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

Iain Nash[1]

5 April 2020

Abstract
Smart Devices 'cross the streams' of both the physical and the virtual worlds and can benefit greatly their users as well as society in general. However, with the growth in popularity of these devices, there is a corresponding growth in risks, both to the user and to the internet at large.

This paper outlines the threats which are posed by the hacking of Smart Devices, and provides a rudimentary methodology to apportion liability to either the manufacturer or the user, where appropriate, following a hack. This is done in a robust manner, from a technologically agnostic perspective, to ensure a persistent relevance in the face of unrelenting technological advancement.

Consumer rights and products liability are also examined from both an American and European perspective; legislative and judicial shortcomings are identified and remedies are proposed, with the intention of establishing a solid legal basis and treatment for cybersecurity.

Keywords: *Cybersecurity, Negligence, Products Liability, Consumer Rights, Internet of Things*

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.[2] Urquhart et al. (2018: 2) 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.[3] 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.[4] It is

[1] School of Law, Queen's University Belfast. Email: inash01@qub.ac.uk. The author thanks the contributions and support from Prof. Daithi MacSithigh, Dr. Philip O'Kane and Dr. Emma Lyons.

[2] 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.

[3] Lachlan Urquhart, Tom Lodge, and Andy Crabtree, 'Demonstrably Doing Accountability in the Internet of Things', *International Journal of Law and Information Technology,* 27/1 (2018), 1-27.

[4] Alan Butler, 'Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?', *University of Michigan Journal of Law Reform,* 50 (2017), 913-30., Darina

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.[5]

The connected nature of a Smart Device means that the manufacturer must ensure that 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 authors,[6] 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.[7] 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 which examines the question of how to assign liability in the context of either a failure of cybersecurity or a more general programming defect.

The aim of this paper is to re-evaluate the principles of product liability for Smart Devices from a cybersecurity perspective by taking into account both the nature of cybersecurity threats and the connected nature of software, including damages caused by the device to third parties, arising from the compromise of the Smart Device. This paper also outlines, for the first time, the key-points of a novel liability framework which is 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.

Overview of Cybersecurity

The relevance and importance of cybersecurity in legal theory should be evaluated within the context of the changing nature of computing. The term 'Information Technology', meaning the study or use of systems for storing, retrieving and sending information, has become synonymous with the use of computers,[8] and accordingly, computers have become tantamount with the processing of information, as opposed to a means of controlling physical

Lynkova, 'Iot Statistics and Trends to Know in 2020', *Leftronic Blog* <https://leftronic.com/internet-of-things-statistics/>, accessed 23 March 2020

[5] 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', <https://www.idc.com/getdoc.jsp?containerId=prUS45213219>, accessed 23 March 2020 2020.

[6] See, e.g., P. A. Alces, 'W(H)Ither Warranty: The B(L)Oom of Products Liability Theory in Cases of Deficient Software Design', *CALIFORNIA LAW REVIEW,* 87 (1999), 269-304., Daniel Boos et al., 'Controllable Accountabilities: The Internet of Things and Its Challenges for Organisations', *BEHAVIOUR INFORMATION TECHNOLOGY,* 32/5 (2013), 449-67., Broder Kleinschmidt, 'An International Comparison of Isp's Liabilities for Unlawful Third Party Content', *International Journal of Law and Information Technology,* 18/4 (2010), 332-55., and Rick Wash, Emilee Rader, and Chris Fennell, 'Can People Self-Report Security Accurately? Agreement between Self-Report and Behavioral Measures', *CHI '17* (Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, 2017), 2228-32.

[7] See, e.g., Alan Butler (n 4) and Liis Vihul, 'The Liability of Software Manufacturers for Defective Products', *Tallin Papers,* 2 (2014).

[8] As defined by the Oxford English Dictionary

devices. It is a common 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, which has resulted in the advent of the Smart Device.[10] Furthermore, as noted by Schneier (2018), computers by their nature are extensible which means 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 must now 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.

Friedman and Allan (2014: 39) 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 centrifuges,[13] redirect satellites,[14] and shut down global shipping facilities.[15] All of these acts, although having originated in cyberspace and thus representing failures of cybersecurity, have manifested as physical criminal acts in 'real life'. Therefore, it is clear how cybersecurity has now evolved beyond just the protection of intangible data to now 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.

Accordingly, it can be seen from a brief examination of the nature of cyber threats that the risks associated with Smart Devices are no longer limited to the misuse of the voluminous amounts of data which these devices generate and store, but also now include the risk that a

[9] See, e.g., Paul N. Otto, 'Reasonablenes Meets Requirements: Regulating Security and Privacy in Software', *Duke Law Journal,* 59/2 (2009), 309-42., and Giancarlo F. Frosio, 'Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility', *International Journal of Law and Information Technology,* 26/1 (2017), 1-33.

[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* (1 edn.; New York: W.W. Norton & Company, 2018).

[12] Peter W. Singer Friedman and Allan, *Cybersecurity & Cyberwar* (1 edn.; New York: Oxford University Press, 2014).

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

[14] Deborah Housen-Couriel, 'Cybersecurity Threats to Satellite Communications: Towards a Typology of State Actor Responses', *ACTA ASTRONAUTICA,* 128 (2016), 409-15.

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

person's possessions can be utilised in criminal acts which manifest directly against them or against third parties. Kolias et al. (2017) note how the most successful (at the time) Distributed Denial of Service attack was run by a botnet (a network of compromised machines which are under singular control) called Mirai that was composed of Smart Devices such as webcams, DVRs and routers as opposed to what would traditionally have been seen as a computer.[16]

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, was deployed in 2010 against a specific range of targets and 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, ransomware programs such as *WannaCry* and *NotPetya* have been developed and were able to shut down critical global infrastructure, such as hospitals,[17] manufacturing plants,[18] and ports,[19] 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 within ten years of Stuxnet, cybercriminals can now conduct a cyberattack against critical and global infrastructure using widely available tools.[20] 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.[21] 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,[22] demonstrating how a failure to follow basic cybersecurity practices, such as applying security updates, can result in substantive issues in the 'real' world.

[16] Constantinos Kolias et al., 'Ddos in the Iot: Mirai and Other Botnets', *Computer,* 50 (2017), 80-84.

[17] Russell Brandom, 'Uk Hospital Hit with Massive Ransomware Attack', *The Verge* (updated 12/05/2017) <https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin>, accessed 23 April 2020

[18] Andrew Liptak, 'Renault Shut Down Several French Factories', ibid.(updated 14/05/2017) <https://www.theverge.com/2017/5/14/15637472/renault-nissan-shut-down-french-uk-factories-wannacry-cyberattack>

[19] Mike Greenberg (n 15)

[20] Bruce Schneier, 'Data and Goliath', (New York: W. W. Norton & Company, 2015), 320.

[21] The 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)

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

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,[23] 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,[24] 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. It is clear that there have been some legislative attempts to provide a statutory basis to, *inter alia*, consumer rights but it is clear that cybersecurity has yet to be effectively (and predictably) dealt with either on a judicial or legislative basis.

When evaluating the legislative treatment of cybersecurity, it is important to note that although the term 'cybercrime' does not have any specific legal definition, it is a very common term in legal literature. There are many examples of works which engage with the topic of cybercrime,[25] but which do not actually provide a specific definition of the term. In these papers, the lack of a specific definition does not in any way impact on the quality of the paper, and it is clear that the term within the broader legal literature is used frequently to mean something approximating a 'wrong conducted via a computer'. However, in order to correctly assess the legislative relevance of cybersecurity, it must be acknowledged that not all cybercrimes are equal, and not all cybercrimes fall primarily within the remit of cybersecurity. A degree of precision and differentiation regarding the scope of cybersecurity is consequently required.

Urquhart (2019) defines cybercrime as a term that relates to a spectrum of acts ranging from traditional crimes which are aided by the advent of computers (such as tax evasion and financial fraud), to 'true' cybercrimes which would not exist but for the Internet (such as the theft of cryptocurrencies),[26] and it is clear that such a treatment is based on the Budapest Convention on Cybercrime, and the subsequent communication from the Commission of the European Union on this subject.[27]

Wall (2007),[28] notes how legislation that has been written to codify offences that are virtual in nature have focused on key issues such as data protection, copyright and piracy, privacy

[23] Ross Anderson et al., 'Measuring the Changing Cost of Cybercrime', *Workshop on the Economics of Information Security (WEIS),* (2019).

[24] David Harvey, *Collisions in the Digital Paradigm: Law and Rule Making in the Internet Age* (Oxford, United Kingdom: Bloomsbury Publishing Plc, 2017).

[25] See, e.g., Michael L. Rustad and Thomas H. Koenig, 'The Tort of Negligent Enablement of Cybercrime', *Berkeley Technology Law Journal,* 20 (2005)., Mohammad Hanif Jhaveri et al., 'Abuse Reporting and the Fight against Cybercrime', *ACM Computing Surveys,* 49 (2017), 68:1-68:27., and Benoit Dupont, 'Bots, Cops and Corporations: On the Limits of Enforcement and the Promise of Polycentric Regulation as a Way to Control Large-Scale Cybercrime', *Crime, Law and Social Change,* 67 (2017), 97-116.

[26] Lachlan Urquhart, 'Exploring Cybersecurity and Cybercrime: Threats and Legal Responses', in Lillian Edwards (ed.), *Law, Policy and the Internet* (Hart Publishing, 2019), 393-416.

[27] COM(2007) 267

[28] David S. Wall, *Cybercrime* (Polity Press, 2007).

and child pornography, and while there has been subsequent amendments to legislation,[29] there is still little in the way which covers cyberattacks. Brenner (2004) takes a different approach to analysing cybercrime and 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,[30] 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 as merely 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 able to now 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.[31]

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.

The Nature of Hacks

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 subversion. Although, as mentioned above, there is no specific legal definition of cybersecurity, for the purposes of this paper, a proposed definition for the term is the practice of securing a computer system from unauthorised use or attack. 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 principles and for the users of software, as they 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

[29] For example, Section 42 of the 2015 Serious Crime Act amends the 1990 Computer Misuse Act to include both causing or creating the risk of damage to a computer and using a computer as a tool to commit computer misuse offences

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

[31] Brian Krebs, 'Who's Behind the Gandcrab Ransomware?', *Krebs on Security* <https://krebsonsecurity.com/2019/07/whos-behind-the-gandcrab-ransomware/>, accessed 23 March 2020

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 developers themselves. Exploits are usually also reported to third party databases, with the most commonly used, according to Sánchez et al. (2020),[32] being the MITRE Corporation's Common Vulnerability and Exposure (CVE) database which is a free and open-access resource.[33] It is important to note that cyber-criminals 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.

Exploits can be further subdivided into two categories; *known exploits* which are vulnerabilities which have been reported and are '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 (when the software exists in the cloud and the responsibility for maintenance remains with the original developer, or when the software developer has created a channel allowing the automatic deployment of patches and the user has consented to the patch being deployed), 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.[34] August et al. (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.[35] 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. 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.[36] It is clear how these systems allow third parties to find Smart Devices which could be subverted by either a known

[32] M. C. Sánchez et al., 'Software Vulnerabilities Overview: A Descriptive Study', *Tsinghua Science and Technology,* 25/2 (2020), 270-80.

[33] https://cve.mitre.org/

[34] Leyla Bilge and Tudor Dumitras, 'Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World', *CCS 12 Proceedings of the 2012 ACM conference on Computer and Communications Security* (ACM, 2012), 833-44.

[35] Terrence August, Duy Dao, and Kihoon Kim, 'Market Segmentation and Software Security: Pricing Patching Rights', *Management Science,* (2019).

[36] Huichen Lin and Neil W. Bergmann, 'Iot Privacy and Security Challenges for Smart Home Environments', *Information,* 7 (2016), 44-44.

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.

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.[37] This is not generally correct (although this does not compromise the conclusions of the papers), 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* which is 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 there were c. 50,000 scripts built which depended on React and it was used in over two million projects.[38] 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.[39] A final example is *Argon2*, a cryptographically strong method of encrypting and storing passwords. Most programming languages will have a pre-built package which is based on the Argon2 function. 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*,[40] 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

[37] See, e.g., Jennifer A. Chandler, 'Information Security, Contract and Liability', *Chicago-Kent Law Review,* 84/3 (2009)., and Se-Hak Chun, 'E-Commerce Liability and Security Breaches in Mobile Payment for E-Business Sustainability', *SUSTAINABILITY,* 11/3 (2019), 715.

[38] Tanguy Krotoff, 'Front-End Frameworks Popularity (React, Vue, Angular)', (updated 12/12/2019) <https://gist.github.com/tkrotoff/b1caa4c3a185629299ec234d2314e190>, accessed 05/04/2020

[39] Hostingtribunal, '62 Node Js Stats That Prove Its Awesomeness', <https://hostingtribunal.com/blog/node-js-stats/>, accessed 05/04/2020

[40] Dilara Acarali et al., 'Modelling the Spread of Botnet Malware in Iot-Based Wireless Sensor Networks', *SECURITY AND COMMUNICATION NETWORKS,* 2019 (2019), 1-13.

how,[41] 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. 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. This is especially important when it comes to a home network which has multiple Smart Devices and a multiplicity of security settings.

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.

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 is 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 a single command.[42] This paper focuses in particular on compromises aimed at increasing the number of devices within a botnet, as if data is stolen, there are sufficient avenues for recovery of damages under the General Data Protection Regulation as enacted by Member States,[43] and if direct physical damage occurs, damages can 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 et al. (2017) outline the nature of threats posed to and by Smart Devices.[44] 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 Kreb's *Krebs on Security's* website as well as the critical infrastructure provider Dyn,

[41] Huichen Lin and Neil Bergman (n 36)

[42] Jennifer A. Chandler, 'Liability for Botnet Attacks', *Canadian Journal of Law and Technology,* 5 (2006).

[43] For example, S168 of the Data Protection Act 2018 in the United Kingdom provides the grounds for an individual to seek compensation for either material or non-material damages arising from a breach of the rights as set out by the Act.

[44] Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson, 'The First International Workshop on Pervasive Smart Living Spaces 2017 - Welcome and Committees', *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)* (2017), 1-2.

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,[45] 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.[46]

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. A number of reports,[47] note how in the United States in 2018, it is estimated that an adult will spend between ten and twelve hours per day engaging with a computer or television and utilising services which require cybersecurity in order to ensure continued access and to protect the data which is entered into these systems.

Vulnerabilities from a legal perspective

From the earlier parts of this paper, 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 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 (Directive 2013/40/EU) is the source for member states' specific criminal statues 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,

[45] Natalija Vlajic and Daiwei Zhou, 'Iot as a Land of Opportunity for Ddos Hackers', *COMPUTER,* 51 (2018), 26-34.

[46] Alan Butler (n 4)

[47] See, e.g., Nicole Fisher, 'How Much Time Americans Spend in Front of Screens Will Terrify You', *Forbes Magazine* <https://www.forbes.com/sites/nicolefisher/2019/01/24/how-much-time-americans-spend-in-front-of-screens-will-terrify-you/>, accessed 23 March 2020

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.

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,[48] 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 relating to the Sale of Goods which requires that goods are of merchantable quality.[49] There is a common law basis also, as outlined in *Power v Bedford Motor Company & Another*,[50] and in *Duffy v Rooney & Dunnes Stores (Dundalk) Ltd,*[51] that a person can recover damages from the producer of a product if they are able to demonstrate that i) there was a duty of care between the producer and the user, ii) there was a breach of the duty of care and iii) 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 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 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),[52] 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.

[48] e.g., Directive 85/374/EEC

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

[50] [1959] IR 391

[51] [1997] IEHC 102

[52] 1999/44/EC

Products which rely in part or in full on software do not fit 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 in order 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 (which are enacted),[53] and in the EU (which have yet to be transposed by the majority of Member States),[54] 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.

This raises a question as to whether a Smart Device is digital content and which was examined in some detail by Mak (2016),[55] who suggests that when looking at a particular Smart Device, if the digital element of the device is primary to its nature and to its use by a consumer, then it falls under the scope of a digital device whereas if the Smart elements of the device are of a secondary nature, then it should be treated as a good.

However, given that there has been no modification to the European Product Liability Directive,[56] the defences available to the producer of the good or digital content will still continue to apply, including the defence that the vulnerability wasn’t known about at the time,[57] which suggests that until the courts begin to look at the nature of the exploits, and in particular if the exploit was known (or should have been known) to the developer at the time of release, it will not be possible to correctly apply the principles as outlined in the 2019 EU Consumer Protection Directive.

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 its libraries. 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 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.

[53] Consumer Rights Act 2015

[54] Directive 2019/2161

[55] Vanessa Mak, 'The New Proposal for Harmonised Rules on Certain Aspects Concerning Contracts for the Supply of Digital Content', (Director General for Internal Policies, 2016).

[56] Directive 85/374/EEC

[57] Article 7, Directive 85/374/EEC

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.[58] 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,[59] 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 (either in the core code or in components used by the program). However, that the manufacturers are aware of the fact that vulnerabilities are common place, and that there exists tools to allow third parties to discover vulnerable Smart Devices, and that it is now common and expected by consumers that Smart products are updated, this defence should no longer be valid for producers.

Within the jurisdiction of the United Kingdom, the conclusions of both Hecht (2005) and Butler (2017), while being similar to the UK, are not directly applicable.[60] The position of the UK courts with regard to products liability can be summarised by Burton J in *A & Ors v. National Blood Authority,*[61] 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.[62] Further insight can also be gleaned from both *Wilkes v. DuPuy*,[63] and *Hastings v. Finsbury Orthopaedics Ltd & Stryker UK Ltd.*[64] 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.

[58] Myron Hecht, 'Products Liability Issues for Embedded Software in Consumer Applications', *2005 IEEE Symposium on Product Safety Engineering* (2005), 42-48.

[59] Alan Butler (n 4)

[60] Myron Hecht (n 58), Alan Butler (n 4)

[61] [2001] 3 All E.R. 289; [2001] Lloyd's Rep. Med. 187

[62] Ibid, paragraph 39

[63] [2016] EWHC 3096 (QB)

[64] [2019] CSOH 96

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 will translate 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 and accordingly, and from the discussions above, it will always be possible that a device will be compromised but at no fault to the manufacturer or owner.

However, when looking at a negligence claim, it is important to note the findings in *Howmet v. Economy Drives Ltd & Ors,*[65] where it was found that if a user of a device (the device in question was not a Smart Device but 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 suggests that under the current principles of negligence, if a Smart Device manufacturer alerts their users as 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,[66] 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 chance to the software, the device would have to be returned to the manufacturer,[67] 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 a) held accountable for risks which were not known to them at the time of manufacture and b) 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.

[65] [2016] EWCA Civ 847

[66] Ibid, paragraph 76

[67] 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.

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 clear that responsibility for ensuring that the embedded software should remain with the producer for at least a specified period of time.

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.[68] This is mainly due to the fact that, ignoring issues such 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*,[69] where it was determined by Lord Denning MR that, following a power cut which meant that steel which was 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.[70] However, it is proposed in this paper that the doctrine is overly restrictive in the singular instance where the plaintiff is the victim of cyberattack conducted by a Smart Device. 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.

[68] See, e.g., J. P. Mcmenamin, 'Does Products Liability Litigation Threaten Picture Archiving and Communication Systems and/or Telemedicine?', *JOURNAL OF DIGITAL IMAGING,* 11/1 (1998), 21-32., and Ling Zhu and Richard W. W. Xing, 'A Pioneering Study of Third-Party Liability Insurance for Unmanned/Autonomous Commercial Ships', *Journal of Business Law,* 6 (2019), 442-58.

[69] [1973] QB 27

[70] C. W. 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).

The primary mechanism for such a cyberattack is to block access to an online resource (such as a website or a directory) by flooding it with requests made by a large number of subverted 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 'bandwith' usage, and furthermore, there are also costs and charges associated with the operation of their servers which 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 cyber defence 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 United States average $1.5m per attack,[71] and from *British Telecommunications PLC v. Geraghty & Miller International,*[72] 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 that a company can demonstrate what the losses associated with the downtime were, and how much of this was made up over subsequent day's 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 particular vulnerable to DDOS attacks. From 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 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 the test of negligence should incorporate an analysis of the nature of the compromise of the Smart Device. Liability should attach to the manufacturer of the Smart Device if the nature of the vulnerability was such that it should have been known and patched, or if the company was reckless in the development of its software by not following secure software development principles, while the owner would be negligent to a claim by a third party (or would have their claim limited in part by their own contributory negligence) if they had failed to update or had blocked the update of the Smart Device. The fact that a Smart Device was subverted is not, in and of itself proof of negligence by any party, as this can only be determined by looking at the nature of the subversion.

[71] Alan Butler (n 4)

[72] [2004] EWHC 2530 (QB)

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 American and other common law jurisdictions as within the USA, 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 (such as those of the United Kingdom and Ireland), the test is based on factual causation and foreseeability. However, the principles underlying both proximate causation and foreseeability are quite similar. Within both the UK and the USA, there must not be an *novus actus interveniens* – an action by an unrelated party, without with, 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 actions of the plaintiff must also be taken into account and this is outlined in *Clay v. TUI UK Ltd,*[73] 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 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 there are now (legal) systems which allow for a third party to find a Smart Device and obtain information about its software, and there are now many automated systems 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 paribas*, it is now likely that this device will be subverted and therefore 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).[74]

Currently, it would not be 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

[73] [2018] EWCA Civ 1177

[74] Michael Rustad and Thomas Koenig (n 24)

discussed in detail in the Irish Supreme Court case *Breslin v Corcoran & Anor.*[75] In this case, the owner of a car had left it idling on a street while he entered into 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 reasonable 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 seen as a reach too far. However, when this principle is applied the compromise of Smart Devices, it 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, when applying the general principles as outlined earlier in this paper, claims would be limited to cases only where actual negligence, as opposed to all hacks, had occurred.

Liability in other technical products

Hubbard (2018) performs an analysis of the key points of legislation regarding autonomous vehicles in the United States. Similar to the academic questions surrounding IoT device,[76] 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 on legal writing 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,[77] 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 and this suggests 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

[75] [2001] IEHC 238

[76] Sarah Hubbard, 'Automated Vehicle Legislative Issues', *TRANSPORTATION RESEARCH RECORD,* 2672 (2018), 1-13.

[77] Ling Zhu and Richard Zing (n 68)

Government’s approach to regulating cybersecurity in Smart Devices, which outlines three clear (and welcome) cybersecurity requirements:[78]

- Default passwords must be unique and cannot be reset to a ‘global’ default;
- Manufactures 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,[79] which can be considered as one of the primary markets whereby failures in technology can result in direct physical discomfort, harm and mortality, that 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,[80] 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.

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 who suffer 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.

[78] Culture Department for Digital, Media & Sport 'Government Response to the “Regulatory Proposals for Consumer Internet of Things (Iot) Security” Consultation', (London: The Government of the United Kingdom of Great Britain and Northern Ireland, 2020).

[79] Muireann Quigley and Semande Ayihongbe, 'Everyday Cyborgs: On Integrated Persons and Integrated Goods', *Medical Law Review,* 26/2 (2018), 276-308.

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

Conclusion

This paper has attempted to propose a high level methodology which, following a successful cyberattack of a Smart Device, sets the first hurdle so that in order to proceed with a claim, 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 also outlines how it is currently impossible, with the exception of a small number of scenarios which have the potential for the causation of limited damage, to bring an action following a cyberattack, and a number of remedies for these impediments are outlined. Finally, a number of recommendations are made to help ensure clear consumer choice with regard to Smart Devices.

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. Therefore, in addition to the legislative proposals outlined in this paper, it is also proposed that when a consumer purchases a Smart Device;

- It is made clear to the consumer prior to the time of purchase if they are responsible for the device's security or if the device will update itself;
- The manufacturer outlines how long the device will be supported with functional updates;
- The manufacturer outlines how long the device will be supported with security updates; and
    - How the device will continue to function after security updates have ceased; e.g., the 'Smart' component is deactivated, the device will only connect with other devices contained within the network or the device will continue to function but the owner will be responsible for the damages arising from a subversion

These proposals will allow a consumer to make an informed choice about the level and duration of cybersecurity which the manufacturer of the Smart Device is offering to them when purchasing a Smart Device, as well as making its end-of-life outcome a part of their purchasing decision. The options provided by the manufacturer to the consumer can also be used as part of the analysis of their liability to any subsequent compromise of the device.

Only when we reach a time when both the manufactures and owners of Smart Devices can be held liable for the damages arising from the subversion of their devices, which were caused due to their negligent treatment of the device's security, can cybersecurity begin to be considered as having a robust legislative basis. Such an outcome will require reform of approaches to consumer rights, products liability and the law of Tort as well as the understanding and incorporation of technical risk into legislative and judicial deliberations.

However, it must be noted that the judiciary in most jurisdictions have proven adept at being able to establish and apportion liability in highly complex and idiosyncratic circumstances.[81] When it comes to cybersecurity, the nature of the subversion may be esoteric and highly technical, but it is deterministic and therefore determinable, which suggests that there is little doubt that the matter can be dealt with very comprehensively by both the legislature and the judiciary.

[81] 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