Working Paper LAW 2011/05 <https://ssrn.com/abstract=1824237> accessed 3 April 2018.

Verbruggen P et al., *Towards Harmonised Duties of Care and Diligence in Cybersecurity* (European Foresight Cyber Security Meeting 2016) <https://ssrn.com/abstract=2814101> accessed 23 August 2017.

Verhagen L, ‘18-jarige jongen opgepakt in verband met ddos-aanvallen op Belastingdienst’ *Volkskrant* (Amsterdam, 5 February 2018) <https://www.volkskrant.nl/media/18-jarige-jongen-opgepakt-in-verband-met-ddos-aanvallen-op-belastingdienst~a4566981/> accessed 20 February 2018.

Verheij A J, ‘Vergoedbaarheid van angstschade’ (2018) 3 Nederlands Tijdschrift voor Burgerlijk Recht.

Verhoeven D, ‘Productveiligheid en productaansprakelijkheid’ (PhD dissertation, University of Antwerp 2016).

VVD, CDA, D66 en ChristenUnie, ‘Regeerakkoord 2017-2021: Vertrouwen in de Toekomst’ (10 October 2017).

Waaijers C and Kasteleijn N, ‘Zware DDoS-aanvallen: wie, wat, waar en waarom?’ (*NOS*, 21 January 2018) < https://nos.nl/artikel/2214400-zware-ddos-aanvallen-wie-wat-waar-en-waarom.html> accessed 6 February 2018.

Walree T F, ‘De vergoedbare schade bij de onrechtmatige verwerking van persoonsgegevens’ (2017) 7172 Weekblad voor Privaatrecht, Notariaat en Registratie 921, 926.

Waters R and Kuchler H, ‘Intel and Microsoft sow confusion over security flaw’ *The Financial Times* (San Francisco, 11 January 2018) <https://www.ft.com/content/f31e0b2a-f6f6-11e7-88f7-5465a6ce1a00> accessed 12 January 2018.

Weber R and Studer E, ‘Cybersecurity in the internet of things: Legal aspects’ *Computer Law and Security Review* 32 (2016) 715.

Webopedia, ‘Authentication’ <https://www.webopedia.com/TERM/A/authentication.html> accessed 5 December 2017.

Weinberger M, ‘Google had to disable a feature on its new $50 smart speaker after the gadget listened in on some users’ (*Business Insider*, 10 October 2017) < http://www.businessinsider.com/google-home-mini-accidentally-listening-to-users-2017-10?r=UK&IR=T> accessed 22 February 2018.

Wenzel S L, ‘Not Even Remotely Liable: Smart Car Hacking Liability’ (2017) University of Illinois Journal of Law, Technology and Policy 49.

Whitaker S, *Liability for Products* (Oxford University Press 2005).

Wollerton M, ‘Here's what happened when someone hacked the August Smart Lock’ (*CNet*, 25 August 2016) < https://www.cnet.com/news/august-smart-lock-hacked/> accessed 6 February 2018.

Written Question No 706/88 by Gijs de Vries to the Commission: Product liability for computer programs, Official Journal (OJ) C 114/42.

Wuyts D, ‘The Product Liability Directive – More than Two Decades of Defective Products in Europe’ (2014) 5 *Journal of European Tort Law* 1.

Zeng E et al., ‘End User Security & Privacy Concerns with Smart Homes’ (Symposium on Usable Privacy and Security, Santa Clara, California, July 12-14 2017).

Zittrain J L, *Future of the Internet and How to Stop it* (New Haven and London, Yale University Press 2008).

Legal texts

European Union

European Union Charter of Fundamental Rights [2012] OJ 326/02 (Article 7, 8, 38 and 47).

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 [1985] OJ L 210/29 (Product Liability Directive)

Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999 amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products [1999] OJ L 141/20.

Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety [2001] OJ L11/4 (Product Safety Directive).

Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market [2005] OJ L 149/22 (Unfair Commercial Practices Directive).

Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights [2011] OJ L 304/64 (Consumer Rights Directive).

Proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content COM(2015) 634 final (proposal for a directive on digital content).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L 119/1 (General Data Protection Regulation, GDPR).

Council of Europe

European Convention of Human Rights, Article 6, 8 and 13.

Table of cases

Court of Justice of the European Union

Case 152/84 *M. H. Marshall v Southampton and South-West Hampshire Area Health Authority (Teaching)* [1986] ECR 723.

C-300/95 *Commission v. United Kingdom* [1997] ECR I-02649.

Case C-210/96 *Gut Springenheide* [1998] ECR I-4657.

Case C-203/99 *Henning Veedfald* [2001] ECR I-03569.

Case C-402/03 *Skov v Bilka* [2006] ECR I-199.

Case C-127/04 *Declan O'Byrne v Sanofi Pasteur MSD Ltd and Sanofi Pasteur SA* [2006] ECR I-01313.

Case C-285/08 *Société Moteurs Leroy Somer v Société Dalkia France and Société Ace Europe* [2009] ECR I-04733.

Case C-495/10 *Centre hospitalier universitaire de Besançon v Thomas Dutreux and Causse primaire d'assurance maladie du Jura* [2011] ECR I-14155.

Case C-470/12 *Pohotovost/Vasuta* [2014] ECLI:EU:C:2014:101.

Joined Cases C-503/13 and C-504/13 *Boston Scientific Medizintechnik* [2015] ECLI:EU:C:2015:148.

The Netherlands

Hoge Raad 30 juni 1989, *Halcion*, NJ 1990, 652.

Hoge Raad 24 december 1993, *Leebeek / Vrumona*, ECLI:NL:HR:1993:ZC1197.

Hoge Raad 9 juli 2004, *Groningen / Lammerts*, NJ 2005, 391.

Hof ‘s Hertogenbosch 1 September 2009, JA 2010/7 (annotated by I. van der Zalm).

U.S. Case law

Olmstead v. United States, 277 U.S. 438 (1992).

Seegers Grain Company v. US Steel Corporation 577 N.E.2d 1364, 1370 (Ill 1991).

Escola v. Coca Cola Bottling Co., 150 P.2d 436, 24 Cal. 2d 453, 1944 Cal.