Smart Device Manufacturer liability and redress for third-party cyberattack victims

Iain Nash*

Abstract
Smart Devices are used to facilitate cyberattacks against both their users and third parties. While users are generally able to seek redress following a cyberattack via data protection legislation, there is no equivalent pathway available to third-party victims who suffer harm at the hands of a cyberattacker. Given how these cyberattacks are usually conducted by exploiting a publicly known and yet un-remediated bug in the Smart Device's code, this lacuna is unreasonable. This paper scrutinizes recent judgments from both the Supreme Court of the United Kingdom and the Supreme Court of the Republic of Ireland to ascertain whether these rulings pave the way for third-party victims to pursue negligence claims against the manufacturers of Smart Devices. From this analysis, a narrow pathway, which outlines how given a limited set of circumstances, a duty of care can be established between the third-party victim and the manufacturer of the Smart Device is proposed.

Keywords
Cybersecurity, Cyberattacks, Smart Devices, Duty of Care, Omissions.

Introduction
Should a third-party victim of a cyberattack, which was carried out using a network of hacked Smart Devices, be able to seek redress from the manufacturer of the Smart Devices, if the hacks were enabled by the manufacturer failing to remedy a known security issue?

This is the question which this paper seeks to answer by examining recent decisions in both the UK and Irish Superior Courts. This paper draws from both jurisdictions for two reasons. The first reason is that the key questions which need to be answered to reach a conclusion regarding the manufacturer of the Smart Device are discussed on an individual basis by the UK and Irish Superior Courts. This is augmented by the fact that the Irish Supreme Court has delved further into the questions regarding omissions and liability than the UK courts have to date. Accordingly, decisions from both jurisdictions are needed to form an answer to the opening question. The second reason is that it allows the analysis to draw on recent but independent UK and EU legislative developments with regards to Smart Device cybersecurity, and how these developments could support a negligence claim.

The question is divided into two distinct pieces of analysis. The first piece examines whether the victim of a cyberattack, which was carried out by an unknown cyberattacker who used, as part of the attack, a Smart Device under a set of specific and limited conditions, could successfully ground a claim of negligence against the third-party manufacturer of the Smart Device (the Smart Device Manufacturer), while the second analysis (which assumes the success of the first) examines whether the nature of the damage suffered by the claimant is recoverable under a negligence claim.

* Senior Lecturer, School of Law, Criminology and Policing, Edge Hill University, iain.nash@edgehill.ac.uk
PhD Candidate, Centre for Commercial Law Studies, Queen Mary University of London
The author would like to thank Prof. Ian Walden and Prof. Iris Benöhr, the anonymous referees, the participants of the 2022 SLS Annual Conference (Torts), in particular Eoin Quill and the participants of the 2022 Cybersecurity Law and Policy Scholars Conference, in particular Prof. Charlotte Tschider for their comments, feedback and suggestions for this paper. Any errors or omissions that remain are the responsibility of the author.

Negligence claims made against a defendant in relation to alleged cybersecurity failures are not entirely novel. However, despite the cases of *Warren,*[1] *Smith,*[2] and *Collins,*[3] who all sought in some form or other to allege negligent cybersecurity practices which resulted in the tort of misuse of personal data, tort cases involving a cybersecurity failure remain rare. This is a confusing situation, given the exponential level of growth of information technology systems which have a direct impact upon our daily lives. The dearth of cases can perhaps be explained by the fact that, within Europe and the UK at least, the imposition of the General Data Protection Regulation has meant that national Data Protection regulators have become a *de facto* arbiter for cybersecurity,[4] but whether there are circumstances which would allow a third-party victim of a cyberattack to be awarded damages from a hypothetically negligent Smart Device Manufacturer remains an open question.

Throughout this paper, the term 'Smart Device' is defined as a product which has been sold to a consumer and is a physical device which was designed to carry out a specific function. Furthermore, the Smart Device must contain a Central Processing Unit and be capable of being accessed remotely. Finally, the Smart Device must communicate with a remote service which is integral to its 'smart' operations.

Whilst the first element of this definition is trivial, the second element is also relatively straight forward; the Smart Device must be physical in nature (and therefore comprise of both software and hardware components) and have been designed to carry out a specific function, while also having been augmented to include 'smart' features. Devices which were designed to be 'general purpose' computing devices, such as a Smart Phone, Laptop or Tablet, are outside the scope of this definition. Examples of Smart Devices include home security systems, smart lighting systems, smart home appliances such as fridges, kettles and washing machines and smart thermostats.

For the purposes of this paper, mere communication with a remote service is not sufficient to meet the definition of a Smart Device. Devices which communicate with remote, non-internet services in a 'read only' manner, such as devices with a built in GPS device or radio receiver, or devices which engage in two-way communication with a service which is unable to fundamentally alter the behaviour of the device beyond its normal function, such as a non-smart phone receiving a call or sending a text message, are themselves not sufficient to meet the definition of a Smart Device. It must be possible for the device to have its operating system altered by communication with a remote service in order to meet the definition.

The nature of cyber risks associated with Smart Devices

A Smart Device can be considered as a child of two worlds: it is a physical product which interacts in a tangible manner with its user and their property. However, a Smart Device is also a child of an intangible world. In addition to its physical properties, it comprises of firmware, a kernel, an operating system, and various software applications.

It is this second world which extends the risks associated with the Smart Device beyond those of a traditional consumer device. Were the device simply a 'dumb' or non-internet enabled device, the

1 *Warren v DSG Retail Ltd* [2021] EWHC 2168 (QB).

2 *Graeme Smith v Talktalk Telecom Group Plc* [2022] EWHC 1311 (QB).

3 *Collins v Ticketmaster* [2021] WL 05585718 (2021) (Chancery Division).

4 Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016 (OJ L 119) Article 32.

risks associated with the Device are, broadly speaking, limited to the risk of harm to people who use or are physically close to the device, or damage to other goods and property in a direct physical nexus with the device. However, once the device is 'smart', it allows for people who are physically remote from the device to either engage with and control the device, and for the device to engage with a remote online resource on the instruction of the cyberattacker.

Broadly speaking, the risks associated with the Smart Device can be divided into four areas:

- Direct Physical Risks; where there is a risk of physical harm to a person or property, who are physically near the Smart device, and the harm is caused by a defect in the device or by the actions of a cyberattacker.
- Direct Electronic Risks; where there is a risk to information stored within the Device or a risk of the Smart Device engaging in attacks on other devices on its local network.
- Remote Physical Risks, a risk of a cyberphysical attack facilitated by the Smart Device against a remote Smart Device, which is operating on a distant network.
- Remote Electronic Risks, a risk of a Distributed Denial of Service (DDoS) attack facilitated by the Smart Device against a remote online service or a risk of a cyberattack which was enabled by the Smart Device, and carried out against a remote online service.

This paper focuses on the remote physical and electronic risks, as there are existing legal remedies for direct risks associated with the Smart Device.[5] A remote risk is one where a cyberattacker can cause harm or loss to a remote third party who does not have a physical nexus with the Smart Device, using the Smart Device as an intermediary instrument. These risks may manifest themselves as physical harm to a person or to property, or as economic loss because of some form of availability attack.

An availability attack, a term first coined by Kilovaty,[6] is an attempt by a cyberattacker to deny the world at large access to a specific online resource. An availability attack, in its original form includes malicious techniques such as a DDoS attack. This is where a group of compromised devices flood the target with requests so as to render the service unavailable,[7] as well as ransomware attacks, which mutate the data which the service relies upon, in order to render it unreadable and thus the service inoperable.[8] DDoS attacks are computationally trivial to conduct, so the fact that a Smart Device has low levels of computational capability when compared to a general purpose computing device, such as mobile phone, laptop or desktop, is immaterial in terms of the effectiveness of the device carrying out the attack. DDoS attacks are a simple, straight forward command that is repeated at high speeds by a Smart Device and the effect of the attack is scaled due to the coordinative efforts of all of the other compromised Smart Devices in the botnet (a network of compromised devices).[9] DDoS attacks

5 E.g., Products Liability legislation will grant a consumer protection against the device failing to perform as expected. Data Protection Legislation, along with a Misuse of Personal Information tort provide avenues for remedies if the consumer's data is unlawfully processed or accessed. Should the device cause damage to the consumer's property, a negligence claim could be brought against the Smart Device Manufacturer if the facts justify such a claim.

6 Ido Kilovaty, 'Availability's Law' (2020) 88 Tennessee Law Review.

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

8 Chesti Ikra Afzal, Humayun Mamoona and Sama Najm Us, 'Evolution, Mitigation and Prevention of Ransomware', *2nd International Conference on Computer and Information Sciences* (Institute of Electrical and Electronics Engineers Inc 2020).

9 Polly Wainwright and Houssain Kettani, 'An Analysis of Botnet Models', *Proceedings of the 2019 3rd International Conference on Compute and Data Analysis* (ACM 2019) <https://dl.acm.org/doi/10.1145/3314545.3314562> accessed 24 September 2020; Neamen Negash and Xiangdong Che, 'An Overview of Modern Botnets' (2015) 24 Information Security Journal: A Global Perspective 127.

are frequently associated with Smart Devices, and are the specific form of attack identified by ENISA (the European Union's Cybersecurity Agency) as the primary risk associated with Smart Devices.[10]

DDoS attacks are usually quite fleeting, usually lasting for minutes as opposed to days,[11] and their short-term nature can lead to the assumption that the risks and consequences of such an attack are but a mere bagatelle compared to other cyberattacks. However, when used strategically by an adversary, the effects of a DDoS attack can be material, as was the case when the Katana botnet aimed to reduce the availability of news, government and financial services during the early hours of the invasion of the Ukraine,[12] or when, in 2017 the (then) recently released Mirai source code was used to create a botnet which was able to deny consumers in Europe and North America access to the internet by overwhelming a core internet backbone service.[13]

Furthermore, as we are transitioning from a '4G' environment of mobile connectivity, where devices operate autonomously but are supported by remote services, to a '5G' environment, where devices are becoming more dependent on large volumes of data being provided by remote services at high speeds in order to function,[14] the risks associated with interference to these remote services are becoming more material.

Remote cyber-physical attacks are a niche and very rare form of cyberattack, where an attacker can use a compromised Smart Device to engage directly with another Smart Device, either through an internet connection or a local connection (e.g., Bluetooth,[15] WiFi,[16] or Zigbee[17]) and cause a change in the Smart Device's physical behaviour. There are no known examples of cyber-physical attacks involving a Smart Device occurring in the wild, however, such attacks have been demonstrated as possible using real-world conditions,[18] and the results include both damage to property and personal injury (the triggering of epilepsy).

---

10 ENISA Advisory Group, 'Opinion: Consumers and IoT Security' (2019) <https://www.enisa.europa.eu/about-enisa/structure-organization/advisory-group/ag-publications/final-opinion-enisa-ag-consumer-iot-perspective-09.2019> accessed 18 June 2022.

11 Lance Whitney, 'Why Certain Companies Are More Heavily Targeted by DDoS Attacks' (*TechRepublic*, 5 February 2020) <https://www.techrepublic.com/article/why-certain-companies-are-more-heavily-targeted-by-ddos-attacks/> accessed 21 February 2022; European Union Agency for Law Enforcement Cooperation., *IOCTA 2021: Internet Organised Crime Threat Assessment 2021.* (Publications Office 2021) <https://data.europa.eu/doi/10.2813/113799> accessed 7 June 2022.

12 Cado Security, 'Technical Analysis of the DDoS Attacks against Ukrainian Websites' (*Cado Blog*) <https://www.cadosecurity.com/technical-analysis-of-the-ddos-attacks-against-ukrainian-websites/> accessed 21 April 2022.

13 Constantinos Kolias and others, 'DDoS in the IoT: Mirai and Other Botnets' (2017) 50 Computer 80; Schneier, Bruce, 'Lessons From the Dyn DDoS Attack' (*Schneier on Security*, 8 November 2016) <https://www.schneier.com/blog/archives/2016/11/lessons_from_th_5.html> accessed 10 May 2022.

14 Marton Varju, '5G Networks, (Cyber)Security Harmonisation and the Internal Market: The Limits of Article 114 TFEU' (2020) 45 European Law Review 21.

15 Bluetooth SIG, 'Bluetooth Network Encapsulation (BNEP) Specification' (2003) <https://www.bluetooth.com/specifications/specs/bluetooth-network-encapsulation-protocol-1-0/> accessed 11 October 2022.

16 See, e.g., IEEE Standards Association, 'IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications' (1998) IEEE 802.11-1997 <https://standards.ieee.org/ieee/802.11/1163/> accessed 11 October 2022 as an example of original WiFi specifications.

17 zigbee alliance, 'Zigbee Specification' (Connectivity Standards Alliance 2017) <https://csa-iot.org/wp-content/uploads/2022/01/docs-05-3474-22-0csg-zigbee-specification-1.pdf> accessed 11 October 2022.

18 See, e.g., Eyal Ronen and others, 'IoT Goes Nuclear: Creating a Zigbee Chain Reaction' (2018) 16 IEEE Security & Privacy 54.

There have been many examples of direct cyber-physical attacks against Smart Device and Internet of Things (IoT) Devices,[19] and, indeed, there have been cases of direct cyber-physical attacks which did not involve Smart Devices.[20] However these attacks were conducted directly by an attacker and did not use a Smart Device as either an intermediary platform or as a tool to support and engage in the attack and so are out of scope for this paper.

For a remote cyber-physical attack to be in scope for the negligence claim proposed in this paper, the attacker must first compromise a Smart Device through the 'negligence' of the Smart Device Manufacturer, and then use this compromised Device as part of the attack which results in damage to either property or person. At the time of writing, such an attack is not yet known to have occurred outside of a cybersecurity research environment. Therefore, for the purpose of this paper, any availability attack or cyber-physical attack which is carried out by a Smart Device under the instruction of a cyberattacker against a third party will be called an 'in scope attack'.

When thinking about an availability attack caused by a Smart Device, the analysis must begin with the method by which an adversary gains access to device's operating system. In general, there are two mechanisms available to a remote third party to achieve such access; they can do so because of a vulnerability in the underlying software which allows direct access via an exploitable vulnerability.[21] The second way can be done by convincing or inducing a user of the device to run a piece of carefully crafted malicious code, which may then allow the attacker to either exploit a vulnerability inherent to the system which was not accessible remotely, or it can exploit the user's level of privilege (their ability to carry out administrative operations) to enable the creation of a persistent access point to the system.[22] This latter approach can be considered as 'indirect' access as it will require the (usually unintentional) support of a user to facilitate access whereas the former requires neither subterfuge nor user involvement, allowing for direct access to the Smart Device. Cyberattacks against a Smart Device which have used an indirect approach are very rare, and those which occur will fall outside of the scope of this paper as the actions of the user in allowing the cyberattacker to access the device will constitute a clear break in the chain of causation, a topic which is discussed later in this paper.

Overview of Smart Device cybersecurity

In order for a claim of negligence to be successfully made, there must be an action (or an inaction, given the omissions argument presented further on in this paper) made by the defendant which results in the harm suffered by the claimant, and which itself is found to be negligent. Therefore,

19 See, e.g., Brian Krebs, 'What's Most Interesting about the Florida Water System Hack? That We Heard about It at All.' *Krebs on Security* (10 February 2021) <https://krebsonsecurity.com/2021/02/whats-most-interesting-about-the-florida-water-system-hack-that-we-heard-about-it-at-all/> accessed 16 February 2021 for a summary of how an IoT device was attacked and instructed to poison a water supply. See also 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 for a more general discussion of the risks arising from IoT in an industrial context.

20 See, e.g., Kim Zetter, Countdown to Zero Day (1st edn, Broadway Books 2014); and Ronen Bergman, Rise and Kill First: The Secret History of Israel's Targeted Assassinations (John Murray 2019) for a discussion about how a combined team from US and Israel was able to damage Iranian centrifuges via a cyber attack; and Andy Greenberg, Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers (1st edn, Doubleday 2019) for a discussion of how a hacking exercise was able to de-stabilise a power grid.

21 See, e.g., Iain Nash, 'Cybersecurity in a Post-Data Environment: Considerations on the Regulation of Code and the Role of Producer and Consumer Liability in Smart Devices' (2021) 40 Computer Law & Security Review for a more detailed discussion on exploitable vulnerabilities.

22 Mohammad Hanif Jhaveri and others, 'Abuse Reporting and the Fight Against Cybercrime' (2017) 49 ACM Computing Surveys 68:1.

before the legal analysis can take place, the technical measures which the Smart Device Manufacturer can take (or fail to take) which give rise to the cybersecurity failure need to be discussed.

Firstly, it is important to make clear that this paper does not propose that a Smart Device Manufacturer is obliged to prevent all forms of cyberattacks made against the Smart Devices which they have built. Nor is it proposed that a Smart Device Manufacturer must develop an 'open ended' security operation. Instead, it will be argued that a Smart Device Manufacturer has a responsibility to prevent their Smart Devices from falling prey to known security vulnerabilities, which have been made public and are accessible in vulnerability databases and are known (or at least ought to be known) to security professionals and software developers.

When thinking about the digital elements of a Smart Device, it should be recalled that the 'software' is composed of different layers: the firmware which governs the interaction between the hardware on the device and other software layers; the kernel, which allows the Operating System and other higher level software applications to utilise the firmware and the device's hardware; the Operating System, which manages all software applications; and finally, the individual software applications themselves, some of which will be employed by the user in order use the Device and the others which have been developed to carry out various functions.

It is common for Smart Devices to utilise the Linux kernel,[23] free and open-source software.[24] This means that it is developed by contributors to the Linux foundation. Indeed, for most Smart Devices the only truly 'bespoke' software will often be the software applications which were developed either by or on-behalf of the Smart Device manufacturer. This is a crucial distinction to make, because when the Smart Device Manufacturer purchases the hardware to make the device, it will often come pre-loaded with firmware, kernel and operating system.[25] The Smart Device Manufacturer will not have chosen these software packages; however, by utilising them, should be responsible for maintaining their security.

Maintaining the security of these packages is a less onerous task than it may initially appear. There are databases of vulnerabilities which are updated once a security researcher or a research team have identified and reported a vulnerability, and it is a rather trivial exercise for a company to track if software which is present in their products has a vulnerability, and if a remediating patch has been

23 See, e.g., Sarfaraz Ahamed and Ramanathan Lakshmanan, 'Real-Time Heuristic-Based Detection of Attacks Performed on a Linux Machine Using Osquery' (2022) 3 SN Computer Science 405; and Luca Vignati, Stefano Zambon and Luca Turchet, 'A Comparison of Real-Time Linux-Based Architectures for Embedded Musical Applications' (2021) 70 Journal of the Audio Engineering Society 83; and Saroj Kumar Panda, Man Lin and Ti Zhou, 'Energy Efficient Computation Offloading with DVFS Using Deep Reinforcement Learning for Time-Critical IoT Applications in Edge Computing' [2022] IEEE Internet of Things Journal 1; and Xuechao Du and others, 'AflIot: Fuzzing on Linux-Based IoT Device with Binary-Level Instrumentation' (2022) 122 Computers & Security 102889 for a discussion of Linux and Unix as commonly used firware, kernels and operating systems for Smart Devices. .

24 'The Linux Kernel Organisation' <https://www.kernel.org/category/about.html> accessed 16 October 2022.

25 Bruce Schneier, 'Router Security' (*Schneier on Security*, 19 February 2021) <https://www.schneier.com/blog/archives/2021/02/router-security.html> accessed 12 February 2022.

developed.[26] Alternatively, a Smart Device Manufacturer can employ a third party to monitor for vulnerabilities and security patches.[27]

It can be considered common cause that security updates are recognised as a critical aspect of cybersecurity for Smart Devices,[28] and that security vulnerabilities are a prime means for a cyberattacker to gain access to a system or device.[29] Therefore, for the duration of this paper, it is proposed that the 'negligent act' is where a Smart Device Manufacturer fails to apply security patches, within a reasonable time frame, which have been developed for the software which the Smart Device Manufacturer is using the Smart Device. If the Smart Device Manufacturer has developed their own software, the negligent act will be the failure to develop a security patch for their software once a vulnerability has been discovered. It is a known fact that Smart Device Manufacturers frequently fail to deploy or develop security patches to their devices which have been sold to consumers,[30] and the rest of this paper will be devoted to determining if these potential failures met the legal definition of negligence.

Accordingly, it should be clear how one of the key aspects of this paper's proposal is that the Smart Device Manufacturer will only be held responsible for failing to apply security updates and patches. The use of third-party software, such as the Linux kernel, will not result in the attachment of liability for unknown and as of yet undiscovered vulnerabilities within that software, but instead liability will only attach for failing to apply security remedies to vulnerabilities which have become public. The well-known and extensively discussed issues involved in detecting and remedying vulnerabilities in open-source software,[31] is not proposed to be a factor in determining liability for Smart Device

26 See, e.g., Jonathan Greig, 'CISA Directs Federal Agencies to Track Software and Vulnerabilities' *The Record* (3 October 2022) <https://therecord.media/cisa-issues-directive-ordering-federal-agencies-to-track-software-used-and-vulnerabilities/> accessed 16 October 2022; and National Cyber Security Centre, 'Vulnerability Management' (2016) Guidance <https://www.ncsc.gov.uk/guidance/vulnerability-management> accessed 16 October 2022; and National Institute of Standards and Technology, 'CVEs and the NVD Process' <https://nvd.nist.gov/general/cve-process> accessed 16 October 2022.

27 PricewaterhouseCoopers (Switzerland), 'Vulnerability Management: Why Managing Software Vulnerabilities Is Business Critical and How to Do It Efficiently and Effectively' (2021) <www.pwc.ch/cybersecurity> accessed 10 September 2021.

28 See, e.g., Rebecca Herold, David Lemire and Noel Hoehn, 'IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements' (National Institute of Standards and Technology 2021) Special Publication 800–213 <https://doi.org/10.6028/NIST.SP.800-213> accessed 16 October 2022; and Michael Fagan and others, 'Foundational Cybersecurity Activities for IoT Device Manufacturers' (National Institute of Standards and Technology 2020) NISRIR 8259 <https://doi.org/10.6028/NIST.IR.8259> accessed 16 October 2022; and Internet Society, 'IoT Security for Policymakers' (2008) <https://www.internetsociety.org/resources/2018/iot-security-for-policymakers/> accessed 16 October 2022; and National Cyber Security Centre, 'Device Security Guidance' (2022) <https://www.ncsc.gov.uk/collection/device-security-guidance/security-principles/provide-updates-securely> accessed 16 October 2021 for a discussion on why patching vulnerabilities is a requirement for cybersecurity.

29 See, e.g., Artturi Juvonen and others, 'On Apache Log4j2 Exploitation in Aeronautical, Maritime, and Aerospace Communication' (2022) 10 IEEE Access 86542; and Naba M Allifah and Imran A Zualkernan, 'Ranking Security of IoT-Based Smart Home Consumer Devices' (2022) 10 IEEE Access 18352; and Tiago M Fernández-Caramés and Paula Fraga-Lamas, 'Teaching and Learning IoT Cybersecurity and Vulnerability Assessment with Shodan through Practical Use Cases' (2020) 20 Sensors 3048 for a discussion on vulnerabilities. .

30 Peter Weidenback and Johannes vom Dorp, 'Home Router Security Report 2020' (Fraunhofer-Institut fur Kommunikation, Informationsverabeitung und Ergonomie 2020) <https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf> accessed 18 February 2022.

31 See, e.g., Chinmayi Sharma, 'Tragedy of the Digital Commons' (2022) Forthcoming North Carolina Law Review for a discussion on the challenges of sourcing security vulnerabilities and developing patches for open source software projects. and James Lewis, 'Heartbleed and the State of Cybersecurity' (2014) 36 American Foreign Policy Interests 294; and Keith Larson, 'Visibility Key to Log4j Response' *Control* (18 January 2022)

Manufacturers, merely that they apply security updates once they have become publicly available. It is possible that other actions by a Smart Device Manufacturer may give rise to a claim for negligence, but such hypothetical actions are not included in this paper.

An immediate criticism of this approach is that, as it stands, it creates the potential for an open-ended obligation to be placed on a Smart Device Manufacturer so that security updates are provided for the working life of every Smart Device sold, which is unreasonable and, as discussed later in this paper, will poison the ability to mount a successful negligence claim. However, there are two pieces of legislation, one enacted and one proposed, which would outline a minimum set of cybersecurity requirements for Smart Devices in both the UK and in Ireland. Within the UK, the Product Security and Telecommunications Bill,[32] allows for the introduction of minimum standards in relation to cybersecurity for Smart Devices which have been released in the UK. Within the EU, the proposed Cyber Resilience Act also outlines minimum standards in relation to cybersecurity for Smart Devices which have been released in the Common Market. The requirements which arise from these pieces of legislation will allow the courts to apply a relevant, clear and constrained set of cybersecurity obligations on Smart Device Manufacturers. For convenience, for the duration of this paper, we refer to these proposed pieces of legislation which outline minimum cybersecurity standards as the 'Proposed Requirements'. It is important to note that the UK's Product Security Bill does not grant consumers a direct right of action where a Smart Device Manufacturer is not in compliance with the bill's security requirements, and so the bill will not prohibit a negligence claim by either a first- or third-party. Within the Common Market, the proposed Cyber Resilience Act will form part of the product's CE mark, and so will not prevent a remote third party from bringing a negligence claim as they have no standing under the Product Liability Directive.[33]

Why should Smart Device manufacturers be liable to third parties?

As discussed above, in-scope Smart Device attacks represent a specific niche of cyber-attacks, where the attack is conducted by a criminal actor, but it is enabled by a cybersecurity flaw which is present in an intermediate Smart Device. It is this compromised Smart Device (normally in conjunction with many others) which is used to carry out the attack against a third party. What distinguishes this cyberattack from most others is the fact that while the Smart Device is owned or operated by a consumer, it is not, in any real sense of the word, controlled or administered by its user. The extent of control is determined by the Smart Device Manufacturer and the choice of whether to grant the owner administrative control is the sole gift of the Smart Device Manufacturer.[34] Given the level of control that the Smart Device Manufacturer maintains, as they retain either active control over the Smart Device or choose not to retain an active control over the Smart Device (where, for example, the Smart Device Manufacturer chooses not to enable the ability to remotely update the Device) but still prevents the Smart Device owner from obtaining administrative control of the Smart Device, the traditional perspective where the manufacturer's responsibility in statute for a product terminates once the product has left the factory is not appropriate, as the Smart Device Owner will not have administrative control over the Smart Device which they purchased.

<https://www.controlglobal.com/protect/cybersecurity/article/11288976/visibility-key-to-log4j-response> accessed 16 October 2022 for a discussion of this topic.

32 Product Security and Telecommunications Infrastructure Bill 2022. The proposed standards were introduced in the Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations (S.I. No 1007) and will take effect in April 2024.

33 Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products 1985 (OJ L 210).

34 'Administrative Control' is used in the context of a system administrator as outlined in, e.g., Aeleen Frisch, *Essential System Administration* (3rd Edition, O'Reilly Media Inc 2002).

It is a perfectly logical and valid counter argument to outline how the consumer purchaser of a non-smart device, such as a fridge, toaster, or thermostat, is subject to the same level of restrictions. They are only able to use the device in the manner which was determined and prescribed by the manufacturer. The owner of a kettle, for example, is unable to control the temperature to which it will heat the water, they can only turn the kettle on or off. While this argument is correct (total control over the device is not granted to the consumer user), the user is protected from a fault or issue with the product through product liability legislation. That the device cannot be used as a tool to engage in attacks against remote people means that existing product liability legislation is sufficient to grant protection for all relevant (local) users against an error by the product's manufacturer, and where the error results in harm, the consumer can bring an action for redress via negligence or breach of statutory duty.[35] However, this is insufficient for Smart Devices, as the Device can be used to conduct cyberattacks against remote third parties if the manufacturer makes a foreseeable mistake with regards to cybersecurity of the device, and there is no recourse possible for the victim via product liability legislation, as the victim of the attack is neither the owner nor user of the product, and will not be in a direct nexus with the product. Indeed, it is likely that the remote victim could reside in a different country or even continent from the Smart Device.

It is clear, therefore, how there is a lacuna in existing legislation in relation to the accountability of the Smart Device Manufacturer as if there is a physical issue arising in the device, this is covered under product liability, even if the issue doesn't cause harm or loss to the consumer. The physical aspect of the Smart Device is covered by a variety of regulatory standards, and while there have been legislative improvements which extend product liability to cover the digital aspects of the product, they do not protect third parties who suffer harm or loss as a result of the manufacturer's failure and indeed have only recently begun to protect the owner or user of the product.[36] This lacuna is augmented further by the fact when detection of compromised Smart Devices is discussed in the literature, there is little reference to owners of the compromised devices being a meaningful mechanism for detection.[37] This is due to the unattended nature of the Smart Device, and the fact that the cyberattacker will be 'time sharing' the Smart Device rather than using it exclusively. Time sharing is the concept where multiple distinct users will 'share' a computer's resources to carry out simultaneous but distinct actions, and so long as one user is not conducting a particularly onerous task, the performance reduction for other users will be negligible.[38] At the time of this publication, a successful claim has not been brought by a consumer in relation to a failure of a Smart Device on the basis of defective cybersecurity. This is most likely explained by the fact that most cybersecurity failures do not cause the device to stop functioning as expected; rather they will also carry out the functions of the cyberattacker, in addition to their normal operation, so there is no ground for a claim through Product Liability. The ability for a third party to seek redress following loss or harm,

35 E.g., if the user is resident within the Common Market, they can seek redress through their local implementation of the Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.

36 See, e.g., Directive 2019/771 on certain aspects concerning contracts for the sale of goods 2019 (OJ L 136); Directive 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services 2019 (OJ L 136); Consumer Rights Act 2015 which extend the protections of the physical good to the digital element o the good. However, these examples do not incorporate cybersecurity standards as a protection unless the manufacturer has made a specific claim in relation to the security of the good which is discovered to be untrue.

37 See, e.g., Wainwright and Kettani (n 9); Gulbadan Khehra and Sanjeev Sofat, 'Botnet Detection Techniques: A Review', *2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS)* (IEEE 2018) <https://ieeexplore.ieee.org/document/8663082/> accessed 13 September 2020; Negash and Che (n 9).

38 Peter Clark, 'DEC Timesharing' (1965) 1 The DEC Professional.

based on recent decisions which are discussed further on in this paper, is a means to close this lacuna.

Establishing Negligence

The first step in establishing whether a third-party victim of a cyberattack can ground a claim in negligence against a Smart Device Manufacturer, is to determine if a duty of care exists between the two parties. It is a simple and uncontroversial fact of law that a manufacturer of a product, or the provider of a service can be fixed with a duty of care not only to a first party, but also to a third party who may be unknown to them.[39] As such, would a claim by a third-party victim, as outlined earlier in this paper, against a Smart Device Manufacturer for negligence arising from harm or loss caused by a Smart Device, which was sold to an unharmed consumer and which had insufficient cybersecurity protection to the extent that a third party was able to gain control and carry out the attack, be considered under an existing duty of care? The answer would have to be seen as highly unlikely. The extent of a manufacturer's duty of care towards a claimant is determined, *inter alia*, by their proximity to the claimant,[40] and there are no examples of cases where a manufacturer has been found to have sufficient proximity to an unknown claimant who suffered harm or loss at the hands of the criminal actions of a third party who used the product of the manufacturer to cause the claimant's harm or loss.[41]

The current approach in English law, to determine whether a duty of care is owed is summarised in *Robinson*,[42] where it is outlined how the court will seek to fit the facts of the case before them into existing, distinct categorisations of duty of care, and use these past decisions to infer either the presence or absence of a duty of care between the parties in the case before them. Only when a situation is novel, will the courts return to a 'first principles' approach, and it must be noted how there is a reluctance to do so, in order to maintain coherency and consistency in the recognition of a duty of care between parties.[43]

Do third-party victims of cyberattacks involving Smart Devices fall under an existing categorisation of a duty of care? Or do they represent a novel situation? One argument that would suggest it is the latter is that the nature of Smart Devices has resulted in new legislation being introduced in the UK, EU and in other jurisdictions to ensure that sale of goods legislation continues to function as expected,[44] or in other words, Smart Devices did not fit the traditional definition of a consumer product, and legislative changes were needed to ensure that consumer protection for Smart Devices remained equivalent to traditional products. Furthermore, the unique role that a Smart Device Manufacturer plays in protecting the consumer from cyberattacker has also been recognised by

---

39 See, e.g., *Muirhead v Industrial Tank Specialities Ltd and others* [1985] 3 All ER 705; *Aswan Engineering Establishment Co v Lupdine Ltd and Another (Thurgar Bolle Ltd, third party)* [1988] LRC (Comm) 313 for an overview of the duty care of care owed to third parties in the case of defective products, and ; and see, e.g., *D&F Estates Limited and Ors v Church Commissioners for England & Ors* [1988] 1 AC 177 for an overview of the duty of care owed to third parties in relation to a defective provision of a service.

40 *Corr v IBC Vehicles Ltd* [2008] UKHL 13 893.

41 See, e.g., *Breslin v Corcoran & Motors Insurers Bureau of Ireland* [2003] IESC 23 as an example of where such a set of circumstances were examined.

42 *Robinson v Chief Constable of West Yorkshire Police* [2018] UKSC 4 WL 00747028, [21] – [30]

43 *McFarlane and Another Respondents v Tayside Health Board Appellants* [2000] 2 A.C. 59, 108.

44 See, e.g., Directive 2019/771 on certain aspects concerning contracts for the sale of goods 2019 (OJ L 136); Directive 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services 2019 (OJ L 136); Consumer Rights Act 2015 which extend the protections of the physical good to the digital element of the good. However, these examples do not incorporate cybersecurity standards as a protection unless the manufacturer has made a specific claim in relation to the security of the good which is discovered to be untrue.

policy makers in the EU, UK and in other jurisdictions, and legislation has either been passed or proposed to impose a positive, ongoing duty to ensure that the security of Smart Device is maintained for a reasonable period of time.[45] Accordingly, it is hard to argue that a Smart Device would fit an existing categorisation of a duty of care, given how the nature of the product required new consumer protection legislation and the unique role of the Smart Device Manufacturer has been recognised in legislation in different jurisdictions.

The current, general,[46] test in English law for determining if a novel duty of care can be established is outlined in *Caparo,*[47] and the tripartite principles established in the case have also been used in Irish law.[48] The three elements which a claimant must demonstrate is whether the harm was reasonably foreseeable, if there was a sufficiently proximate relationship between the parties and if there is there a just and reasonable basis to impose a duty of care.

Foreseeability of harm

A fundamental question in determining whether a duty of care can exist is whether it is reasonably foreseeable that a Smart Device, which contains a known but unpatched exploitable vulnerability, will be used to cause harm to a third party? To correctly answer this question, the normal deployment of a consumer's Smart Device must be examined.

It is reasonable for a Smart Device Manufacturer to believe that a Smart Device will be deployed in a consumer's residence, and it will be connected to a router.[49] However, it must be recalled that internet access from a consumer's home is enabled via a Smart Device which is commonly called a 'router'. The router is supplied by the consumer's Internet Service Provider ("ISP") and can be considered as a device of two 'halves'. The first half of the device contains the consumer's ISP account details, and is connected directly to the internet, usually via a fibre optic, PSTN or radio connection. This half of the router will be assigned an Internet Protocol or 'IP' address which can be accessed from any device which is connected to the internet. All internet traffic, whether originated from the consumer's home or sent to the consumer's home by other online resources (e.g., the data needed to load and render a web page or the data-stream from Zoom) will flow through this IP address. An analogy for an IP address is the front door of a building – this is where people enter or leave the building, no matter what room or floor of the building that they are going to.

The second half of the router is the Local Area Network (the "LAN") which is present only in the consumer's home. All of the person's computing devices, which are in her home and that require an internet connection will connect to the LAN.[50] This connection is usually via WiFi or via an ethernet cable. These connections may be permanent, such as for Smart Devices or intermittent, such as for

45 See (n 32) and (n 33)

46 It must be noted that in recent cases such as *Poole BC v GN* [2019] UKSC 25 a different test called the 'voluntary assumption of responsibility' test was applied instead of Capero. However, this test requires that a direct connection and interaction exist between the claimant and the defendant, and so is not applicable in the scenario examined by this paper. The Capero test, although not used, was affirmatively cited in Poole.

47 *Caparo Industries PLC v Dickman* [1990] 2 AC 605.

48 See, e.g., *Glencar Exploration p.l.c v Mayo County Council (No 2)* [2001] IESC 64.

49 See, e.g., Allifah and Zualkernan (n 29); Roni Mateless and others, 'IPvest: Clustering the IP Traffic of Network Entities Hidden Behind a Single IP Address Using Machine Learning' (2021) 18 IEEE Transactions on Network and Service Management 3647; Bassam Naji Al-Tamimi, Mohamed Shenify and Rahmat Budiarto, 'PROTECTING HOME AGENT CLIENT FROM IPv6 ROUTING HEADER VULNERABILITY IN MIXED IP NETWORKS' 17; Javid Habibi and others, 'Heimdall: Mitigating the Internet of Insecure Things' (2017) 4 IEEE INTERNET OF THINGS JOURNAL 968 for a discussion of the average set of a consumer's home network.

50 O Hundt and others, 'Methods to Improve the Efficiency of Wireless LAN for Multimedia Home Networks' (2007) 53 IEEE Transactions on Consumer Electronics 8.

mobile devices which often leave the premises or are routinely powered off.[51] The router will assign each of these devices a local 'internet protocol' (IP) address, but this address is only accessible to other devices which are on the LAN; it is not accessible to any devices which are not connected to the LAN.

When a device, which is a member of the LAN, wants to connect with an external device or service on the Internet, it will send a request to the router and the router will create a connection to the internet, establishing the pathway to the requested remote device. When this remote device sends a response, it is delivered to the router, which then forwards the response through the LAN to the consumer's device which is expecting it.[52] This is a concept called network address translation ("NAT"), and it means that a consumer's device which is present on a LAN will never actually engage directly with a remote device. More importantly, from the perspective of cybersecurity, a remote service will only ever engage with the router and not with the devices on the LAN. The router, as a matter of course, will only forward on a remote service if a device on the LAN has asked for it.[53]

NAT is the standard way in which consumer router devices operate, suggesting that any devices which are unpatched and contain a vulnerability are protected by the fact that no remote attacker will be able to access them, unless requested to by the vulnerable device itself. Theoretically, no remote attacker will be able to search and seek for a vulnerable consumer device as they will only be able to engage with the first half of the router which is connected to the internet.[54] Accordingly, for a Smart Device which is located behind a router, this would suggest that a Smart Device Manufacturer would not have an expectation that an unpatched Smart Device can be accessed by a cyberattacker.

However, Smart Devices are designed to be accessible from the internet while working through NAT.[55] A Smart Device which cannot be accessed remotely (e.g., a camera or thermostat) will not be able to provide the "Smart" features to a consumer since they will only be able to access and use the device when physically present in the same premises as the device. Therefore, Smart Devices will instruct the router to open a 'port' and to forward all traffic on that port to the Smart Device.[56] The Smart Device will then send the IP address of the router to the services which a consumer will use to access the device, along with the port number.[57] Any requests which are made of that IP address and port number will be automatically delivered to the Smart Device. The router will not block traffic which originated on the internet and will not prevent a third party from confirming that

51 K Jostschulte, R Kays and W Endemann, 'Enhancement of Wireless LAN for Multimedia Home Networking' (2005) 51 IEEE Transactions on Consumer Electronics 80.

52 Fu-Hau Hsu and others, 'Handover: A Mechanism to Improve the Reliability and Availability of Network Services for Clients behind a Network Address Translator' (2018) 67 Computers & Electrical Engineering 159.

53 See, e.g., Takashi Yamanoue, 'Monitoring of Servers and Server Rooms by IoT System That Can Configure and Control Its Terminal Sensors Behind a NAT Using a Wiki Page on the Internet' (2020) 28 Journal of Information Processing 204 for an overview of NAT functionality.

54 Younchan Jung and Ronnel Agulto, 'Virtual IP-Based Secure Gatekeeper System for Internet of Things' (2020) 21 Sensors 38.

55 See, e.g., Aamir H Bokhari and others, 'Empirical Analysis of Security and Power-Saving Features of Port Knocking Technique Applied to an IoT Device' (2021) 29 Journal of Information Processing 572; F Paolucci and others, 'P4 Edge Node Enabling Stateful Traffic Engineering and Cyber Security' (2019) 11 Journal of Optical Communications and Networking 84.

56 See, e.g., Mateless and others (n 71); Xiaobo Ma and others, 'Inferring Hidden IoT Devices and User Interactions via Spatial-Temporal Traffic Fingerprinting' (2022) 30 IEEE/ACM Transactions on Networking 394.

57 For example, if a router has an IP address of 11.12.13.14, and a Smart Camera has requested port 4455 to be opened, any internet connected device can send a request to 11.12.13.14:4455 and this request will be delivered directly to the Smart Camera, irrespective of whether the Smart Camera had initiated the exchange or not.

a device which is LAN resident is listening for traffic on that port. This issue is further compounded by the fact that most Smart Devices (as well as Smart Device Manufacturers) are normally consistent in their choice of port number which will allow a cyberattacker to narrow the range of ports which need to be scanned when searching for a vulnerable Smart Device.

It must be noted at this stage that although consumer routers which employ NAT offer security benefits when compared to directly connecting Smart and other devices to the internet, NAT itself is not a security solution but was developed primarily to reduce the number of IP addresses required by consumers as there is a finite number of IPv4 addresses available globally.[58]

From this, it can be seen how a core risk associated with a Smart Device is that an attacker can automatically scan the IP address which is assigned to the router and identify that a Smart Device is present. Once identified, the cyberattacker can use automatic tools which will try and access the device by trying commonly used user-names and passwords and by looking to see if vulnerabilities are present in the Smart Device and exploiting them to gain access. Therefore, it is starting to become clearer how an unpatched vulnerability, even when placed behind a router, can lead to exploitation of the Smart Device by a remote cyberattacker.

Several studies have been conducted which sought to establish the time it would take an attacker who was using automated IP and port scanning to identify a new device connected to the internet. These studies were conducted in the early 2000s, as NAT routers were not commonly used at the time and devices were connected directly to the internet via a phone (PSTN) line. Cybersecurity researchers identified that the device was found and scanned in time frames ranging from five minutes in 2008,[59] twenty minutes in 2004,[60] and up to one thousand minutes (sixteen hours) under circumstances which replicated a consumer's network set-up in 2008.[61] A 2019 analysis of a cyberattacker's automated tools established how they were able to add c. 33,000 new devices to a botnet in thirty one hours by exploiting an unpatched vulnerability, which demonstrates how automated scanning and attack tools are still both operating and an efficient means of compromising Smart Devices.[62]

These findings have been replicated in an exercise carried out in Japan, where the Ministry of Internal Affairs and Communications, the National Institute of Information and Communications Technology, and the ICT Information Sharing and Analysis Center Japan, in cooperation with local ISPs, are analysing every single internet connected household via automatic means and searching for IoT devices which can be accessed directly from the internet and which have weak or otherwise insecure login details. The scan is also searching for evidence of malware, and where found the household will be notified via their ISP.[63]

---

58 Yair Meidan and others, 'A Novel Approach for Detecting Vulnerable IoT Devices Connected behind a Home NAT' (2020) 97 Computers & Security 101968.

59 Lorna Hutcheson, 'Survival Time on the Internet' (*Internet Storm Centre*, 13 July 2008) <https://isc.sans.edu/diary/Survival+Time+on+the+Internet/4721/> accessed 1 October 2022.

60 Robert Lemos, 'Study: Unpatched PCs Compromised in 20 Minutes' [2004] *CNET* <https://www.cnet.com/news/privacy/study-unpatched-pcs-compromised-in-20-minutes/> accessed 1 October 2022.

61 Gregg Keizer, 'Unpatched Windows PCs Fall to Hackers in under 5 Minutes, Says ISC' [2008] *Computerworld* <https://www.computerworld.com/article/2534742/unpatched-windows-pcs-fall-to-hackers-in-under-5-minutes--says-isc.html> accessed 1 October 2022.

62 Stephen Herwig and others, 'Measurement and Analysis of Hajime, a Peer-to-Peer IoT Botnet', *Proceedings 2019 Network and Distributed System Security Symposium* (Internet Society 2019) <https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_02B-3_Herwig_paper.pdf> accessed 3 October 2022.

63 'Overview of the NOTICE and NICTER Projects' <https://notice.go.jp/en> accessed 19 October 2022.

As of August 2022, the operation has detected c. 189,000 Smart Devices which could be accessed directly from the internet, and of which c. 52,000 (27.5%) had weak or non-secure user-names and passwords.[64] Furthermore, during August the project had detected c. 1,500 IP addresses per day which seemed to have a networked device which contained malware, a figure which although lower than the c. 2,500 devices identified per day in July and down from the peak of 3,288 devices identified per day during June 2022, can be considered as quite high.[65] It is hard to disagree in the face of the evidence gathered over almost the past two decades, that it is not reasonable to foresee that an unpatched Smart Device, even when connected to the internet via a router, will be identified and an exploitation attempted using either weak default credentials or an known vulnerability in short order.

Causation and Proximity

The second element of the *Caparo* tripartite is to determine if there was a sufficiently proximate relationship between the parties, and if the actions of the defendant will satisfy the tests for causation. Without wishing to juxtapose causation with the imposition of a duty of care, the question as to whether the act of the cyberattacker counts as a *Novus Actus Interveniens*, and so represents an irrecoverable break in the chain of causation, can be used both to answer the question as to whether there is sufficient proximity between the two parties in order to determine if a duty of care should be established, and also used (assuming that a duty of care can be established) to determine whether there is a sufficient break in the causal link in order to deny a negligence claim. The latter element is discussed in more detail further on in this paper. The question of how to determine whether a deliberate and criminal act of a third party represents a break in the chain of causation has been discussed in detail in cases such as *Smith & Ors v Littlewoods*,[66] and in *Mitchell v Glasgow City Council*.[67] While the results of these cases suggest that apart from the narrowest and most esoteric of circumstances, the third party's deliberate and criminal act does sever the chain of causation and so demolishes any duty of care between the defendant and the victim, the facts of the cyberattack using a Smart Device suggest that it may well be an exception to the general rule. Unlike *Smith,* as has been determined earlier in this paper, the foreseeability of a Smart Device being subjected to an attempted cyberattack is not only a probability, it is a certainty and the consequences of a successful cyberattack resulting in an availability attack are well known and understood, while in *Mitchell*, the claim foundered as the defendant was not responsible for, and had not assumed any such responsibility for, the claimant's safety,[68] whereas recent legislative changes in the UK (and forthcoming legislative changes in the EU) have imposed a responsibility on the Smart Device Manufacturer to maintain the security of the Smart Device post sale, thus establishing on on-going relationship between the Smart Device Manufacturer and the Smart Device.

The question, however, can be better examined from the context of the cyberattack proposed in this paper by a case from the Irish courts, that of *Breslin v Corcoran*,[69] which examines in detail some of the key questions that must be asked when examining a cyberattack against a third-party. It is noted that while Ireland operates a common law jurisdiction, and while English jurisprudence is routinely

64 The Ministry of Internal Affairs and Communications, 'August Update' (2022) National Operation Towards IoT Clean Environment (NOTICE) <https://notice.go.jp/docs/status_202208_en.pdf> accessed 19 October 2022.

65 ibid.

66 *Smith & Ors v Littlewoods Organisation Ltd* [1987] 1 AC 241.

67 *Mitchell and another v Glasgow City Council* [2009] UKHL 11, 1 AC 874.

68 ibid 890 D.

69 *Breslin v Corcoran & Motors Insurers Bureau of Ireland* (n 59).

cited in Irish cases,[70] and indeed the case in question is similar to, and relies on the English case of *Topp*,[71] the judgement in question is not binding in English law. Despite this, however it is a persuasive judgement and there is no barrier which would prevent its discussion in a similar English case.[72]

In *Breslin*, the owner of a car had left it idling on a street while he entered a coffee shop. As he was returning, he saw a thief enter the car and abscond with the vehicle. The thief subsequently undertook a joyride which resulted in injuries to the plaintiff, who sought damages both from Motor Insurance Bureau of Ireland (the entity which operates a fund to cover the damage arising from uninsured drivers) and from the owner of the car. While the plaintiff succeeded in his initial action in the Irish High Court,[73] the decision was overturned upon appeal to the Supreme Court, where it was held that the actions of the thief stealing the car broke the chain of causation as it was not reasonably foreseeable that a) the car would be stolen, b) the thief would engage in a joyride and c) that the joyride would occasion the injury of a passer-by.

At first reading, the finding would support the general principle that one party cannot be held responsible for the actions of another and so a duty of care could not be imposed upon Smart Device Manufacturers towards victims of cybercriminal who had exploited the Smart Device Manufacturer's failure to update their Smart Devices, however, as stated by Fennelly J;[74]

> "… I draw the following conclusion. A person is not normally liable, if he has committed an act carelessness, where the damage has been directly caused by the intervening *independent* act of another person, for whom he is not otherwise vicariously responsible. *Such liability may exist, where the damage caused by that other person was the very kind of thing which he was bound to expect and guard against and the resulting damage was likely to happen, if he did not."*

It is clear that where the acts of the third party are to be expected, and there is at least a preventative relationship between the first party and the actions of the third, liability can be found. Taking the conclusion of Fennelly J, and given how in the specific context of Smart Devices it is recognised that once a Smart Device has been connected to the internet, there will be automated attempts by nefarious third parties to firstly identify that such a device has now been connected to the internet, and, secondly, to automatically attempt to access the device via known exploits and known security vulnerabilities (such as automated username and password attacks).[75] Accordingly, if a Smart Device

---

70 Indeed, English and Scottish cases are cited throughout this judgement. However, at the time of writing (30 December 2021) there is no suggestion that this case has been cited within a UK judgement.

71 *Topp v London Country Buses (South West) Ltd* [1993] EWCA Civ 15 .

72 At the time of writing, however, the author of this paper could not find any example where the case had been used in an English court.

73 *Breslin v Corcoran & Anor* [2001] IEHC 238.

74 *Breslin v Corcoran & Motors Insurers Bureau of Ireland* (n 59) para 31 (emphasis added).

75 See, e.g., Giovanni Bottazzi and Gianluigi Me, 'The Botnet Revenue Model', *Proceedings of the 7th International Conference on Security of Information and Networks - SIN '14* (ACM Press 2014) <http://dl.acm.org/citation.cfm?doid=2659651.2659673> accessed 22 September 2020; Masarah Paquet-Clouston, David Decary-Hetu and Olivier Bilodeau, 'Cybercrime Is Whose Responsibility? A Case Study of an Online Behaviour System in Crime' (2018) 19 Global Crime 1; Zhen Li and Qi Liao, 'Toward a Monopoly Botnet Market' (2014) 23 Information Security Journal: A Global Perspective 159; Manos Antonakakis and others, 'Understanding the Mirai Botnet', *26 Usenix Security Symposium* (2017); Hwankuk Kim, Taeun Kim and Daeil Jang, 'An Intelligent Improvement of Internet-Wide Scan Engine for Fast Discovery of Vulnerable IoT Devices' (2018) 10 SYMMETRY-BASEL 151; Seul-Ki Choi, Chung-Huang Yang and Jin Kwak, 'System Hardening and Security Monitoring for IoT Devices to Mitigate IoT Security Vulnerabilities and Threats' (2018) 12 KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS 906.

manufacturer releases a Smart Device for sale, and it either contains a known vulnerability or one is subsequently discovered and not remedied, it is only short a matter of time before such a device is identified by the cyberattacker's automated scanning programs, and once identified, subversion attempts using known exploits will be attempted, and the quantitative evidence cited earlier in this paper suggests that such attacks will take place within minutes and hours of the Smart Device going online, as opposed to some indeterminate time in the far off future.

Therefore, in the limited case of Smart Devices, it is reasonable for a Smart Device manufacturer to know that a vulnerable device will be both identified and compromised, because of the automated tools which are persistent threats to all internet connected devices, and as such, the compromise of the device and its use to carry out cyberattacks is foreseeable. This level of foreseeability would, in this narrow and specific context, appear to meet the conclusion of Fennelly J and allow the questions of causation and proximity to be satisfied with regards to the establishment of a duty of care.

The Omissions Problem

However, it must be recognised that, in English law (and indeed, in most common law jurisdictions), "*It is one thing to require a person who embarks on action which may harm others to exercise care. It is another matter to hold a person liable in damages for failing to prevent harm caused by someone else.*"[76]

The omissions rule is not absolute, however, and there have been notable exceptions such as the case of *Robinson,*[77] where it was held that there are occasions when both public and private bodies can be found to have a duty a care towards a party where 'responsibility' has been taken by the first party to the second.[78] Thus, a key question to be answered is whether a Smart Device manufacturer could be found to have a responsibility to the victims of a cyberattack facilitated by negligent cybersecurity, even though the harm was caused by a third-party. It will be necessary to demonstrate how this question can be answered in the affirmative in order to meet the requirement of the second element of the *Caparo* tripartite test.

Returning to the question of whether a Smart Device Manufacturer can be said to ever have a responsibility towards the victims of a cyberattack which was conducted through exploitation of a Smart Device created by them, the current leading cases would suggest that this would be a very difficult hurdle to clear, as where a duty of care has been found, it has been in cases where there was a strong and formal relationship between the parties, such as where a party was acting *in loco parentis*,[79] or where the party had given express authorisation for the conduct in question. It is not proposed in this paper to argue that there exists a formal relationship between a Smart Device manufacturer and the victim of a cyberattack, and indeed it is conceded that the cyberattacker will be unknown to the Smart Device Manufacturer, although it is maintained that the attempted attacks made by any given cyberattacker are foreseeable.

Tofaris and Steele have summarised the question of duty of care as including the situation where '*A has a special level of control over that source of danger'*.[80] This definition has been cited affirmatively

76 *Michael and others (FC) v The Chief Constable of South Wales Police and another* [2015] UKSC 2 WL 55945 [97].

77 *Robinson v Chief Constable of West Yorkshire Police* [2018] UKSC 4 WL 00747028.

78 See *Gorringe (by her litigation friend June Elizabeth Todd) (FC) v Calderdale Metropolitan Borough Council* [2004] UKHL 15 [39–40] for a more complete explanation of this exception.

79 *Barrett v Enfield LBC* [2001] 2 AC 550.

80 Stelios Tofaris and Sandy Steel, 'NEGLIGENCE LIABILITY FOR OMISSIONS AND THE POLICE' (2016) 75 The Cambridge Law Journal 128.

in the UK Supreme Court,[81] is persuasive and can accordingly be read as good law. In the specific case of Smart Devices, the Smart Device manufacturer is the only party who has control over the source of danger of a cyberattacker who is using a known vulnerability to engage in a cyberattack as the Smart Device Manufacturer is the only entity who can manage and control the source code of the Smart Device.[82] There are no other parties who are able to remedy any deficiencies in the code in order prevent the attacker from exploiting a vulnerability, and while it could be argued that consumer owners of Smart Devices and third party entities could avail of additional cybersecurity services to deflect an attack caused, this shifts the burden of the externality away from the producer and onto the world at large. Accordingly, in the limited case of Smart Devices, there does seem to be a scaffold which has been accepted by the UK Supreme Court which a claimant can use to clear the hurdle of attaching liability on a third party for an omission.

The question of what constitutes 'a special level of control', as presented in *Robinson,* is discussed in *Rushbond*.[83] While there have been a number of cases heard which examine omissions since *Robinson*,[84] and although these cases affirm the 'special level of control' exception, *Rushbond* is the only case to date which examines this exception in some, if rather limited detail.[85] The case involves the owner of a dis-used cinema, who was exploring the possibility of renovating the property with an architect and building surveyor, which required on-site visits by these specialists. In the normal course of events, when the architect accessed the property, they did so in the presence of an estate agent who facilitated access to the building. However, on the day in question, the estate agent was unable to visit the property and so gave the key to the architect, who then accessed the property unaccompanied.

During their visit, it was agreed by all parties that they opened a door which allowed access to the street, and did not lock the door after using it, as was the custom with the estate agent. This door, due to it not having a self-activating lock, would have then opened in the wind and enabled access to the building from the street for a third-party. The evening after the visit of the architect, a fire was started in the property, and it was argued this was caused by an unknown third-party who gained access because of the negligence of the architect.

---

81 *Robinson v Chief Constable of West Yorkshire Police* (n 77) para 34.

82 In many cases the Smart Device Manufacturer will own their source code, however, given that it is not uncommon for Smart Device Manufactures to use third party modules, many of which are open-sourced and licenced under the GNU General Public Licence, ownership is not a given. This, in no way, undermines or limits the control that the Smart Device Manufacturer has over their code base. Smart Device Manufacturers have total control over their own codebase, irrespective of the ownership of any given module, as they determine its composition and have full control over what code is deployed to the Smart Device. It is noted, of course, that should a Smart Device Owner amend the software on their device, than this argument will break down. This is discussed in more detail further on in this chapter.

83 *Rushbond PLC v The JS Design Partnership LLP* [2021] EWCA Civ 1889, 2021 WL 05890119.

84 See, e.g., *Poole Borough Council v GN (through his litigation friend 'The Official Solicitor') and another* [2019] SC 25, [2017] EWCA Civ 2185; *The Chief Constable of Essex Police v Transport Arendonk BVBA* [2020] EWHC 212 (QB); *ABC v St George's Healthcare NHS Trust, South West London and St George's Mental Health NHS Trust, Sussex Partnership NHS Foundation Trust* [2020] EWHC 455 (QB), 2020 WL 00978000; *YXA (a protected party by his Litigation Friend, The Official Solicitor to the Senior Courts) v Wolverhampton City Council* [2021] EWHC 1444 (QB), 2021 WL 02194754; *DFX (A Protected Party by her Litigation Friend the Official Solicitor), RFX, SFX (A Protected Party by her Litigation Friend the Official Solicitor), DGX (A Protected Party by his Litigation Friend, TG) v Coventry City Council* [2021] EWHC 1382 (QB), 2021 WL 02109484; *Tindall and another v Chief Constable of Thames Valley Police and another* [2022] EWCA Civ 25.

85 *Rushbond PLC v The JS Design Partnership LLP* (n 83) para 41.

This was contested by the plaintiffs,[86] who argued that by holding the key to the door where it was believed the unknown third party gained access to the property, the architect had a 'special level of control' over the property and, according to the criteria as outlined by Tofaris and Steele in *Robinson,*[87] could be held liable. This was not held by O'Farrel J, as the architect was not an expert in building security, fire control or door locks. Furthermore, as there had been no dealings between the two parties involved, it was found that reliance upon one party by the other was unreasonable.[88]

While the outcome of *Rushbond* is illustrative in answering the question of whether a Smart Device Manufacturer owes a duty of care to the victim of a cyberattack, it is unfortunate that this element of law remains relatively underdeveloped in comparison to the other elements of Tofaris and Steele's determinates of duty of care.[89] However, despite the short treatment, it is still possible to derive the two elements which drove O'Farrel J's decision. The first is that the defendant must demonstrate, or have held themselves out as having some special knowledge or expertise relating to the third party's action. In relation to a Smart Device Manufacturer, this would be a simple hurdle to clear as there is no other entity who has as much specialist knowledge in relation to both the software and the security of the Smart Device. Quite simply, there is no plausible way for a Smart Device Manufacturer to claim that they don't have expertise relating to their own products.

The second element of the judgment requires that there is some relationship between the two parties which can ground the reliance of the plaintiff on the party. On its face, this would seem to act as a barrier which prevents the successful raising of an omissions claim since it has already been accepted earlier in this paper that the Smart Device Manufacturer will not be aware of the specific identity of the cyberattacker and will not have engaged with them in anyway. However, O'Farrel J's second requirement must be read in the context of the facts of the case; there had been no dealings between the two parties, although one party had been given temporary possession of a key to the property. O'Farrel J's finding should be read as relating to her dismissing that the mere act of loaning a key does not create an expectation for reliance.

This is supported by O'Farrel J's reference to the case of *Essex,*[90] where it was held that the police force had created a danger of theft by arresting the driver of a truck and leaving the truck parked in a lay-by, where it was subsequently robbed.[91] There was no prior relationship between the police and thieves (nor the driver and the thieves) but it was held that the Police had a special level of control over the source of the danger, as they had the knowledge that there were criminals operating in that specific area who targeted vehicles, and the officers chose to leave the vehicle in question parked in that (reasonably foreseeably) dangerous area. Accordingly, where the Smart Device Manufacturer can be seen as having created the danger by allowing a cyberattacker to access a device by failing to update the Smart Device against known vulnerabilities, they will not be able to rely on the omissions principle to avoid a duty of care being established. It must be noted, however, that many of the above cited cases refer to public authorities. Can it be considered the case, therefore, that public authorities have a greater duty than private bodies when it comes to determining liability in the presence of an omission? It is hard to see how this is correct. The cases in question focus solely on the level of control which the defendant exerts over the contested

86 ibid.
87 *Robinson v Chief Constable of West Yorkshire Police* (n 77) para 34.
88 *Rushbond PLC v The JS Design Partnership LLP* (n 83) para 41.
89 In Rushbond, the 'special level of control' is discussed only over two paragraphs, compared to a much greater level of discussion relating to assumption of responsibility (ibid, paras 28-40).
90 *The Chief Constable of Essex Police v Transport Arendonk BVBA* (n 84).
91 *Rushbond PLC v The JS Design Partnership LLP* (n 109) para 42.

situation, there is no distinction made between private and public defendants,[92] and in *Rushbond,* it is clear how findings made against public bodies are applicable in determining the liability of a private body. Furthermore, it can be considered a normal state of affairs that such cases would draw heavily from public bodies, given the higher level of control which public bodies such as the police forces, health agencies and social services exert over their 'clients' when compared to a private body.

It is of particular interest to note that the omissions problem is one which has received more attention and more deliberation in the Irish courts than in the UK. The Irish position can be seen as instructive for the purposes of evaluating the determinants of 'a special level of control'.

University College Cork – National University of Ireland v. The Electricity Supply Board is the leading Irish case with regards to omissions.[93] The case draws on *Robinson,*[94] and the classification provided by Tofaris and Steele is cited affirmatively by Clark CJ,[95] and the 'special level of control' exception to the do no harm principle is recognised as being good law in Ireland.[96] The case was taken by University College Cork (UCC), a University which is situated in a floodplain (as is the city of Cork) downstream of two dams which are operated by the Electricity Support Board (the ESB), the body in Ireland responsible for the generation and distribution of electrical power. During November 2009, following a period of prolonged and heavy rain, the ESB released a volume of water which resulted in widespread flooding and associated property damage in Cork. The ESB were required to release the water in order to prevent damage, and ultimately catastrophic structural failure to the dams. However, UCC argued that in the days preceding the spill, the ESB was negligent in not lowering the water level to allow for an increased holding capacity, which would have reduced the amount of water spilled from the dam. Thus, the case became a test of the general principle of omissions, as it was alleged by UCC that the ESB's failure to act (lowering the water level) in good time resulted in exacerbated damages caused by the flooding. It is important to note that at no time was the cause of the flooding attributed to a wrongful action by the ESB.

It was alleged by UCC that the ESB had a duty of care to, *inter alia*, UCC, and this duty of care arose in the context of an omission. While UCC relied on three of the four points identified by Tofaris and Steele to ground their claim, and these are examined in great detail by Clarke CJ, of particular relevance to this paper is point iii, where a party has 'a special level of control over the source the danger'. Clarke CJ notes how this special level of control does not need to stem from a pre-existing legal arrangement,[97] and the appropriate test is outlined to determine:

> *(a) Whether there is a reasonable relationship between any burden which would arise from imposing such a duty of care and the potential benefits to those who may be saved from the danger in question; and*
> *(b) Whether it is possible to define the duty of care in question with a sufficient, but not absolute, level of precision so as to avoid imposing a burden which is impermissibly vague and imprecise.*[98]

92 In *Stovin v Wise* [1996] AC 923 (HL), it is confirmed that public authorities are not treated differently from private bodies with regards to imposing a positive duty to act. This *dicta* was affirmed in *Mitchell* (n 67).
93 *University of Cork - National University of Ireland v The Electricity Supply Board* [2020] IESC 66.
94 *Robinson v Chief Constable of West Yorkshire Police* (n 60).
95 *University of Cork - National University of Ireland v. The Electricity Supply Board* (n 93) para 7.8.
96 ibid 11.9.
97 ibid 12.4.
98 ibid 11.18.

This test is applied to the question of whether a Smart Device Manufacturer could be held responsible for a failure to keep a Smart Device safe, as outlined in the Proposed Requirements. [99]

In relation to the first question, whether there is a reasonable relationship between the burden associated with the Proposed Requirements and the potential benefits to third parties? This should be a simple hurdle to clear; the Smart Device Manufacturer is responsible, through the decisions which are made during the software development process, as to whether the Smart Device will adhere to the Proposed Requirements or not, and whether cyberattackers will find it effectively trivial to access the Smart Device through a known vulnerability. It can only be considered reasonable that the entity responsible for the security of the Smart Device can be found to have a duty of care to both the owners of the Smart Device and to the entities who suffer harm from the Smart Device Manufacturer's failure to maintain the Proposed Requirements. Furthermore, one of the key arguments against imposing an affirmative duty on parties is that omissions do not generally generate risks,[100] but rather are a failure to respond to risks generated by other parties. However, the omission by a Smart Device Manufacturer is the very (in)action that creates the risk of the use of a Smart Device in a cyberattack against a third-party.

With regards to the second question, the Proposed Requirements have been drafted by the UK Government and the EU Commission respectively, so as to ensure that the Smart Device Manufacturer is not held to an absolute level of security, but instead has a clear and well-defined set of requirements which will prevent the Smart Device from being exploited by known vulnerabilities and will ensure that the Smart Device is removed from the network once it has reached the stage where it is no longer supported by the Smart Device Manufacturer. Accordingly, it is clear how within both the UK and the Irish legal systems there is precedent for a duty of care to be established, subject to the Proposed Requirements, for Smart Device Manufacturers.

Despite these arguments, is it clear that a UK court would recognise an in-scope claim as an example of an omissions case? Morgan provides an excellent (and up-to-date) summary of the hurdles that must be made in an omissions claim in order to distinguish it from an ordinary 'acts' case.[101] He notes how it was held by Stuart-Smith LJ that a mere intervention is not sufficient to overcome the acts distinction, but that the party in question must cause harm or create the danger.[102] Such a finding is tempered, however, as although a third party may have the power to prevent harm, they are not automatically burdened with a duty to do so.[103] Yet, in the context of in-scope cyberattacks, the Smart Device Manufacturer has effectively total control over the cybersecurity of the Smart Device, unless they have taken a positive action to not enable the provision of security updates which will create a Smart Device where no party has control over it, or the owner of the Smart Device has altered the code within the Smart Device which would remove any liability from the Smart Device Manufacturer. Accordingly, it should be clear how Clarke CJ's test can be satisfied.

Is there a just and reasonable basis to impose a duty of care?

99 It should be noted that the Court examined the issue of whether there was a difference between public bodies and private agents with regards to establishing a duty of care, and concurred with the trial judge that there was not. (ibid [9], [10]).

100 Eoin Quill, 'Affirmative Duties in the Common Law' (2011) 2 Journal of European Tort Law 151, 174.

101 Jonathan Morgan, 'MAINTAINING THE ELEGANT FAÇADE OF THE ACTS–OMISSIONS DISTINCTION' (2022) 81 The Cambridge Law Journal 245.

102 *Tindall and another v Chief Constable of Thames Valley Police and another* (n 110).

103 ibid 72.

The final hurdle which a claimant will have to clear, in order to establish a duty of care under the *Caparo* principles is that there is a just and reasonable basis to impose a duty of care. For the majority of envisaged in-scope potential claimants, this may prove to be the hardest hurdle to clear.

The first task that the claimant must achieve is to demonstrate how the damages sought are recoverable, given how "*It is never sufficient to ask simply whether A owes B a duty of care. It is always necessary to determine the scope of the duty by reference to the kind of damage from which A must take care to save B harmless".*[104]

As discussed earlier in this paper, there are two primary limbs through which an in-scope cyberattack can take place; the first being an in-scope cyber-physical attack, and the second being an availability attack. A cyber-physical attack would, by its nature, result in damage to the third-party's property and so it is common cause that the third party can seek damages to compensate them for harm accruing to their property.[105] Accordingly, when evaluating an in-scope claim which lies on the cyber-physical limb, there just remains the question of whether such a claim is compatible with public policy, a question which is discussed later in this article.

The second limb, an in-scope claim arising following an availability attack will be much harder to ground, as there would be appear to no property damage suffered by the third-party, which would make any claim one for pure economic loss and so effectively unrecoverable under common law, unless one of the recognised exceptions to this principle can be established.[106] It must be noted, however, that such a claim should not fall under the exclusionary rule associated with Relational Economic Loss,[107] due to the fact that the claimant is claiming directly against the Smart Device Manufacturer due to their alleged negligence which enabled a cyber-attack to take place and which resulted in harm directly accruing to the claimant, as opposed to harm accruing to a third-party which results in economic loss arising for the claimant due to some pre-existing relationship between the claimant and the third party.

When evaluating the damage that a third party suffers during, and as a result of, an availability attack, it is clear how there are two principal categories. The first category can be seen as 'immediate' damages, these are the costs incurred by the execution of the availability attack such as the bandwidth fees incurred by the attack, service fees paid to a security vendor during the attack to restore availability, and the provisioning of new resources to increase the capacity of the network to respond and fulfil genuine connection requests. These fees are estimated to be between $120,000 and $218,000 per attack on small to medium sized businesses.[108]

The second category of damages is 'subsequent' damage which arise from the 'lost profits' which the business could have expected to claim during the time of the attack and the reduced functionality arising in the immediate aftermath of the attack. Estimates for small to medium sized

104 *South Australia Asset Management Corporation v York Montague Ltd* [2010] UKHL 10 [627].

105 See, e.g., *SCM (UK) Ltd v WJ Whittall & Son Ltd* [1971] QB 337; *Spartan Steel & Alloys Limited v Martin & Co (Contractors) Ltd* [1973] QB 27.

106 *Armstead v Royal and Sun Alliance Insurance Co Ltd* [2021] Walsall County Court [31].

107 See, e.g., Russell Brown, 'Justifying the Impossibility of Recoverable Relational Economic Loss' (2005) 5(2) Oxford University Commonwealth Law Journal.

108 'How Much Will a DDoS Attack Cost Your Small Business?' (*TechInsurance*) <https://www.techinsurance.com/resources/ddos-small-business-costs> accessed 23 October 2022; Sean Newman, 'The True Cost of DDoS Attacks' [2021] *Infosecurity Magazine* <https://www.infosecurity-magazine.com/opinions/the-true-cost-of-ddos-attacks/> accessed 23 October 2022.

businesses are from $7,000 to $84,000 per attack hour.[109] These subsequent losses are a text-book definition of 'pure economic loss' and as such, it is not argued that these are recoverable.

Is it reasonable to assume that a party bringing an in-scope negligence claim on the basis of having suffered an availability attack has the ability to succeed in grounding their claim for direct damages? From *The Orjula*,[110] it is clear how the definition of damage can go beyond actual damage. In this case, the deck of a ship was contaminated with acid requiring decontamination. The deck itself was not actually harmed, but it was held that the cost of the decontamination was recoverable. There are clear and obvious analogies between this and an availability attack where the digital resources affected must be 'decontaminated' from the consequences of the availability attack in order to be rendered usable again. Furthermore, judgements starting from *Hedley Byrne,*[111] and continuing with those such as *Network Rail v Conarken,*[112] *Nykredit v Erdman*[113], *Network Rail v Handy,*[114] and *Arrowhead v Dragon,*[115] where the courts have taken the approach of evaluating whether a loss incurred can be considered as both foreseeable and sufficiently proximate to the defendant so as to be recoverable, even when the loss is economic in nature and no actual damage has occurred, would suggest that an in-scope claim for damages could succeed and is not ruled out-of-bounds due to the economic nature of the damages sought. The case of *Glencar* confirms that the Irish courts also follow this principle.[116]

A complete evaluation of the nature of 'damages' and their application to availability attacks is beyond the scope of this paper, which was written with the intention of examining whether the omission of a Smart Device Manufacturer in deploying a security update for a known vulnerability could be potentially recoverable via a negligence claim brought by a third-party. However, from the above it should be clear that while substantial hurdles remain, it is not appropriate to posit that all such negligence claims must fail due to the nature of the damages sought. The above cited cases demonstrate how there is potential (albeit limited) for recovery of at least the direct damages incurred during an availability attack. A potential claimant, therefore, in establishing that their claim for damages is recoverable, is left with the challenge of threading the eye of a particularly small needle as opposed to being required to encourage a camel to successfully transit through the eye of said needle.

Having demonstrated, to at least a tentative level, how there is potential for direct damages suffered during an availability to be recoverable, the second task which a claimant must complete is to demonstrate that there are no public policy reasons so as to deny the imposition of a duty of care on the Smart Device Manufacturer. This would appear to be possible to achieve for three reasons. The first is the specific nature of an in-scope claim which limits potential claimants to a well-defined and small set, combined with the well-defined proposed requirements should remedy any judicial fears of 'opening the floodgates' in terms of future cybersecurity claims.[117] It must also be noted how it is, *actual public policy* that Smart Device Manufacturers keep their Smart Devices updated.[118] Finally, the Smart Device Manufacturer, as argued in the foreseeability section of this paper, is the

109 'How Much Will a DDoS Attack Cost Your Small Business?' (n 108).
110 *The Orjula* [1995] CLC 1325.
111 *Hedley Byrne & Co Ltd v Heller & Partners Ltd* [1964] AC 465.
112 *Network Rail Infrastructure Ltd v Conarken Group Ltd* [2010] EWHC 1852 (TCC) [63].
113 *Nykredit Mortgage Bank Plc v Edward Erdman Group Ltd* [1997] 1 WLR 1627.
114 *Network Rail Infrastructure Ltd v Simon Handy* [2015] EWHC 1175 (TCC).
115 *Arrowhead Capital Finance Ltd (In Liquidation) v KPMG LLP* [2021] EWHC 1801 (Comm) [76].
116 *Glencar Exploration p.l.c. v Mayo County Council (No. 2)* (n 48).
117 *Spartan Steel & Alloys Limited v Martin & Co (Contractors) Ltd* (n 105).
118 See (n 28)

only party capable of managing the security of their Smart Devices, and the damages for which they could be required to pay would be expected to be covered by their own insurance policies.

Accordingly, it is proposed that recent decisions in the UK and Irish courts would allow a third-party to, at the very least, argue that a duty of care is owed to a third-party victim of a cyberattack by the Smart Device Manufacturer, that was facilitated by a Smart Device being compromised by the cyberattacker. However, the establishment of a duty of care is a necessary but not sufficient condition to meet the criteria of a successful negligence claim. The claimant, having established that they are owed a duty of care by the Smart Device Manufacturer,[119] will still need to satisfy the general requirements of negligence,[120] of having established a duty of care, that the harm was foreseeable, the defendant's conduct was both the factual and legal cause of the harm, and the defendant's conduct fell below the standard of care which was due to the claimant.

With regard these requirements, the claimant will be supported by the fact that to establish a duty of care under the *Capero* test, they will have already demonstrated sufficient factual and legal causation between the defendant and the foreseeable harm arising from the cyberattack. This is not to say that the defendant will not be able to rebut these assertions and demonstrate how the facts of a particular claim fall outside of the scope of the duty of care or how there are other, independent factors in the specific attack which break the chain of causation. It is also probable that were such a claim to make it to court, the defendant would assert that the behaviour of the claimant, such as their own cybersecurity infrastructure or IT set up, had a material role in the outcome of the cyberattack, thus introducing contributory negligence as a mitigating factor. However, such defensive actions would be the result of a claimant successfully bringing a negligence claim to court, and as such, they do not preclude the action, the bringing of which is the fundamental question which is asked in this paper.

The primary challenge for the claimant in bringing a claim for negligence, which was not addressed in the establishment of a duty of care, is to establish that the behaviour of the defendant breached the standard of care that was due to them. To do so, the claimant will need to demonstrate how the conduct of the defendant fell below what the relevant policy makers expect of the Smart Device Manufacturer, when it comes to maintaining the security of their Smart Devices. Such expectations can be sourced both in legislation (in the case of the EU, forthcoming) as well as guidelines posted by either policy makers or relevant regulators. The claimant could also use the statements made by the Smart Device Manufacturer if it can be demonstrated that the Smart Devices are not maintained to the standards and levels which the Smart Device Manufacturer has claimed that they were, an approach often taken by the Information Commissioner's Office when determining if a company's cybersecurity posture matches the standard to which it is held.[121] As with regard to the other requirements for negligence, the defendant can rebut the assertion that the standard of care was breached, but such an action does not preclude that an objective standard of care can be determined as part of a claim of negligence.

Accordingly, it should be clear that if a court were to accept that a claimant, who has suffered harm due to a Smart Device Manufacturer's alleged negligence with regards to their maintenance of the cybersecurity of their Smart Device, represents a novel categorisation of a duty of care, then there is scope for such a claim to be heard and for the duty of care to be established. It would remain a

119 It would be remiss not to note that the judgements of both *ESB* and *Rushbond* could be distinguished from the future development of omissions principles which would make establishing such a claim extremely difficult.

120 See, e.g., *Smith v Littlewoods (n 88)*

121 See, e.g., ICO v British Airways [2020] Penalty Notice, COM0783542

very difficult challenge for the claimant to succeed in their case, but there do not appear to be any specific legal arguments which would make the negligence claim itself impossible, which is a new state of UK and Irish law.

Conclusion

This paper has demonstrated how, given a very limited and narrow set of circumstances, third-party victims of a cyberattack may be successful in bringing a claim of negligence against the Smart Device Manufacturer who enabled it, and may be able to seek recovery of at least the costs that arose because of the cyberattack. This finding, if applied successfully in a UK or Irish court, will not only be a positive event for the third-party victims of in-scope cyberattacks, but is also likely have a positive impact on the cybersecurity of Smart Devices which are sold into these markets. This is because remediating vulnerabilities in Smart Devices is currently an extra cost for Smart Device Manufacturers, and one for which there is little incentive for them to bear. Furthermore, currently in both Ireland and in the UK, there are little to no consequences for Smart Device Manufacturers who don't maintain a reasonable level of cybersecurity in their products, and there are no legal mechanisms for recovery available if the victims are third-parties, as opposed to users. This is despite the fact that third-parties are more likely to by the victims of in-scope cyberattacks when compared to the users of Smart Devices. This lacuna has enabled Smart Device Manufacturers to continue to ignore their responsibility to ensure that their Smart Devices are reasonably secure, and to prevent them from being used in cyberattacks. A successful application of the approach outlined in this paper would see this lacuna closed, and the cybersecurity of Smart Devices improved.

Since the advent of Lord Atkin's neighbour principle in *Donoghue v Stevenson*,[122] negligence has been used as a means for people who suffer reasonably foreseeable harm at the hands of others to seek recompense from those who caused the harm. This has also led to the encouraging of manufacturers to improve their processes and practices to reduce instances of harm. It is fitting therefore, that over 90 years after this seminal case was decided, the principles of negligence can still be used to correct (in)actions that have resulted in harm occurring in novel situations, even when involving technology that would have been unfathomable to the judges who developed this strand of legal theory. The arguments in this paper outline a way in which a legal principle which is almost a century old remains not just relevant, but also sufficiently robust to respond to the exigencies of an ever-evolving digital era.

122 Donoghue v Stevenson [1932] AC 562