**QUEEN'S
UNIVERSITY
BELFAST**

Cybersecurity in a post-data environment: Considerations on the regulation of code and the role of producer and consumer liability in smart devices

Nash, I. (2021). Cybersecurity in a post-data environment: Considerations on the regulation of code and the role of producer and consumer liability in smart devices. *Computer Law and Security Review*, 40, [105529]. <https://doi.org/10.1016/j.clsr.2021.105529>

Published in:
Computer Law and Security Review

Document Version:
Peer reviewed version

Queen's University Belfast - Research Portal:
[Link to publication record in Queen's University Belfast Research Portal](#)

Publisher rights

Copyright 2021 Elsevier Ltd.

This manuscript is distributed under a Creative Commons Attribution-NonCommercial-NoDerivs License

(<https://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits distribution and reproduction for non-commercial purposes, provided the author and source are cited.

General rights

Copyright for the publications made accessible via the Queen's University Belfast Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy

The Research Portal is Queen's institutional repository that provides access to Queen's research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person's rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact openaccess@qub.ac.uk.

Cybersecurity in a post-data environment: Considerations on the Regulation of Code and the role of Producer and Consumer Liability in Smart Devices

1 Introduction

Over the past decade, there has been exponential growth in so-called ‘Internet of Things’ or ‘Smart’ Devices. These devices, hereafter referred to as ‘Smart Devices’, are consumer products which have both a CPU and an internet connection and combine their physical operations with software activity; normally augmenting the device's internal system by accessing cloud services.¹ Urquhart, Lodge and Crabtree (2018) note how soon there will be billions of Smart Devices in use as we are in the early stages of an exponential growth phase of such products and that these products are becoming common in all aspects of daily life.² Butler (2017) notes that it was forecast that, by 2020, there would be c. 26 billion Smart Devices globally, while Lynkova (2019) states that this number was reached in August 2019.³ It is forecast by the International Data Corporation that the number of smart devices will exceed 40 billion by 2025 and accordingly, although the market for Smart Devices can be considered relatively new, it must be viewed as an established and robust market.⁴

The connected nature of a Smart Device means that the manufacturer must ensure the operations of the physical product are safe for consumers as well as ensuring that the software run on the device is secure. However, the primary questions relating to Smart Devices within the academic legal environment have mostly focussed on issues relating to data protection and consumer privacy whereas there has been a much smaller focus on the questions of cybersecurity and liability following the compromise and subversion of the device by a third party. Some authors⁵ argue that the developers of the Smart Device bear the primary, if not the sole, responsibility for the cybersecurity of their products while other authors believe responsibility is more a function of a multi-stakeholder model.⁶ However, when examining the question of liability arising from the subversion of a product owing to a failure of the security of the software, there appears to be little in the literature examining whether liability should be assigned to either the developers or users of the Smart Device and how to assign liability in the context of either a failure of cybersecurity or a more general programming defect.

¹ Cloud services are where a device will connect with a remote server and either pull data down to the device, or will send data generated by the device to the cloud.

² Lachlan D Urquhart, Tom Lodge and Andy Crabtree, ‘Demonstrably Doing Accountability in the Internet of Things’ (2018) 27 *International Journal of Law and Information Technology* 1, 2.

³ Alan Butler, ‘Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?’ (2017) 50 *University of Michigan Journal of Law Reform* 913; Darina Lynkova, ‘IoT Statistics and Trends to Know in 2020’ (*Leftronic Blog*, 2019) <<https://lefronic.com/internet-of-things-statistics/>> accessed 23 March 2020.

⁴ International Data Corporation, ‘The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast’ (2019) <<https://www.idc.com/getdoc.jsp?containerId=prUS45213219>> accessed 23 March 2020.

⁵ See, e.g., PA Alces, ‘W(h)lther Warranty: The b(l)oom of Products Liability Theory in Cases of Deficient Software Design’ (1999) 87 *CALIFORNIA LAW REVIEW* 269; Daniel Boos and others, ‘Controllable Accountabilities: The Internet of Things and Its Challenges for Organisations’ (2013) 32 *Behaviour & Information Technology* 449; Broder Kleinschmidt, ‘An International Comparison of ISP’s Liabilities for Unlawful Third Party Content’ (2010) 18 *International Journal of Law and Information Technology* 332; Chris Fennell and Rick Wash, ‘Emotional Impact: How Stories Affect Password Behavior’ (2017).

⁶ See, e.g., Butler (n 3); Liis Vihul, ‘The Liability of Software Manufacturers for Defective Products’ (2014) 2 *Tallin Papers* <<https://ccdcoe.org/library/publications/the-liability-of-software-manufacturers-for-defective-products>>.

The first premise of this paper is that software developers need to be held accountable for the vulnerabilities in their code. It has been noted by Schneier (2003) that software developers who ship code quickly, but at the cost of vulnerabilities, are rewarded by the market while companies who have a slower release cycle but develop more secure code are punished by the market.⁷ This outcome is enabled due to the lack of liability which software firms face when producing software and accordingly, only a reform of liability will result in software development firms increasing the standard of cybersecurity of their products.

The second premise of this paper is to re-evaluate the principles of product liability for Smart Devices from a cybersecurity perspective, including damages caused by the device to third parties, arising from the compromise of vulnerabilities found in the Smart Device. This paper outlines, for the first time, a novel liability framework which is based upon the tort of Negligence and incorporates the principles of robust cybersecurity principles, the nature of the threat posed by compromised Smart Devices and the roles of the victim, producer and owner of Smart Devices in ensuring the maintenance of cybersecurity.

2 Overview of Cybersecurity

The relevance and importance of cybersecurity in legal theory should be evaluated within the context of the changing nature of computing. It is a commonly held view that when someone uses a computer, their actions are seen as virtual, existing only in cyberspace, and therefore not 'real' (with the exception of copyright infringements).⁹ Consequently, when people thought about cybersecurity and the risks arising from a breach of a system, the focus was on the data contained within the system, and not about the risks of damage in the real world.

However, since the advent of fast, cheap and generally available internet access, there has been a change in products from devices which may have contained a simple and standalone operating system, to a connected computer which carries out an action. It is this change which has resulted in the advent of the Smart Device.¹⁰ Furthermore, as noted by Schneier (2018), computers by their nature are extensible, meaning that the potential outcome of their use is not limited to their original goals.¹¹ Thus, we are now in an era where everyday items such as cars, kettles, pens, pace-makers, pet collars, ovens and thermostats, which we have coupled to computers and connected to the internet, can now become tools which can be used in potentially unexpected ways by unexpected people. In addition to the normal rigorous development process that a consumer device must go through, these Smart Devices now must be additionally designed to operate when connected to the internet, to be cybersecure and to prevent third party agents from getting either access to, or control over the device. However, unlike ordinary products, which have clear and well understood liability principles in relation to defects, failures and consumer safety, there is no such framework for the software element of Smart Devices.

Friedman and Allan (2014) note that there are only three things that can be done to a computer,¹² you can steal its data, misuse credentials, and hijack resources. However, in an era of extensible, internet-connected and computer-controlled devices, misused credentials can now destroy nuclear

Bruce Schneier, 'Testimony before the Subcommittee on Cybersecurity, Science, and Research and Development' (*Schneier on Security*, 25 June 2003)
<https://www.schneier.com/essays/archives/2003/06/testimony_before_the.html> accessed 23 July 2020.

¹⁰ Bruce Schneier identifies this inflection point as 2007, when the iPhone was released, and refers to this, post-data environment as Internet+.

¹¹ Bruce Schneier, *Click Here to Kill Everybody* (WW Norton & Company 2018).

Peter W Singer and Allan Friedman, *Cybersecurity & Cyberwar* (Oxford University Press 2014) 39.

centrifuges,¹³ redirect satellites,¹⁴ and shut down global shipping facilities.¹⁵ Therefore, it is clear how cybersecurity has evolved beyond just the protection of intangible data to encompass physical security, and the potential damages arising from a subverted device mean that the legal treatment of cybersecurity is now a topic of increasing importance.

From a more general perspective, the speed at which the nature of cyberthreats are evolving at can be seen over the past decade. Taking, for example, the Stuxnet worm, which is widely believed to have been developed by two nation states over a period of five years and was deployed in 2010 against a specific range of targets. Stuxnet is seen as the first example of a cyberattack against a physical target. The sophistication of the worm was such that it was limited to targets which were considered high priority by nation states, and, as such, would not have represented an immediate threat to the average internet user. Yet, within seven years of the release of Stuxnet, ransomware programs such as *WannaCry* and *NotPetya* had been developed and were able to shut down critical global infrastructure, such as hospitals,¹⁸ manufacturing plants,¹⁹ and ports,²⁰ on an unprecedented global scale. Bruce Schneier notes how “today’s top-secret programs become tomorrow’s PhD thesis and the next day’s hacker tools”, and unfortunately this has proven to be true, as cybercriminals can now conduct a cyberattack against critical and global infrastructure using widely available tools.²¹ The evolution of cyberthreats is also supported by a lax approach taken to cybersecurity by the majority of computer operators. Both *WannaCry* and *NotPetya* used an exploit called *EternalBlue*, which is based on a vulnerability in various versions of Microsoft Windows.²² Despite both of these exploits taking place in 2016 and 2017, and Microsoft releasing a patch to prevent the future use of *EternalBlue* in 2017, Perlroth and Shane (2019) note how the city of Baltimore was successfully attacked in 2019 by a ransomware worm that gained access via the *EternalBlue* exploit,²³ two years after a patch had been developed. This demonstrates how responsibility for cybersecurity does not lie solely with the producer, and that failures by users to deploy patches which have been developed to fix vulnerabilities can result in substantive issues from both a data and physical perspective.

¹³Kim Zetter, ‘An Unprecedented Look at Stuxnet, the World’s First Digital Weapon’ (*Wired Magazine*, 3 November 2014) <<https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>> accessed 23 March 2020.

Deborah Housen-Couriel, ‘Cybersecurity Threats to Satellite Communications: Towards a Typology of State Actor Responses’ (2016) 128 ACTA ASTRONAUTICA 409.

¹⁵Andy Greenberg, ‘The Untold Story of NotPetya, the Most Devastating Cyberattack in History’ (*Wired Magazine*, 22 August 2018) <<https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>> accessed 23 March 2020.

¹⁸Russell Brandom, ‘UK Hospital Hit with Massive Ransomware Attack’ (*The Verge*, 5 December 2017) <<https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin>> accessed 23 April 2020.

Andrew Liptak, ‘Renault Shut down Several French Factories’ (*The Verge*, 14 May 2017) <<https://www.theverge.com/2017/5/14/15637472/renault-nissan-shut-down-french-uk-factories-wannacry-cyberattack>> accessed 23 April 2020.

Greenberg (n 14).

Bruce Schneier, *Data and Goliath* (WW Norton & Company 2015).

²²The vulnerability targeted Microsoft’s Server Message Block which was present in unpatched versions of, *inter alia*, Windows Vista, Windows 7, Windows 8.1 and Windows 10. Full details on the exploit can be found at: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144> (accessed on 24/03/2020)

²³Nicole Perlroth and Scott Shane, ‘In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc’ (*The New York Times*, 2019) <<https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html>> accessed 23 March 2020.

3 Cybersecurity and Legislative Efforts

Is it worth trying to regulate the cybersecurity of Smart Devices? Anderson et al. (2019) note that while cybercrime is ubiquitous,²⁴ there is clear evidence that when security standards improve there can be a marked decrease in specific instances of cybercrime as easier targets are sought, and therefore, if Smart Devices can be secured, cybercriminals will seek easier targets to subvert. From a jurisprudential perspective, Harvey (2017) notes that when a legal system is faced with new technology,²⁵ it may struggle to maintain certainty which has been established through existing principles, and changes may be made through a case-by-case basis. This is a slow process and one that can lead to confusion and apprehension by those who are effected by the principles under consideration. Accordingly, if a clear and comprehensive legislative framework can be developed to improve cybersecurity of Smart Devices, which encourages manufacturers to keep their devices secure, a reduction in cybercrime involving Smart Devices can be expected.

The canonical definition of cybersecurity, as outlined by Singer and Friedman (2004) is the measures taken to ensure the confidentiality, integrity and availability of information.²⁶ However, in order for there to be effective legislation with regard to software in general, and Smart Devices in particular, it must be recognised that there are specific, technical measures which must be taken by software developers (e.g., following secure coding principles, shipping with unique passwords, developing and deploying updates) as well as measures which users must follow (e.g., deploying updates) in order to achieve an increase in cybersecurity standards.

The inclusion of cybersecurity nomenclature within legislation has been increasing over the past decade, and is welcome. The European Union has passed the 2019 Cybersecurity Act,²⁷ and the Network and Information Systems Directive,²⁸ which set a permanent mandate for the European Union Agency for Cybersecurity (ENISA) and require member states to establish plans to secure their critical infrastructure from cyberattacks respectively. While these are very welcome pieces of legislation, and even when taking into account how the 2019 Regulation creates the framework for a voluntary cybersecurity labelling framework, their impact on the cybersecurity of consumer devices is *de minimis* at best. Within EU legislation, there are no objective or minimal standards of cybersecurity defined or mandated, and with the exception of the General Data Protection Regulation,²⁹ there are no consequences for firms whose software contains vulnerabilities. One partial exception to this are the 2019 Digital Content and Digital Service Directive,³⁰ and the 2019 Update to the Sale of Goods Act.³¹ These directives do have reference (of a sort) to cybersecurity and in theory enable a consumer to take action for breach of contract in the event of a vulnerability, and are discussed in more detail in section 6 below.

The legislative efforts outside the European Union are similar. There have been, for example, a number of pieces of legislation enacted in the United States of America which include references to cybersecurity, such as *The Health Information Portability and Accountability Act of 1996*,³² *The Financial Modernisation Act of 1999*,³³ *The Homeland Security Act of 2002*,³⁴ *The Cybersecurity*

Ross Anderson and others, 'Measuring the Changing Cost of Cybercrime' [2019] Workshop on the Economics of Information Security (WEIS).

²⁵David Harvey, *Collisions in the Digital Paradigm: Law and Rule Making in the Internet Age* (Bloomsbury Publishing Plc 2017).

²⁶Singer and Friedman (n 12) 35.

²⁷Regulation 2019/881

²⁸Directive 2016/1148

²⁹Regulation 2016/679

³⁰Directive 2019/770

³¹Directive 2019/771

³²Public Law 104-191 (1996)

³³Public Law 106-102 (1999)

³⁴Public Law 107-296 (2002)

Research Act of 2002,³⁵ and *The Federal Information Management Act of 2002*.³⁶ However, in contrast to the European Union, there is no singular cybersecurity bill in the US and instead, various federal institutions have responsibility for aspects of cybersecurity, but there is no single entity which has overall responsibility. Furthermore, the majority of the legislation outlined above only refers to devices which are operated by the Federal Government; there is no legislation which sets out minimum standards of cybersecurity for devices owned or operated by private individuals or businesses. It is therefore clear that cybersecurity has yet to be effectively (and predictably) dealt with either on a judicial or legislative basis. Furthermore, there are currently no pieces of enacted legislation which impose a duty of care or other liability apportionment mechanisms to software or Smart Device manufacturers, and it is for this reason that such companies are rewarded for the quick shipping of software containing vulnerabilities instead of releasing more secure software and ensuring that it remains secure after sale.

The impact which this current and suboptimal state of affairs has on cybercrime needs to be fully understood. It is the vulnerabilities in the code bases of, *inter alia*, Smart Devices which are exploited by cybercriminals to conduct their attacks. The scope for damage caused by cybercriminals is much greater than 'ordinary' crime. Brenner (2004) notes that the key distinction between acts of cybercrime and physical crime is a lack of a physical nexus and direct proximity between the victim and the criminal,⁴² as well as the perpetrator not being subject to physical limitations which are present during the commission of a 'normal' crime. For this reason, cybercrime should not be viewed merely as a linear extension of ordinary crime, but as a force-multiplier as criminals are now able to utilise distributed networks of compromised computers towards a specific (but not necessarily singular) goal. Criminals are now able to exploit the connected networks of machines to escape the physical nexus restriction, and exploit the extensible and replicable nature of computers operating either in parallel or in series to commit multiple instances of crime through a single action. Krebs (2019) notes how one particular strain of ransomware, a crime whereby a computer system is accessed, and its files are encrypted until a ransom is paid, called GrandCrab, has generated over two billion dollars in ransom payments.⁴³

Ransomware is an excellent example of the new dangers arising from the modern tool of cybercrime which can self-replicate and compromise other systems, either within the compromised network or external to it, without manual intervention by its creator. In what non-cyber environment would a criminal enterprise be able to engage in repeated, self-perpetuating acts of ransom demands, ultimately generating payments in excess of two billion dollars? Furthermore, ransomware by its nature is only an 'intermediate' physical crime, as the outcome of ransomware is the denial of access to both data and a service. We have not yet reached an environment whereby cybercriminals extort payments from the manufacturers of Smart Devices in order to prevent them from causing damage across multiple continents to their customer's home, but such a hypothesis is no longer far-fetched given the capabilities and actions of cybercriminals and the speed of development of malicious software.

4 The Nature of Software Vulnerabilities

In order to ensure a sound and robust legal treatment of cybersecurity, there must first be clarity around how computers are subverted and what can be done to prevent such subversion. As already mentioned above, it is important to note that cybersecurity is a concept that is relevant for both the developers of software, as they must develop the software according to robust cybersecurity

³⁵Public Law 107-355 (2002)

³⁶Public Law 107-347 (2002)

Susan W Brenner, 'Towards a Criminal Law for Cyberspace: Product Liability and Other Issues' (2004) 5 *Journal of Technology Law and Policy*.

Brian Krebs, 'Who's Behind the GandCrab Ransomware?' (*Krebs on Security*, 2019)

<<https://krebsonsecurity.com/2019/07/whos-behind-the-gandcrab-ransomware/>> accessed 23 March 2020.

principles, and for the users of software, who should follow cybersecurity guidelines to ensure that systems remain secure. When software is being developed, errors may be introduced to the code which can create a *vulnerability* which could, in theory, create an opportunity for a third-party to engage in unauthorised use or compromise of the software. However, in many cases such vulnerabilities are theoretical and only when there is a mechanism which will allow the third party to leverage the error in code can it be considered as an *exploitable vulnerability* (hereafter referred to as an ‘exploit’). Exploits are active threats to software and are discovered and reported by, *inter alia*, security researchers, users, other developers, government departments and the engineers themselves. Exploits are usually also reported to third party databases, with the most commonly used, according to Sánchez et al. (2020),⁴⁴ being the MITRE Corporation's Common Vulnerability and Exposure (CVE) database which is a free and open-access resource.⁴⁵ It is important to note that cybercriminals can also discover exploits, but it is not the norm that they will report these discoveries to programming communities. Sabottke et al. (2015) examine this topic in some detail and find that social media accounts can be a source of discovery for previously unknown exploits and threats as the cybercriminals can share this knowledge with other cybercriminals, usually with the aim of selling access to the exploit.⁴⁶

Exploits can be further subdivided into two categories; *known exploits*, which are vulnerabilities that have been reported and are therefore ‘known’ to the programming industry, and *zero-day exploits*, which are vulnerabilities which have been discovered by a third party, but which are not known to the developer of the software. This differentiation is crucial as if an exploitable vulnerability is known, it means that the software developers can augment the compromised software to remove the exploit. This augmentation is normally called a ‘patch’ and comes in the form of an update which can either be applied automatically or applied manually by the user. Bilge and Dumitras (2012) note the dangers of zero-day attacks and emphasize that, by their nature of being unknown, it is not possible to patch and protect systems against the threat until it becomes known and the developers have had sufficient time to develop a patch.⁴⁷ August, Dao and Kim (2019) cover in detail the patching behaviour (or lack thereof!) of users and also note that, in order to develop a patch, there must be extensive testing conducted by both the developer and the user, to ensure that the patch does not cause a conflict with other pieces of software.⁴⁸ Time-frames of between 30 and 180 days are discussed as being ‘acceptable’ from the time of discovery of the exploit to the successful deployment of the patch.

Discoverability of these exploits has been made easier by tools which enable to cybercriminals to find devices which contain vulnerabilities. Lin and Bergmann (2016) outline how there are now publicly available and fully legal search engines such as Shodan and Censys, which are designed to find Smart Devices that are connected to the internet and return information about their operating systems.⁴⁹ It is clear how these systems allow third parties to find Smart Devices which could be subverted by either a known or a zero-day attack. However, for the first time in an academic legal environment, it is proposed to establish if the compromise of a system was a result of a ‘known’ or ‘unknown’ exploit.

MC Sánchez and others, ‘Software Vulnerabilities Overview: A Descriptive Study’ (2020) 25 Tsinghua Science and Technology 270.

⁴⁴ <https://cve.mitre.org/>

Carl Sabottke, Octavian Suciú and Tudor Dumitras, ‘Vulnerability Disclosure in the Age of Social Media: Exploiting Twitter for Predicting Real-World Exploits’ (USENIX Association 2015) <<https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/sabottke>>.

Leyla Bilge and Tudor Dumitras, ‘Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World’ (ACM 2012) <<http://doi.acm.org/10.1145/2382196.2382284>>.

Terrence August, Duy Dao and Kihoon Kim, ‘Market Segmentation and Software Security: Pricing Patching Rights’ [2019] Management Science.

Huichen Lin and Neil W Bergmann, ‘IoT Privacy and Security Challenges for Smart Home Environments’ (2016) 7 Information 44.

Furthermore, it is a common misconception among non-technical commentators that when developers write code, they operate within what can be perceived as a ‘partial vacuum’; that code written for one product is independent of other computer software programs.⁵⁰ This is not generally correct as developers will often rely on shared software components when they develop software. These components are third party objects which are written by other developers and provide pre-built functionality which can be used when developing software. Examples of components would include *react.js*, a javascript library used for creating user interfaces. This component was developed in 2013 and is currently maintained by Facebook. Analysis of *React.js* usage by Krotoff (2019) on GitHub, a repository used by over forty million professional and amateur developers to store either open-source or private code, showed that, in 2019, c. 50,000 scripts built which depended on React were built, and it was used in over two million projects.⁵¹ Another example is *node.js* which is a javascript environment for which engineers create scripts which are then executed by node.js on both server side and client side applications and is maintained by the Node.js Foundation. Node.js was first released in 2009, and analysis by HostingTribunal (2020) shows how it is used by large ecommerce sites such as Netflix, LinkedIn, AliExpress, eBay and PayPal.⁵² From these examples we can see not only must software engineers ensure that their own code is free from vulnerabilities, but that for their software to be secure, they must ensure that any third-party components are also vulnerability free. For components which are written and maintained by large foundations, user-groups or organisations, this is a relatively straight-forward process however it is a common occurrence in software development that a component used by a developer is no longer actively maintained and therefore no longer being actively patched.

Finally, it is important to note that the compromise of a system can arise from a lack of security rigour during the development process. There are a number of Smart Devices that are shipped with well-known default passwords or with no passwords at all. From a technical perspective, this actually is not a vulnerability as discussed above *per se* but instead can be considered as a total lack of cybersecurity rigour. Acarali et al. (2019) highlight how *Mirai*,⁵³ one of the most successful botnets which had, at its peak, over 600,000 devices subverted, was able to source new nodes by scanning for new devices and then trying a dictionary attack of 62 commonly used default user-names and passwords. Lin and Bergmann (2016) show how,⁵⁴ during the course of their work, they have identified hundreds of Smart Device developers who do not provide any updates to their devices post sale which means that such devices, which will be connected to the internet but will never be patched to remove any vulnerabilities can be accessed by cybercriminal who has knowledge of a relevant exploit and can find the device’s IP. The authors also note that many devices need to have their security settings configured manually by the purchaser, who would not be considered an expert when it comes to optimising security.

From the above, it can be seen how the analysis of software security vulnerabilities from a technical perspective is a multi-dimensional problem and not all of the code which will be ultimately be compiled will be written, or perhaps even fully understood by the developer. The recognition of this problem is not one that has been often been found in legal texts when it comes to the analysis of liability arising from the failure of cybersecurity and therefore, has not been addressed in legislation. However, it forms a fundamental part of the model which is proposed in this paper.

See, e.g., Jennifer A Chandler, ‘Information Security, Contract and Liability’ (2009) 84 Chicago-Kent Law Review; Se-Hak Chun, ‘E-Commerce Liability and Security Breaches in Mobile Payment for e-Business Sustainability’ (2019) 11 SUSTAINABILITY 715.

Tanguy Krotoff, ‘Front-End Frameworks Popularity (React, Vue, Angular)’ (12 December 2019) <<https://gist.github.com/tkrotoff/b1caa4c3a185629299ec234d2314e190>> accessed 4 May 2020.

HostingTribunal, ‘62 Node JS Stats That Prove Its Awesomeness’ (2020) <<https://hostingtribunal.com/blog/node-js-stats/>> accessed 4 May 2020.

Dilara Acarali and others, ‘Modelling the Spread of Botnet Malware in IoT-Based Wireless Sensor Networks’ (2019) 2019 SECURITY AND COMMUNICATION NETWORKS 1.

⁵⁴Lin and Bergmann (n 41)

5 The Threats posed by Compromised Smart Devices

If a third party compromises a Smart Device, the compromise can generally be assigned to one of two categories; either the compromise effects the owner of the device (for example, by stealing data, damaging property, shutting down the device or causing harm to the network to which the device is connected) or to use the compromised device to attack another individual or business. The latter frequently occurs where the device becomes part of a 'botnet' which, as described by Chandler (2006) is a portmanteau of 'Robot' and 'Network' and is where a large number of devices are subverted to follow the commands of the botnet operator.⁵⁵ Damage caused to a third party is an example of which is of particular interest to the author of this paper as if personal data relating to the owner of device is stolen by the botnet operator, there are sufficient avenues for recovery of damages under the General Data Protection Regulation,⁵⁶ and if direct physical damage occurs, damages may be recovered via tort, whereas it is generally not possible to recover damages from either the developer or operator of a third-party device which engaged in a cyberattack while under the control of a cybercriminal.

Bugeja, Jacobsson and Davidsson (2017) outline the nature of threats posed to and by Smart Devices.⁵⁷ The authors focus more on physical damage which can be caused by the compromised device; however, excluding corporate espionage, the focus is more on how nation-state, terrorist hackers and hacktivists can cause widespread damage to a locality. Botnets are discussed briefly but only in the context of sending spam, which is at odds with trends in cybersecurity reports over the past few years. The Mirai botnet was able to shut down individual websites, such as cybercrime commentator Brian Krebs's *Krebs on Security*'s website as well as the critical infrastructure provider Dyn, which caused large number of sites hosted in Europe and North America to be unavailable to internet users. Vlajic and Zhou (2018) note that the botnet industry has become so sophisticated that botnets can now be rented by cybercriminals on an hourly basis,⁵⁸ while the average cost of a DDOS attack can be up to \$1.5 million per attack, comprised of both loss of earnings and damaged network assets.⁵⁹

Furthermore, we now inhabit a world where common and routine, yet essential actions are now dependent, wholly or in part, on access to data which is stored on remote computers. Normal communication is now conducted via mobile phones, email and social media platforms. Access to these systems requires three key elements: a device from which we can engage with the systems, an internet connection which allows a two-way conversation with these systems, and the servers in which these systems reside must be functioning. All these elements represent potential vulnerabilities, and this risk can be seen as both a hybrid of the physical and virtual environments. Therefore, demonstrating how cybersecurity is required to ensure continued access to computer systems, and to essential services such as banking, communications and healthcare. It must be clearly noted how Smart Devices were the main components of Mirai, the world's largest (at the time) botnet, and accordingly vulnerabilities in Smart Devices have a direct effect upon a user's personal safety, the safety of internet traffic as well as upon critical networks such as power grids.

6 Vulnerabilities from a legal perspective

As observed above, it is clear that when examining the compromise of a Smart Device, responsibility for the compromise can be determined by examining the nature of the vulnerability which was

Jennifer A Chandler, 'Liability for Botnet Attacks' (2006) 5 Canadian Journal of Law and Technology. Regulation 2016/679

Joseph Bugeja, Andreas Jacobsson and Paul Davidsson, 'An Analysis of Malicious Threat Agents for the Smart Connected Home' [2017] 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) 557.

Natalija Vlajic and Daiwei Zhou, 'IoT as a Land of Opportunity for DDoS Hackers' (2018) 51 COMPUTER 26.

⁵⁹Butler (n3)

exploited. This has no bearing on any criminal actions and it is clear that if a Smart Device is subverted, the instigator of the subversion will be guilty of a criminal offence such as those outlined in Sections 1, 2, 3 and 3ZA of the Computer Misuse Act 1990 in the UK or Sections 2 and 3 of the Criminal Justice (Offences Relating to Information Systems) Act 2017 in the Republic of Ireland. Within the EU, the Cybercrime Directive,⁶¹ is the source for member states' specific criminal statutes which relate to cybercrime. However, there is currently no criminal legislation which takes the mode of the compromise into account.

If damages are sought, the claimant must raise an action either through tort or through some form of statutory relief, and these civil claims may examine the nature of the subversion in order to determine if liability should be assigned, and if so, to whom it should attach. However, to date and with the exception of data protection infringements, it is very difficult for a plaintiff to successfully bring a civil action following the commission of a cybercrime involving a Smart Device against either the manufacturer of the device or the owner of the device (if the plaintiff was an injured third party). If the plaintiff is the owner of the device, action may be taken against the device manufacturer or the software producer and the modes of claim are:

- Products Liability
- Sales of goods legislation
- Negligence

However, if the plaintiff is an injured third party, they may seek recovery from both the owner of the device, as well as the manufacturer or software developer and their claim will be limited to one of negligence.

6.1 Products Liability

When examining failure in a product, there are several avenues through which a claimant can seek relief. There is a statutory basis for seeking recovery through civil action under product liability legislation,⁶² which ensures that the producer of the product is liable in tort if the product fails to provide the safety which the owner should reasonably expect. There is a further contract basis also, as most countries have statutes which require that goods are of merchantable quality.⁶³ There is a common law basis also, as outlined in *Power v Bedford Motor Company & Another*,⁶⁴ and in *Duffy v Rooney & Dunnes Stores (Dundalk) Ltd*,⁶⁵ that a person can recover damages from the producer of a product if they are able to demonstrate that 1) there was a duty of care between the producer and the user, 2) there was a breach of the duty of care and 3) the breach of this care was the reason that the damage was caused. In the case of *Power*, the plaintiff brought the case against a garage following the sale of a car which had damage (which the garage was aware of) to the steering linkage and it was held they were liable for the death of the plaintiff following a crash, while in *Dunnes*, the claim against the second defendant, although failing to establish that Dunnes were liable for the injuries caused to the defendant following a piece of clothing catching fire, demonstrated the mechanism and the above requirements for bringing a claim through common law.

It is clear that producer's liability, as it stands today, is the result of balancing both the problems and issues facing a manufacturer, and the expectations of the consumer in terms of both product safety and durability. Manufacturers of goods need to be able to produce their wares on an economic basis while consumers are entitled to assume that these goods will work as intended for a reasonable period of time. As a product gets older and has been used regularly, the consumer's potential to claim against

⁶¹Directive 2013/40/EU

⁶² e.g., Directive 85/374/EEC

⁶³ e.g., Sale of Goods and Supply of Services Act 1980 (Sale of Goods Acts) in the Republic of Ireland

⁶⁴ [1959] IR 391

⁶⁵ [1997] IEHC 102

the manufacturer begins to decay. Section 19 of the European Sales of Consumer Goods Directive provides all consumers with a guarantee for at least 24 months from purchase (albeit each Member State can decide at what time period after the sale the liability switches from strict to normal, requiring the consumer to demonstrate the specific point of failure as opposed to just demonstrating that the item no longer works),⁶⁶ as well as when the consumer's use of the product and any associated 'wear and tear' becomes relevant in determining the outcome of the claim.

Products which rely in part or in full on software do not fit as easily into this category as unlike a physical good, the producer is still (or at least in theory, should be) able to access and deploy amendments to the software after the product has been manufactured, shipped and sold, and unlike a physical product, the software will not be subject to wear and tear, but may subsequently turn out to have a vulnerability which would require fixing. Unlike a product recall, or the return of a faulty product, the cost to the manufacturer to access and update a product, is effectively trivial, while the complications arising from ensuring that the software of a connected device is secure are much higher than with purely physical goods.

Recent developments in the UK,⁶⁷ and in the EU,⁶⁸ have attempted to bridge this gap with the creation of a digital product. The UK Act defines digital content as "data which is produced and supplied in digital form", while the EU Directive definition is somewhat more specific as it defines digital content, digital service and goods with digital elements. The question as to whether a Smart Device falls under Sale of Goods legislation or the Digital Content Directive,⁶⁹ is addressed in the 2019 Update to the Sale of Goods Directive.⁷⁰ This directive states that goods which have digital content or services or are inter-connected with digital goods in a manner that removal of the digital aspect would render it unable to perform its functions are not covered by the Digital Content and Digital Services directive, but rather the Sale of Goods Directive.

This Sale of Goods Directive broadly reflects provisions of the European Product Liability Directive,⁷² in that the producer is responsible for vulnerabilities which were known about at the time of delivery, although Art 10 (2) does make reference to the fact that the provider is required to ensure that the device remains functional for either two years, or as long as was stated in the sales contract, whichever is longer. There is no objective requirement for the producer to develop patches for vulnerabilities, unless this has been agreed in the sales contract. Reference is made to 'security updates' in the Directive, but this term is not defined. As with the 1985 Product Liability Directive, liability for vulnerabilities which were existed prior to shipping would be appear to be straight forward to apply under the 2019 Directive, but liability for vulnerabilities which occur after delivery and which don't hinder functionality will be harder to attach, unless the seller has already committed themselves to do so.

The nature of software vulnerabilities is such that they can arise subsequent to the development of the software, and the vulnerability can apply to either the core code of a program, or within libraries which are used by the product but not written by its developers. This is a critical difference between software and ordinary products, as when a physical product has a defect, it arises normally from an error that occurred during the manufacturing process, such as a batch of circuit boards being defective due to a defect in the resin used in that batch only. The defect may not be visible and may not impact the user immediately, but it is an inherent part of the product and can be compared to other identical products which were manufactured in different batches but do not contain the defect, so there is a clear difference between the faulty and faultless product. Such a distinction is not possible for

⁶⁶ 1999/44/EC

⁶⁷ Consumer Rights Act 2015

⁶⁸ Directive 2019/2161

⁶⁹ Directive 2019/770

⁷⁰ Directive 2019/771

⁷² Directive 85/374/EEC

software, as there is a single code-base which is used for all products and the production process ends once the code-base is complete. Accordingly, exploits in Smart Devices would be considered a defect in design, as opposed to a defect in a given device.

In order to assess a claim on a design defect basis, there are two tests which the courts have developed. There is the consumer expectations test, and a danger utility test. There are a number of criticisms surrounding the use of the consumer expectations test when evaluating software design. Hecht (2005) outlines how American courts have taken the view that a consumer does not have the requisite knowledge in order to validly state their expectations when it comes to complex devices.⁷⁵ It is not clear if this result would hold for a simple device with complex software, but as the principle is the same, it is not expected to yield a similar result. Butler (2017) affirms this stance,⁷⁶ noting that an average purchaser does not have the expertise in programming development and cybersecurity to bring forth such a claim.

Instead, both authors suggest that the danger utility test should be used. Under this test, the courts will assess if the cost of mitigating against the danger outweighs the risk of the danger occurring. However, neither author deals with the fact that a defence to a claim of design defect is that, at the time of the sale of the device, that the state of technical knowledge was not of the proper level to allow the manufacturer to be aware of the design flaw. This is of particular concern for cybersecurity as vulnerabilities are often discovered after the development of software. However, given that manufacturers of Smart Devices are aware that vulnerabilities are common place and that there exists tools to allow third parties to discover vulnerable Smart Devices, it is the belief of author that this defence should no longer be valid in the context of Smart Devices.

Within the UK, the conclusions of both Hecht (2005) and Butler (2017), while being similar to the UK, are not directly applicable.⁷⁷ The position of the UK courts with regard to products liability can be summarised by Burton J in *A & Ors v. National Blood Authority*,⁷⁸ where it was noted that within the American legal system, following on from the Third Restatement, there appears to be almost distinct jurisprudence between questions of defective products, design defects and warnings whereas in the UK, such a distinction is not present.⁷⁹ Further insight can also be gleaned from both *Wilkes v. DuPuy*,⁸⁰ and *Hastings v. Finsbury Orthopaedics Ltd & Stryker UK Ltd*.⁸¹ Both cases relate to plaintiffs who underwent surgery to receive prosthetic joints and who subsequently suffered harm following alleged defects within the devices and from the respective judgements, the principles and methodology which are employed by the courts to determine if a manufacturer is liable for negligence are clear, and require that there is a duty of care between the plaintiff and defendant, this duty of care was breached by the defendant and that there is an unbroken chain of causation between the actions of the defendant and the damage incurred by the defendant. The nature of the defect, be it a design defect or a defective unit, is found during the process and does not change the approach taken by the courts.

From *Wilkes* and *Hastings*, it is clear that the courts take the view that safety is a relative concept, as opposed to being an absolute. It is recognised that manufacturers can reduce risk to an ‘acceptable’ level but that it is not always possible to remove it completely. This concept translates well to a question of cybersecurity as it will never be possible to reduce all risk of a device’s subversion without turning the device off and removing it from the network. From a programming perspective, there will always be some possibility that a device will be compromised but at no fault to the manufacturer or owner and it is not the intention of the author of this paper to propose that where

Myron Hecht, ‘Products Liability Issues for Embedded Software in Consumer Applications’ (2005).

Butler (n 3).

Hecht (n 59); Butler (n 3).

⁷⁸ [2001] 3 All E.R. 289; [2001] Lloyd's Rep. Med. 187

⁷⁹ Ibid, paragraph 39

⁸⁰ [2016] EWHC 3096 (QB)

⁸¹ [2019] CSOH 96

there is a failure of cybersecurity, there is an automatic assignment of liability against the manufacturer. Furthermore, when looking at a negligence claim, it is important to note the findings in *Howmet v. Economy Drives Ltd & Ors*,⁸² where it was found that if a user of a device (the device in question was not a Smart Device, yet the point remains) has knowledge of a defect of the device, this knowledge can be used by the manufacturer to exclude liability arising for damages even when the device itself is faulty. This echoes earlier parts of this paper where it was proposed that users of devices also have a role to play in ensuring the cybersecurity of their device and their behaviour is taken into account when apportioning liability.

Taking into account the principles outlined in *Howmet*, it is clear that if a Smart Device manufacturer alerts their users to the existence of a vulnerability and the user continues to use the Smart Device before a patch is released, a claim made against the manufacturer will not be successful. A natural limitation on this finding would be, however, that such a defence will only be valid for a reasonable period between the discovery and announcement of the vulnerability and the release of a patch, as otherwise the manufacturer can then ‘sit on their hands’ and require a consumer to either stop using the Smart Device for an indefinite period or to run the risk of the device being compromised while not being in a position to protect against the compromise themselves.

Howmet also raises another point whereby current principles of negligence are less than fully suitable for dealing with issues arising from Smart Devices, as Jackson LJ notes,⁸³ that once a product leaves the factory gates, it is then outside of the control of the manufacturer and so limits to their liability begin to accrue. This would be fully correct for a non-internet connected device, as in order to make a change to the product, it would have to be returned to the manufacturer,⁸⁴ however, for Smart Devices the developer will retain a connection to the device and in actual fact, a degree of control over the software embedded within the device. *Wilkes*, *Howmet* and *Hastings* all note how a defence to a claim of negligence raised against a manufacturer is that the design defect wasn’t known to be a defect at the time of manufacture. This is a logical defence, as without it, manufacturers of products would be held accountable for risks which were not known to them at the time of manufacture and would be required to establish a ‘reverse supply chain’ whereby products could be returned and repaired, perhaps multiple times over the products life cycle. Such a state would both raise the cost of products for consumers and limit the number of products available to them.

Nevertheless, for Smart Devices, this logic breaks down. Normal goods, once sold, only interact with their immediate environment and with the exception of a small number of security related products (such as alarms, locks and safes) do not face an active threat of a third party trying to either subvert or break them, and even these products only face a threat from a third party who has a direct nexus with them. Smart Devices, however, at all times will have actors seeking to subvert their programming by both automated and manual means. Furthermore, when a Smart Device is released, its coding will be studied for vulnerabilities and only once it is in the market will these vulnerabilities become visible. Therefore, for Smart Devices, it is proposed that:

- The nature of the vulnerability exploited will form a key component of the liability decision, and if it is shown that there is a security failing, the company must have acted within a reasonable time or else they will be liable under Product Liability, Sale of Good or Common Law approaches.
- Producers are responsible for ensuring the security of the Smart Device for at least two years (or longer if agreed with the client) which requires:
 - Analysis to be performed to determine if vulnerabilities have been discovered; and

⁸² [2016] EWCA Civ 847

⁸³ Ibid, paragraph 76

⁸⁴ Or, the developer had created a channel which would allow the user to apply an update which had been delivered to them or downloaded directly from the developer.

- The creation of patches to remove any exploits found from the Device, ideally deployed to the device automatically within a reasonable amount of time
- Notification sent to users of now insecure devices, however, the *Howmet* liability exclusion will be limited to a short period (e.g., 30 or 60 days) and after that liability can attach to the producer if no patch has been developed or deployed
- Producers are no longer able to use the ‘state of knowledge’ exemption to avoid liability

6.2 Pure Economic Loss

Although the debate within the academic literature on the topic of bringing a successful claim for damages arising from a software defect has been ongoing for decades, it is generally agreed that such a claim would not succeed.⁸⁵ This is mainly due to the fact that, ignoring issues such as software defects and establishing a duty of care, there is no liability in tort arising from damages whose nature is that of *pure economic loss* as opposed to damages arising from physical harm or property damage, and most failures in software result in damages which are of a financial nature, or a loss of data which is covered under separate legislative regimes (e.g. the General Data Protection Regulation). The root of the doctrine of pure economic loss is *Spartan Steel & Alloys Ltd v Martin & Co (Contractors) Ltd*,⁸⁶ where it was determined by Lord Denning MR that, following a power cut which meant that steel being processed in a furnace became waste, the plaintiff was entitled to seek recovery for the cost of the steel, but was unable to seek recovery for the profit that would have been made on the steel.

The rationale behind the doctrine of pure economic loss is a sound one, as it limits tortious claims to those where the plaintiff has suffered damage which is self-limiting, is clearly identifiable and independent of all other property and people. This means that by granting damages, there is no risk that the floodgates would open and there would be a very large increase in the number of tortious claims which would have a chilling effect upon the rendering of services or the provision of critical infrastructure or goods. However, it is important to note that in the case of Smart Devices, should the device be subverted, the nature of the threat in relation to the owner would be primarily that of damage to their person or property so there is no change needed to the doctrine. The primary case where the doctrine becomes a defence for software developers is where a Smart Device has been subverted on the instruction of one party, who then uses the device to cause damage to a second party, and neither of these parties are the owner of the Smart Device.

Johnson (2015) (among others) notes that it is generally not possible to bring forth a claim for damages on the grounds of negligence following a failure of software because of the doctrine of pure economic loss.⁸⁷ However, the author of this paper proposes that this doctrine is overly restrictive in the singular instance where the plaintiff is the victim of cyberattack conducted by a Smart Device. This is because in such a circumstance it is now possible to directly calculate the ‘cost’ of the cyberattack, which is the cost incurred by the party arising from the online infrastructure usage during the attack, and also the ‘loss’ attributed to the company which is a fair representation of the loss of trade arising as a consequence of the attack.

The primary mechanism for such a cyberattack is to block access to an online resource (such as a website or a e-commerce store) by flooding it with requests made by a large number of compromised Smart Devices. These requests have an associated cost as companies will generally pay a fee based on the volume of online traffic requests they receive as they are charged for the ‘bandwidth’ usage, and furthermore, there are also costs and charges associated with the operation of their servers which

See, e.g., JP McMenamin, ‘Does Products Liability Litigation Threaten Picture Archiving and Communication Systems and/or Telemedicine?’ (1998) 11 JOURNAL OF DIGITAL IMAGING 21; Ling Zhu and Richard WW Xing, ‘A Pioneering Study of Third-Party Liability Insurance for Unmanned/Autonomous Commercial Ships’ (2019) 6 Journal of Business Law 442.

⁸⁶[1973] QB 27

CW Johnson, ‘The Role of Cyber Insurance, Market Forces, Tort and Regulation in the Cyber-Security of Safety-Critical Industries’, *10th IET System Safety and Cyber Security Conference 2015* (The IET 2015).

directly ties back to the volume of requests. There will also be charges levied by the victim's hosting company in defending against the cyberattack and in deploying cyberdefence tools. These costs are discrete and directly correlated with the attack, they are self-limiting and they are directly proportionate to the attack. It is proposed that these costs would become recoverable in this particular instance. Butler (2017) notes how the costs associated with a cyberattack against companies in the US average \$1.5m per attack,⁸⁸ and from *British Telecommunications PLC v. Geraghty & Miller International*,⁸⁹ it is clear how the courts are comfortable in assessing and calculating costs incurred by the plaintiff following the negligent conduct of a defendant.

Furthermore, there are now excellent analytics packages which mean a company can demonstrate what the losses associated with the downtime were, and how much of this was made up over subsequent days' trading. This may prove to be relevant for certain firms who have material revenue earned over a very short period of time (such as Black Friday or Christmas) and who, at certain times of the year are particularly vulnerable to DDOS attacks.⁹⁰ From the analytics packages associated with victim, as well as general analytics information, it is possible to calculate lost earnings given historical and contemporary earnings. Such a recovery would contradict the principles outlined in *Spartan Steel*, and would only be relevant for a specific subset of firms, but it would capture seasonal concentrations of revenue.

Therefore, it is clear that following an attack conducted by a botnet of Smart Devices, it is now possible for a company to demonstrate both direct and indirect costs and losses for which it can seek to recover. These claims are in keeping with the public policy reasons for denying pure economic loss requests as they are limited in nature, proportionally related to the attack and result from a direct and positive action taken intentionally by a third party, as opposed to, for example, a power cut which is not aimed in particular at the companies who are affected by it and was not the intent of the negligent party.

For the first time, it is proposed that with regard to a negligence case brought either by the owner of a Smart Device or by a victim of a cyberattack caused (in part or in full) by the Device that such a case should be able to proceed even if the damage caused is economic in nature.

6.3 Chain of Causation

In order to successfully demonstrate that negligence has occurred, the plaintiff must also be able to demonstrate that there is a clear link between the (in)action of the defendant and the harm caused and that the chain of causation is unbroken. Analysis of the chain of causation varies in practice between the US and other common law jurisdictions. Within the US, as outlined in the Third Restatement, there is a distinction between 'factual' (cause-in-fact) and 'legal' (proximate) causation, while within other common law jurisdictions, the test is based on factual causation and foreseeability. However, the principles underlying both proximate causation and foreseeability are quite similar. Within both frameworks, there must not be an *novus actus interveniens* – an action by an unrelated party, without which, the damage would not have been incurred and which is sufficient to break the chain of causation.

Cause-in-fact can be summarised as the 'but for' test; but for the action in question, would the damage have occurred. In the context of cybersecurity and the subversion of Smart Devices, cause-in-fact should be a reasonably low hurdle for a plaintiff to clear as a subversion can only happen following either a vulnerability or a lack a security, and the subversion itself a clear, binary event. However, the

Butler (n 3).

⁸⁹ [2004] EWHC 2530 (QB)

⁹⁰ This is discussed in detail in relation to the Utility Industry by Lachlan Urquhart and Derek MacAuley, 'Avoiding the Internet of Insecure Industrial Things' (2018) 34 Computer Law & Security Review 450.

actions of the plaintiff must also be taken into account; as is outlined in *Clay v. TUI UK Ltd*,⁹¹ where it is outlined how the actions of the plaintiff can constitute a *novus actus interveniens* and the courts will assess if, following an alleged negligent action, the plaintiff's response is proportional to the risk arising from the actions of the defendant. Using these principles, it is suggested that if a Smart Device was known to have a vulnerability, and the owner of the device then connected this device to a new network where it was exposed to a third party who was able to subvert the device via the vulnerability, the owner of the Smart Device would more than likely fail in a negligence claim against the manufacturer as their actions would constitute a *novus actus interveniens*.

The proximate cause / foreseeability test is somewhat more nebulous and opaque, and it examines if the action of a third party is sufficiently related to the outcome which caused the damages to allow for the attachment of liability. When viewed from the perspective of a Smart Device owner, given that systems now exist which allow for a third party to find a Smart Device and obtain information about its software, and there are now many automated systems used by cybercriminals which will be always scanning online to find Smart Devices, it could be construed as common-cause that if there is a vulnerable Smart Device, *ceteris paribus*, it is now likely that this device will be subverted and therefore means this is a foreseeable outcome. From a public policy perspective, by using an analysis of the nature of the subversion and examining the (in)action of both the developer and the owner of the Smart Device, it should now be possible for the courts to establish a proximate relationship without running the risk of opening the floodgates to large scale damage claims as suggested by Rustad and Koenig (2005).⁹²

Currently, it is not possible for a victim of a cyberattack to bring an action against the developer of the subverted device, owned by a third party, which engaged in a cyberattack against the plaintiff. The question of third party liability and the chain of causation has been discussed in detail in the Irish Supreme Court case *Breslin v Corcoran & Anor*.⁹³ In this case, the owner of a car had left it idling on a street while he entered a bakery. As he was returning, he saw a thief enter the car and abscond with the vehicle. The thief subsequently undertook a joyride and this resulted in injuries to the plaintiff, who sought damages both from Motor Insurance Bureau of Ireland (who operate a fund to cover the damage arising from uninsured drivers) and from the owner of the car. While the plaintiff succeeded in his action in the High Court, the decision was overturned in the Supreme Court, on the basis that the theft of the car was a *novus actus interveniens* and that it was not reasonably foreseeable that leaving the keys in the ignition would result in an act of joy riding.

This case would, at first reading, seem to support the assumption that the owner of a device cannot be held liable following the cyberattack, as the hack would be seen as a *novus actus interveniens* and there is an insufficient relationship between the developer and third party. However, it is clear that the Court broke the chain of causation on the principle that while it was not unreasonable for the owner of the car to foresee that it would be stolen, the fact that it was stolen and used for joyriding, which then caused injury, was a reach too far. However, when this principle is applied the compromise of Smart Devices, it is not as apparent that a *novus actus interveniens* would be seen as unlike an opportunistic theft of a vehicle, where the consequences (if any) to the general public are dependent on the thief, there are, as mentioned, automated and persistent threats looking for devices to subvert for the purposes of DDOS attacks and if no further actions were taken, it is a question of when as opposed to if, the device would be subverted. Furthermore, building upon the proposals as outlined in this paper, the application of legal causation to a case would only be necessary where:

- A device is subverted by a malicious third party through an exploit;

⁹¹ [2018] EWCA Civ 1177
Rustad and Koenig (n 25).

⁹³ [2001] IEHC 238

- The exploit was one which was known, or should have been reasonably known to the manufacturer;
- The developer failed to create and deploy or make available a patch to remedy the exploit used within a reasonable amount of time (e.g., 90 days from the discovery of the exploit)
- The victim is able to demonstrate clearly both the direct costs arising from the attack and the indirect costs (if any)

7 Liability in other technical products

Hubbard (2018) analyses the key points of legislation concerning autonomous vehicles in the United States. Similar to the academic questions surrounding IoT device,⁹⁴ data privacy and issues surrounding how to treat personal data obtained from both the journey itself, as well as data obtained by using a computer within the vehicle, are discussed and identified as the salient questions. However, cybersecurity does not form a key point of the analysis, reflecting the general view that seems to be present in legal writings that harm arising from software are 'soft' in nature as opposed to being able to cause physical harm and not as important as topics such as data protection. Zhu and Xing (2019) note how in the UK,⁹⁵ under the Autonomous and Electric Vehicle Act 2018, physical damages caused by autonomous driving cars will be actionable under tort and the producer is expected to be liable; however, the authors also note that if the cause was to be determined to be a failure of cybersecurity, the situation is less clear thus suggesting that damage, either personal or relating to property, arising from a cybersecurity failure has not been thought out, despite recognising that recovery under Tort is not expected to be a viable option. Furthermore, there are no specific cybersecurity guidelines within the legislation. This is contrasted with the UK Government's approach to regulating cybersecurity in Smart Devices, which outlines three clear (and welcome) cybersecurity requirements:⁹⁶

- Default passwords must be unique and cannot be reset to a 'global' default;
- Manufacturers must provide a public contact point for vulnerability disclosure; and
- Manufacturers must disclose the minimum time for which updates will be available.

Quigley and Ayihongbe (2018) discuss how in the medical device market,⁹⁷ which can be considered as one of the primary markets whereby failures in technology can result in direct physical discomfort, harm and mortality, as for reasons of public policy, regulation has been established in such a way that while product safety has been of definite concern, it has not been allowed to stifle innovation. Instead, competitiveness and market advantage are the primary factors which drive product innovation as medical regulation treats implanted devices as being 'fixed at the time of implantation' however, given that many of these devices are now 'smart', the risk profile of the device is constantly and permanently evolving, a fact that is not dealt with by the regulations. Risks arising from the misuse of medical devices by third parties are well known for many years, as demonstrated when Dick Cheney had the wireless aspects of his pace-maker disabled as it was seen as a security risk,⁹⁸ but unfortunately the paper is silent when it comes to liability for the failure of a device's cybersecurity, again suggesting that recovery following harm arising from a cybersecurity failure is not clear.

Sarah Hubbard, 'Automated Vehicle Legislative Issues' (2018) 2672 TRANSPORTATION RESEARCH RECORD 1.

⁹⁵ibid.

⁹⁶Culture Department for Digital Media & Sport, 'Government Response to the "Regulatory Proposals for Consumer Internet of Things (IoT) Security" Consultation' (The Government of the United Kingdom of Great Britain and Northern Ireland 2020).

⁹⁷Muireann Quigley and Semande Ayihongbe, 'Everyday Cyborgs: On Integrated Persons and Integrated Goods' (2018) 26 Medical Law Review 276.

⁹⁸Neta Alexander, 'My Pacemaker Is Tracking Me from Inside My Body' (The Atlantic, 27 January 2018) <<https://www.theatlantic.com/technology/archive/2018/01/my-pacemaker-is-tracking-me-from-inside-my-body/551681/>> accessed 23 March 2020.

The public policy decision putting innovation ahead of patient safety may seem at odds with general product liability law and it would seem to suggest that if product safety is not allowed to impede the development of medical technology, then it is unreasonable to expect that cybersecurity concerns could impact the development of the Smart Device market. However, the medical device market has a primary aim of helping to improve the lives of people suffering from a given illness, and while the market is large from a value perspective, the actual number of devices present would be considered as little more than a rounding error when compared to the Smart Device market, a point which would not apply to either medical device or autonomous vehicle markets.

The size of the Smart Device market and the documented history of its exploitation for cyberattacks, as well as it being a source of detailed personal information mean that product security is of key importance, especially as the added costs to the developers cannot be seen as being a risk to the continued growth of a market that has over 26 billion devices produced and although the market is quite new, it is already very well established.

8 Conclusion

From this paper, the scope and scale for cyberattacks should be clear, along with the potential harm to both personal safety as well as to critical infrastructure that compromised devices can cause. A link between this risk and the lack of liability and accountability for the developers of the code which these devices run on has also been drawn. For the first time, it is proposed that the specific nature of the exploit be examined and in order to bring forward a case of negligence or under a product liability framework, the attack itself must have been executed by relying on a *known exploit*, and that either the exploit had been ignored by the device manufacturer or had not been applied by the device owner (who must have been notified of both the threat of the exploit and the existence of the remediating patch). This paper has also outlined how the victims who suffer the greatest loss from a cyberattack involving a compromised Smart Device are not normally the owners of the device, and therefore a mechanism under the tort of Negligence has been proposed to enable those victims to seek redress.

This mechanism involves limited amendments to both the doctrine of Pure Economic Loss and the establishing of a chain of causation. However, it must be noted that what is proposed in this paper, although novel from the specific points put forward, is actually seeking to have Smart Devices brought into the same liability framework as ‘ordinary devices’, with exceptions made to allow for remote third parties to seek restitution for losses incurred. Furthermore, while the topic of cybersecurity and the nature of the subversion may be esoteric and highly technical, it is deterministic and therefore determinable. The judiciary in most jurisdictions have proven adept at being able to establish and apportion liability in highly complex and idiosyncratic circumstances,⁹⁹ and there is little doubt that the matter can be dealt with very comprehensively by both the legislature and the judiciary.

It is also clear that in the absence of legislative treatment of cyberattacks, there is little corresponding consumer awareness with regard to the cybersecurity of a Smart Device. Over time, as the popularity of Smart Devices continues to increase and they proliferate into being a staple household feature, there will be a large number (many millions) of devices which are no longer supported by their manufacturer but still connected to the internet. These devices will be a prime target for cybercriminals and in particular botnet architects. Currently, there are no legislative provisions (or even proposals) in place to deal with these unsupported devices which pose a threat to both their owners and other internet users. However, there has been some legislative progress. The 2019 Cybersecurity Act,¹⁰⁰ introduces the concept of a certificate or label for consumer products. This is welcome, however, there is no specific minimum standard of cybersecurity contained within the Regulation and the framework itself is voluntary. A similar scheme is in operation in Singapore,

⁹⁹ See, e.g., *Bolitho v City and Hackney Health Authority* [1998] AC 232, *Fletcher v Commissioner of Public Works* [2003] IESC 13 and *Sienkiewicz v Greif (UK) Ltd*; *Knowsley Metropolitan Borough Council v Willmore* [2011] UKSC 10, [2011] 2 AC 229

¹⁰⁰2019/881

although it is initially focused on routers and gateways as opposed to the wider universe of Smart Devices and is yet to produce a clear set of minimum standards for Smart Devices. The Singaporean scheme does reference the European Telecommunications Standards Institute (ETSI) baseline requirements for Internet of Things,¹⁰¹ however, these ‘requirements’ do not require, although they do recommend, that devices can be updated and that vulnerabilities should be patched. It is important to note that neither the proposed European Scheme nor the Singaporean scheme imposes liability on manufacturers for failing to adhere to the standards.

Similar progress has also been noted in the US, where in 2018 the State of California has enacted a law which requires that Smart Devices be equipped with ‘reasonable’ security measures.¹⁰² The aim of this law appears to be focused on stopping Smart Device manufacturers from shipping products which contain a default password as this was what enabled the rapid growth of, *inter alia*, the Mirai Botnet, and the Act does not require devices to be updatable. The Californian law also does not create a mechanism for consumers to bring a private action against developers who fail to adhere to the requirements and as such, only certain members of the California government can bring an action to seek enforcement of the law. The Federal Government has also passed, very recently, a bill which seeks to regulate the Smart Devices which are used by the Federal Government. The *IoT Cybersecurity Act*,¹⁰³ requires the development of minimum standards for IoT devices and in particular deal with the problems of default passwords and patching vulnerabilities. However, similar to the Californian Act, this bill does not create a means for consumers to enforce the usage of standards, nor would it cover devices used by consumers or businesses.

While these steps are welcome, it is the belief of the author of this paper that until 1) producers can be found liable for preventable cyberattacks and 2) device owners and operators can also be found liable for failing to keep their devices secure, cybersecurity will become a prime consideration for neither consumers, as they make their Smart Device purchasing decisions nor the developers of Smart Devices (with perhaps the exception of those developed for sale to the Federal Government of the United States of America), as they face choices in whether to increase the cybersecurity of the device or to deliver a Smart Device with a lower unit cost, to a faster time-line. Until both consumers and the general Smart Device market reward the former, and the courts or legislature hold such companies to account for their products, we will continue in the current environment where Smart Devices are easy tools for cybercriminals to use.

¹⁰¹ETSI EN 303 645

¹⁰²California Internet of Things Security Law, SB-327

¹⁰³H.R. 1688