Software Update Requirements - Striking a Balance between Providers and Users

Benjamin Lim

University of Edinburgh

s2599925@ed.ac.uk

April 10, 2025

1. Introduction

The WannaCry ransomware infection was one of the most prolific cyber attacks, affecting over 200,000 computers in more than 100 countries [1], even resulting in ambulances having to divert as some Emergency Departments were affected and unable to receive patients [2]. A post-mortem found that some affected computers were running the Windows XP operating system which was no longer supported at that time [3]. Due to the unprecedented scale of the attack, Microsoft made the "highly unusual" step of releasing a security update for an unsupported system [4]. This incident sheds light on the challenge of striking the right balance between holding providers responsible for providing software updates while making sure that providers are not trapped into a commercially infeasible lifelong commitment.

In this essay, I will be exploring how the Product Liability Directive (PLD) [5] plays a main role regulating software updates for the benefit of consumers and the various exclusions that shift the balance, ensuring software providers are not overly disadvantaged. I will then look at how the Cyber Resilience Act (CRA) [6], the Digital Content Directive (DCD) [7], and finally the General Product Safety Regulation (GPSR) [8], complement the PLD by introducing additional requirements for security updates and by encouraging proactive identification of bugs so that software updates are not required.

2. Product Liability Directive

The newly passed PLD explicitly states that artificial intelligence (AI) as well as software "is a

1 National Audit Office, *Investigation: WannaCry cyber attack and the NHS* (2018) <https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf>, pp. 4

2 National Audit Office (n 1), pp. 8

3 National Audit Office (n 1), pp. 18

4 Microsoft Security Response Center, 'Customer Guidance for WannaCrypt attacks' (13 May 2017) <https://msrc.microsoft.com/blog/2017/05/customer-guidance-for-wannacrypt-attacks/> accessed 4 March 2025

5 Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC [2024] OJ L series/1

6 Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) [2024] OJ L series/1

7 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services) [2019] OJ L136/1

8 Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC [2023] OJ L135/1

product" and falls under its ambit of the PLD regardless of whether it is provided to the consumer to run on their own computers or if it is provided over the Internet as a service [9]. The previous iteration of the PLD defined a product as a "movable" [10], which would exclude intangibles like software, let alone software provided as a service (SaaS). This is supported by Krone, in which the court ruled that under the previous PLD, health advice "by its nature, constitutes a service" and not a product [11]. Hence, this single change requires Software Providers to comply with all further requirements under the PLD. The overarching requirements are that the provider is liable for compensation for any death, injury or damage to property or data caused by defects in the product [12]. The general motivation is based on age-old tort law where the claimant is "[compensated] for losses caused by the tortfeasor's actions" [13].

However, there are a few clauses which warrant a closer look. Article 8(1) states that liability extends to defective components integrated with a product under manufacturer control while Article 8(2) states that any person that "substantially modifies a product" shall be considered the manufacturer and hence liable for defects [14]. This is relatively interesting in the software context. Most successful software allow the community to contribute add-ons or plug-ins to enhance the software. Browsers have extensions which provide enhanced functionality [15] while mobile operating systems (OS) have apps which provide new capabilities [16]. For successful software like Microsoft Windows, there are even third party companies such as Acros Security which release updates to versions of Windows which are no longer supported by Microsoft [17] or fixes for bugs which Microsoft deems unworthy of patching [18]. Given that defects may be present in these modifications themselves, or in the interface between the modification and the main application, it will be interesting to observe the future court's interpretation of the term "substantial modification". In Delta vs CrowdStrike, Crowdstrike's "faulty security updates" caused 8.5 million Windows computers installed with its software to crash, disrupting *inter alia* airlines, emergency services, banks [19]. Given that Crowdstrike ended up as a party in this US case instead of Microsoft, it appears to be in agreement with Article 8(1)(b) of the EU PLD, as Crowdstrike is the "defective component" that was "integrated into" the Win-

9 Dir 2024/2853 (n 5), para. 13

10 Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products [1985] OJ L210/29, art. 2

11 Case C-65/20 *KRONE – Verlag Gesellschaft mbH & Co KG* ECLI:EU:C:2021:471, para. 32

12 Dir 2024/2853 (n 5), art. 6 and 8

13 Carol Brennan, *Tort Law* (8th, 2022), sect. 1.3

14 Dir 2024/2853 (n 5), art. 8(1) and 8(2)

15 Google, 'Welcome to the Chrome Web Store' (6 March 2025) <https://chromewebstore.google.com/?pli=1> accessed 6 March 2025

16 Apple, 'The apps you love. From a place you can trust.' (6 March 2025) <https://www.apple.com/sg/app-store/> accessed 6 March 2025

17 Thomas Joos, 'Want to safely use Windows 10 after Microsoft ends support? Meet 0Patch' (13 September 2024) <https://www.pcworld.com/article/2456251/windows-10-will-no-longer-receive-updates-from-october-2025-change-that-with-this-tool.html> accessed 6 March 2025

18 Mitja Kolsek, 'The "EventLogCrasher" 0day For Remotely Disabling Windows Event Log, And a Free Micropatch For It' (31 January 2024) <https://blog.0patch.com/2024/01/the-eventlogcrasher-0day-for-remotely.html> accessed 6 March 2025

19 *Delta Air Lines, Inc v CrowdStrike, Inc Complaint* 24CV013621 (2024), pp. 1

20 Dir 2024/2853 (n 5), art. 8(1)(b)

dows operating system [20], hence liability lay with Crowdstrike.

3. Product Liability Directive - Reasonably Foreseeable Use and Effect

Article 7(2) enumerates the conditions under which a product is deemed defective. The conditions are *prima facie* rather subjective and open to interpretation from the court [21]. However, when read together with the rest of the Directive, one can make better deductions into the intent and likely interpretation. For example, Article 7(2)(b) states that "reasonably foreseeable use" of the product should be accounted for when determining defectiveness while Article 6(1)(b)(iii) and 6(1)(c) excludes damages from professional use. Hence, we can determine that the court will likely assess the defectiveness based on domestic use. In 1993, Intel released a CPU with a very rare microcode bug that only occurred in about 1 in 9 billion calculations with the worse case effect that a division will be inaccurate in the 4th significant digit [22]. The bug was discovered by a number theory professor and was estimated to negatively impact only a few users "in the scientific/engineering and financial engineering fields" [23]. It is also pertinent to point out that the affected processors were marketed for personal computers and even found its way into consumer electronics [24], hence its "reasonably foreseeable use" would likely not include calculations requiring a huge degree of accuracy. Thus under Article 7(2)(b) of the PLD, such a bug will most likely not be considered a defect since it is almost statistically impossible to negatively impact domestic use.

Article 7(2)(d) states that the "reasonably foreseeable effect" on other interconnected products must be taken into account in evaluating defectiveness. This clause is especially relevant to software as many products today are dependent on SaaS running in the cloud. Google discontinued the Nest Secure cloud service, turning the $400 devices that customers previously bought into paperweights [25]. Under Article 7(2)(d) of the PLD, consumers will have recourse even though the defect did not lie in the product they purchased but in the interconnected cloud service which the product requires to continue functioning. While this may *prima facie* seem to impose unreasonable requirement on providers to keep the lights on and provide lifetime support for all products, the PLD does specify 10 years as a "reasonable length of time" for providers to remain liable [26]. Therefore a balance is struck ensuring that consumers are able to enjoy utility of a defect free product for a reasonable time while not placing unreasonable demands on providers. This clause also introduces certainty and allows consumers to purchase with confidence knowing that the product will receive updates for a minimum period of time. Once again, it will be of interest to scrutinize the earlier Delta vs CrowdStrike case under Article 7(2)(d). Could CrowdStrike have reasonably foreseen that it's software defect could have caused flights to be canceled and emergency de-

21 Dir 2024/2853 (n 5), art. 7(2)

22 Ken Shirriff, 'Intel's $475 million error: the silicon behind the Pentium division bug' (1 December 2024) <https://www.righto.com/2024/12/this-die-photo-of-pentium-shows.html> accessed 8 March 2025

23 Shirriff (n 22)

24 Cratecode LLC, 'Exploring the History and Impact of Intel Pentium Processors' <https://cratecode.com/info/pentium-processors> accessed 9 March 2025

25 Tyler Lacoma, 'Google's Nest Secure Has Fully Shut Down: We've Got Answers if You're Worried' (24 April 2024) <https://www.cnet.com/home/security/googles-nest-secure-has-fully-shut-down-weve-got-answers-if-youre-worried/> accessed 8 March 2025

26 Dir 2024/2853 (n 5), para. 57

27 Alex Scroxton, 'CrowdStrike update chaos explained: What you need to know' (29 July 2024) <https://www.computerweekly.com/feature/CrowdStrike-update-chaos-explained-What-you-need-to-know> accessed 9 March 2025

partments to turn away patients [27]? It seems plausible that Crowdstrike would be deployed on systems running such scheduling and booking functions and Crowdstrike would be held liable, barring Article 6(1) which excludes professional use. Of note, Crowdstrike was not deployed on the planes itself or on critical equipment keeping patients alive, which could be argued to be a much less reasonably foreseeable effect since there are stricter regulations governing usage of software in safety-critical systems [28] [29] which Crowdstrike may not be certified under.

Finally, paragraph 30 of the PLD describes that when assessing defects, the court is to consider the safety of the "public at large" as opposed to the safety that a particular person expects to receive. This position seems to have its roots in liability of public bodies. In Hill v Chief Constable of West Yorkshire, the court remarked that the police force is motivated by a "general sense of public duty" [30] and it is against public interest to hold the police liable for a murder caused by the police not apprehending a criminal timeously. Perhaps, there are parallels shared with consumer welfare, where the legislation aims to improve the welfare of consumers in general, and discourage unreasonable demands from singular customers which may overstrain the provider's resources. The Intel CPU bug discussed earlier generated huge public outcry, forcing Intel to offer to recall all affected processors, resulting in "huge expense for minimal gain" and is detrimental to "society as a whole" [31]. In total, the product recall cost $475 million and the only people who marginally benefited were a handful of scientific or engineering users [32]. Consumers in general likely ended up footing the bill as companies had to subject future products to more rigorous testing to prevent another occurrence of a 1 in 9 billion bug, resulting in higher product cost and delayed launches of subsequent products.

4. Product Liability Directive - Exemptions and Exclusion

Article 11 of the PLD generally aims to ensure that the party that caused or has the means to rectify the defect, be it the manufacturer, importer or person making substantial modifications, is held liable for the defect [33]. Among the clauses, article 11(1)(d) which indemnify liability should the defect be due to "compliance of product with legal requirements" deserves closer inspection. It seems unfathomable that the government would legally require the provider to include a defect in a product, much to the chagrin of consumers. The US government had at some point in history, required the Clipper Chip to be added to all telecommunications device, which introduced a "defect" which allowed the government to eavesdrop on conversations for "national security" purposes [34]. However, this is in contravention of the right for private communication espoused in Article 7 of the Charter of Fundamental Rights of the European Union [35]. In Podchasov v Russia, the court also reaffirmed the stance that weakening encryption is

28 International Standards Organization, 'IEC 62304:2006 Medical device software — Software life cycle processes' (1 January 2006) <https://www.iso.org/standard/38421.html> accessed 9 March 2025

29 RTCA, Inc, 'Software Considerations in Airborne Systems and Equipment Certification' (1 December 1992) <https://antena.fe.uni-lj.si/literatura/Razno/Avionika/rtca/Rtca%20Do-178B.pdf> accessed 9 March 2025

30 *Hill v Chief Constable of West Yorkshire* [1989] AC 53, pp. 63

31 Shirriff (n 22)

32 Shirriff (n 22)

33 Dir 2024/2853 (n 5), art. 11

34 Electronic Privacy Information Center, 'The Clipper Chip' <https://archive.epic.org/crypto/clipper/> accessed 9 March 2025

35 Charter of Fundamental Rights of the European Union [2000] OJ C364/1, art. 7

"not proportionate to the legitimate aims pursued" and alternative solutions should be explored in criminal investigations [36]. Hence, it is most certainly not the intention of legislators. One theory could be that such legislation paves the way for governments to introduce defects in the interest of public safety. Using a handheld telephone while driving in illegal in most EU countries [37]. Thus, such a legislation may allow software providers to introduce "defects" such as locking the screen of the driver's phone while the car is in motion in the interest of road safety. This clause shifts the balance of power away from users, not into software providers, but into the hands of the government. Nonetheless, it is important to point out recent developments in the EU. The French and the Swedish government are seeking to pass laws which will mandate backdoors in encrypted messaging applications for law enforcement purposes [38] [39]. The British government has also, through the Investigatory Powers Act [40], allegedly influenced Apple to remove its end-to-end encryption feature for British iCloud users [41]. It would be interesting to observe whether the removal of end-to-end encryption could be considered a "product defect" and subsequently whether courts would exempt software providers from liability under article 11(1)(d).

Under article 2(2) of the PLD, free and open-source software is also excluded from liability. The clause is similar in intention to a Good Samaritan Law, or the Social Action, Responsibility and Heroism act in the UK [42]. Under the Act, if the defendant was "acting for the benefit of society" and "demonstrated a generally responsible approach" in considering the safety of the claimant, he could be absolved of negligence or breach of responsibility claims [43]. Similarly, since development of free and open-source software is for the good of the general public [44], it can be argued that such a clause will encourage more to step forward to contribute without fear of legal liability resulting from their actions. However, keen observers will note that article 2(2) does not address the issue of providers acting in a "generally responsible" manner. Developers with nefarious intent have previously succeeded in sneaking in malicious code into popular open source software, planting a bug in a data compression utility that would allow someone with knowledge of the bug to later gain unauthorized access to a system with that util-

36 *Case of Podchasov v Russia* [2024] ECHR 33696/19, para. 78

37 Jeanne Breen Consulting, *Car telephone use and road safety - An overview prepared for the European Commission* (2009) <https://road-safety.transport.ec.europa.eu/document/download/15950308-73f3-4632-a2f6-25fbd1937a5a_en?filename=car_telephone_use_and_road_safety.pdf>, pp. 10

38 La Quadrature du Net, 'All-out mobilization against the French "war-on-drugs" law' <https://www.laquadrature.net/en/warondrugslaw/> accessed 5 April 2025

39 Suzanne Smalley, 'Swedish authorities seek backdoor to encrypted messaging apps' (25 February 2025) <https://therecord.media/sweden-seeks-backdoor-access-to-messaging-apps> accessed 5 April 2025

40 Investigatory Powers Act 2016

41 Alexander Martin, 'Apple turns off iCloud encryption feature in UK following reported government legal order' (21 February 2025) <https://therecord.media/apple-encryption-feature-off-britain> accessed 5 April 2025

42 Government of the United Kingdom, *Fact Sheet - Social Action, Responsibility and Heroism Bill* (2015) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/318839/sarah-bill-fact-sheet.pdf>

43 Government of the United Kingdom (n 42), pp. 2

44 Liane Colonna, 'The end of open source? Regulating open source under the cyber resilience act and the new product liability directive' (2025) 56 Computer Law & Security Review 106105 <https://www.sciencedirect.com/science/article/pii/S0267364924001705>, sect. 2.2

ity installed [45]. Such software updates will not attract liability under the PLD due to the article 2(2) carve-out. Interestingly, such actions may not be illegal under the Computer Misuse Act as well since there is no unauthorized access at the point of contributing the malicious code [46]. Thus, this may create an confounding situation where it is legal to plant traps as long as you don't check the traps later.

Under article 11(1)(c) of the PLD, it is stated that providers are exempt from liability if the "defectiveness that caused the damage did not exist at the time the product was placed on the market" [47]. The motivation of this clause is probably to exclude product liability due to wear and tear from normal everyday use. However, it may have interesting implications on software updates because of the way software is distributed. Most software have similar basic functionality such as a menu bar with various options such as saving to a file and exiting that is implemented by reusing code in a shared library. This shared library can be statically linked, where it is packaged and comes together with the core program, or it could be dynamically linked, where the core program uses a copy that is already on the operating system, that is shared with other programs [48]. The latter case provides a possible scenario where a different software on the operating system could update the shared library with a more recent version that causes a defect in the product in question. This was a rather common issue in earlier versions of Windows, and aptly given the name "DLL (dynamically linked library) Hell" [49]. Under article 11(1)(c) of the PLD, the software provider will not be liable because the defect did not exist when the program was installed, but was introduced by another program that updated a shared library. Under article 7(2)(d) of the PLD, the provider of the other software would also not have reasonably foreseen that updating a shared library could possibly result in a defect in another software. Hence, it creates a *lacuna* where the consumer bears the blame for using software that is "incompatible" with each other. Li and Faure have commented that in such complex scenarios, it can be tricky for courts to correctly determine a "due care level" which may result in a *lacuna* or perceived unfair situation [50].

Finally, paragraph 51 of the PLD excludes liability from software providers if the damage arises from lack of updates which is "beyond the manufacturer's control", such as when the consumer fails to install the updates [51]. Logically, if the consumer's own inaction caused the damage, then it would be natural for the consumer to bear the costs. In the WannaCry incident covered prior, many affected consumers were still using Windows XP which had already reached its end of life [52], they bore the brunt of the damage, which is consistent with the stance taken by the PLD. However, there is still considerable ambiguity as to what constitutes the manufacturer's control. Since the commoditization of the Internet, many software providers have built-in functionality to check for, download, and install updates automatically. How-

45 Sergiu Gatlan, 'Red Hat warns of backdoor in XZ tools used by most Linux distros' (29 March 2024) <https://www.bleepingcomputer.com/news/security/red-hat-warns-of-backdoor-in-xz-tools-used-by-most-linux-distros/> accessed 9 March 2025

46 Computer Misuse Act 1990

47 Dir 2024/2853 (n 5), art. 11(1)(c)

48 European Commission, 'GNU Lesser General Public License (LGPL) 2.1' <https://interoperable-europe.ec.europa.eu/licence/gnu-lesser-general-public-license-lgpl-21> accessed 14 March 2025

49 Nikhil Bhargav, 'DLL Hell Problem' (18 March 2024) <https://www.baeldung.com/cs/dll-hell-problem> accessed 14 March 2025

50 Shu Li and Miachael Faure, 'The Revised Product Liability Directive: A Law and Economics Analysis.' (2024) 15(2) Journal of European Tort Law 140, pp. 146

51 Dir 2024/2853 (n 5), para. 51

52 Microsoft Security Response Center (n 4)

ever, automatic updates bring added risk as we have observed with Crowdstrike [53]. Had they used a manual deployment method, the botched update would not have reached so many devices in such a short period of time. Now, we have also concluded that automatic updates may bring the device under the manufacturer's control which increases the period where a the provider is liable for the product. Will such a clause in the PLD discourage software providers from providing automatic updates to the detriment of consumers? The CRA, which we will discuss in the next paragraph, will provide more clarity on this issue.

5. Cyber Resilience Act and the Digital Content Directive

The CRA differs from the PLD in that it aims to establish a cybersecurity baseline for products [54], and does not impose any requirements on functional defects such as the previously mentioned Intel CPU calculation bug [55]. The DCD's main aim is to ensure "conformity with the contract", with greater focus on ensuring that consumers continue to retain "access" to digital goods after their purchase [56]. Thus it has a similarly narrow relevance on the issue of software updates. Due to the similarities in the relevance of both legislation, I will be simultaneously exploring how both legislations impact the balance of responsibilities between software providers and users with respect to software updates.

Under paragraph 56 of the CRA, providers have to enable the "installation of security updates automatically", especially for consumer products as timely updates will protect devices from newly disclosed vulnerabilities [57]. Thus, this clause appears to address the issue where the PLD may discourage software providers from automatic updates so as to reduce their liability. As explained earlier, the CRA only pertains to security updates and not feature updates. There may be scenarios where a lack of feature updates result in damages. For example, personal tax filing software may need to be updated annually to ensure that the documents produced are compliant with the most recent tax code. Nonetheless, such scenarios where damages arise from lack of automatic feature updates are few and far between.

Under article 13(11) of the CRA, providers who choose to maintain public archives of previous software versions are required to "clearly inform" users on the risks of using "unsupported software" [58]. Under article 8(3) of the DCD, providers will not be liable if they have informed consumers on the "consequences" of failing to update their software "within a reasonable time" [59]. Both these clauses strikes a balance, allowing users the autonomy to choose whether to apply a security update while holding them liable for damages caused by their decision. There are legitimate reasons for not applying security updates. The patch for the Spectre CPU bug resulted in "performance penalties up to 35%" [60], thus consumers would have to sacrifice performance for security. Since the bug is not remotely exploitable, technically competent users may be able to implement alternative safeguards

53 *Delta Air Lines, Inc v CrowdStrike, Inc Complaint* (n 19), pp. 1

54 reg 2024/2847 (n 6), para. 1

55 Shirriff (n 22)

56 Dir 2019/770 (n 7), para. 1

57 reg 2024/2847 (n 6), para. 56

58 reg 2024/2847 (n 6), art. 13(11)

59 Dir 2019/770 (n 7), art. 8(3)

60 Zhiye Liu, 'Intel CPUs Suffer Performance Hit From New Spectre-v2 Mitigations' (11 March 2022) <https://www.tomshardware.com/news/intel-cpus-performance-hit-spectre-v2-migitations> accessed 18 March 2025

such as turning on site isolation in browsers [61], which may reduce the risk to an acceptable level where patching is not necessary.

The CRA also puts in place stricter requirements for "important products with digital elements", requiring *inter alia* dissemination of security updates without delay in an automatic manner, and public disclosure of "information about fixed vulnerabilities" once a security update is available [62]. Such differentiation allows a balance to be struck, so that providers of software products which do not fall under Annex III [63] are not subjected to unnecessarily onerous requirements, thus allowing them more room to innovate, build and release new features. For example, our hypothetical personal tax filing software may suffer from an integer overflow bug that causes the program to crash if a user enters an income of billions. While technically a security bug, no one would be conceivably affected and it would be a waste of resources to mandate security updates and customer announcements.

6. General Product Safety Regulation and Others

While lack of security updates remain a primary concern for consumer welfare, there is a probability that new feature updates or product iterations may introduce safety issues. The GPSR fills that gap, requiring a "risk assessment" be performed on substantial modifications that may impact product safety [64]. This is also supplemented by article 7(2)(b) of the CRA in which products with a "significant risk of adverse effects" on "health, security and safety" or users are set out in Annex III and have to meet more stringent requirements [65]. Much of the software from the Therac-25 was reused from an earlier machine, the Therac-20. However, because there were substantial modifications in the hardware, the same software resulted in defects in the new iteration, resulting in accidents where patients were given a radiation overdose [66]. Under the GPSR and the CRA, the enhanced scrutiny should reduce the risks of such accidents recurring.

For completeness, it should be highlighted that products certified under the EU Cybersecurity Act must be "provided with up-to-date software" without known vulnerabilities [67]. Also, under the General Data Protection Act (GDPR), appropriate measures, including regular software updates, must be taken to protect personal data [68]. However, due to the voluntary nature of certification and the sector specific nature of the GDPR, the impact of these legislations on consumer welfare is relatively minimal.

7. Comprehensively balancing Consumer Welfare, Safety and Business Interests

The legal instruments we explored tackle software reliability using both proactive as well as

61 Zhiye Liu, 'The Meltdown and Spectre CPU Bugs, Explained' (14 February 2019) <https://www.alertlogic.com/blog/meltdown-spectre-cpu-bugs-explained/> accessed 18 March 2025

62 reg 2024/2847 (n 6), Annex I, Part II

63 reg 2024/2847 (n 6), Annex III

64 reg 2023/988 (n 8), para. 25

65 reg 2024/2847 (n 6), art. 7(2)(b)

66 Nancy Leveson, 'The Therac-25: 30 Years Later' (2017) 50(11) Computer 8, pp. 9

67 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L151/15, art. 51(j)

68 Alana Maurushat and Kathy Nguyen, 'The legal obligation to provide timely security patching and automatic updates' (2022) 3(2) International Cybersecurity Law Review 437, pp. 457

69 Yojna Arora, 'Approaches for Enhancing Reliability of Software Product' (2017) 161(5) International Journal of Computer Applications 9, pp. 10

reactive approaches [69]. The PLD, as it namesake suggests, leans towards defining liability for bugs already present in the software, taking a stance that bugs would inevitably make its way into software and thus taking a reactive approach at addressing bugs. However, the CRA has greater focus on "conformity assessments" [70] while the GPSR mandates "risk assessments" [71], both of which are more proactive at discovering issues or higher risk areas and remediating them before the product enters the market, negating the need for software updates. Thus, the legal instruments complement each other providing comprehensive coverage, ensuring that higher impact bugs which affect safety and security are either tackled proactively or prioritized for automatic patching, while mandating reactive software updates for lower impact bugs.

Since the topic of the essay concerns software updates, the PLD has been explored in greater depth and shown to strike a good balance between provider responsibility and consumer welfare. Firstly, it mandates that software providers fix defects in products [72], tipping the scale greatly in the consumer's favour. However, the PLD only applies to reasonably foreseeable uses and effects [73], exclude circumstances when defects are mandated under regulation [74], exclude open-source software for which there may be no formal structure to impose responsibility [75], and exclude damages when beyond the provider's control [76]. These clauses tip the scales back towards the software provider's favour, resulting in a relatively balanced framework.

However, Li and Faure have argued that the revised PLD may stifle innovation in AI by imposing strict liability on defects [77]. The draw of an AI system is it's self learning behaviour, however there is risk that the AI system might learn discriminatory or unsafe behaviour from wrong sources [78]. Microsoft's AI chatbot, Tay, started "tweeting highly offensive things" after learning from user conversations [79], while ChatGPT has been criticized for unsafe advice such as not asking drivers to avoid using their phones while driving [80]. If such updates to the AI model are considered defects and attract liability, software providers may be discouraged from innovation, which would impact consumer welfare in the long run.

Finally, Colonna argues that open-source hosting services could be deemed a "distributor" under the PLD especially if it is part of a commercial enterprise [81]. This could discourage corporations from hosting open-source projects out of goodwill and probably also limit non-profit foundations from any revenue generating activity, even if done on a minimal scale to cover

70 reg 2024/2847 (n 6), art. 32

71 reg 2023/988 (n 8), para. 25

72 Dir 2024/2853 (n 5), art. 6 and 8

73 Dir 2024/2853 (n 5), art. 7(2)(b) and 7(2)(d)

74 Dir 2024/2853 (n 5), art. 11(1)(d)

75 Dir 2024/2853 (n 5), art. 2(2)

76 Dir 2024/2853 (n 5), para. 51

77 Li and Faure (n 50), pp. 159

78 Li and Faure (n 50), pp. 159

79 Oscar Schwartz, 'In 2016, Microsoft's Racist Chatbot Revealed the Dangers of Online Conversation' (25 November 2019) <https://spectrum.ieee.org/in-2016-microsofts-racist-chatbot-revealed-the-dangers-of-online-conversation> accessed 7 April 2025

80 Oscar Oviedo-Trespalacios and others, 'The risks of using ChatGPT to obtain common safety-related information and advice' (2023) 167 Safety Science 106244 <https://www.sciencedirect.com/science/article/pii/S0925753523001868>, pp. 16

81 Colonna (n 44), sect. 5.2.2

costs, thus affecting the viability of open-source projects.

8. Conclusion

The revised PLD has introduced large strides to consumer welfare and safety in software products by holding providers liable for defects from reasonably foreseeable usage. However, this has been adequately balanced by excluding defects mandated by legislation, open-source software and those beyond the provider's control. While the PLD focuses on mandating software updates, the CRA and GPSR attempts to mitigate the need for updates through proactive conformity and risk assessments. Thus, the legislations are complementary and together aid in improving software quality without imposing onerous requirements on providers.

Nonetheless, there are some concerns. The PLD allows defects that are mandated by regulation, *lacunas* may arise especially in complex interactions between incompatible software and when open-source update are not performed in good faith. It has also been argued that strict liability may stifle innovation in the area of AI and introduce uncertainties in open-source hosting services. Future developments in this area will be of interest as the scales continue to shift with each case.

Bibliography

Cases

Case of Podchasov v Russia [2024] ECHR 33696/19.

Delta Air Lines, Inc v CrowdStrike, Inc Complaint 24CV013621 (2024).

Case C-65/20 *KRONE – Verlag Gesellschaft mbH & Co KG* ECLI:EU:C:2021:471.

Hill v Chief Constable of West Yorkshire [1989] AC 53.

Legislation

Charter of Fundamental Rights of the European Union [2000] OJ C364/1.

Computer Misuse Act 1990.

Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products [1985] OJ L210/29.

Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services) [2019] OJ L136/1.

Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC [2024] OJ L series/1.

Investigatory Powers Act 2016.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L151/15.

Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC [2023] OJ L135/1.

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) [2024] OJ L series/1.

Reports

Government of the United Kingdom, *Fact Sheet - Social Action, Responsibility and Heroism Bill* (2015) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/318839/sarah-bill-fact-sheet.pdf>.

Jeanne Breen Consulting, *Car telephone use and road safety - An overview prepared for the European Commission* (2009) <https://road-safety.transport.ec.europa.eu/document/download/15950308-73f3-4632-a2f6-25fbd1937a5a_en?filename=car_telephone_use_and_road_safety.pdf>.

National Audit Office, *Investigation: WannaCry cyber attack and the NHS* (2018) <https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf>.

Books

Brennan C, *Tort Law* (8th, 2022).

Articles

Arora Y, 'Approaches for Enhancing Reliability of Software Product' (2017) 161(5) International Journal of Computer Applications 9.

Colonna L, 'The end of open source? Regulating open source under the cyber resilience act and the new product liability directive' (2025) 56 Computer Law & Security Review 106105 <https://www.sciencedirect.com/science/article/pii/S0267364924001705>.

Leveson N, 'The Therac-25: 30 Years Later' (2017) 50(11) Computer 8.

Li S and Faure M, 'The Revised Product Liability Directive: A Law and Economics Analysis.' (2024) 15(2) Journal of European Tort Law 140.

Maurushat A and Nguyen K, 'The legal obligation to provide timely security patching and automatic updates' (2022) 3(2) International Cybersecurity Law Review 437.

Oviedo-Trespalacios O and others, 'The risks of using ChatGPT to obtain common safety-related information and advice' (2023) 167 Safety Science 106244 <https://www.sciencedirect.com/science/article/pii/S0925753523001868>.

Secondary Sources

Apple, 'The apps you love. From a place you can trust.' (6 March 2025) <https://www.apple.com/sg/app-store/> accessed 6 March 2025.

Bhargav N, 'DLL Hell Problem' (18 March 2024) <https://www.baeldung.com/cs/dll-hell-problem> accessed 14 March 2025.

Cratecode LLC, 'Exploring the History and Impact of Intel Pentium Processors' <https://cratecode.com/info/pentium-processors> accessed 9 March 2025.

Electronic Privacy Information Center, 'The Clipper Chip' <https://archive.epic.org/crypto/clipper/> accessed 9 March 2025.

European Commission, 'GNU Lesser General Public License (LGPL) 2.1' <https://interoperable-europe.ec.europa.eu/licence/gnu-lesser-general-public-license-lgpl-21> accessed 14 March 2025.

Gatlan S, 'Red Hat warns of backdoor in XZ tools used by most Linux distros' (29 March 2024) <https://www.bleepingcomputer.com/news/security/red-hat-warns-of-backdoor-in-xz-tools-used-by-most-linux-distros/> accessed 9 March 2025.

Google, 'Welcome to the Chrome Web Store' (6 March 2025) <https://chromewebstore.google.com/?pli=1> accessed 6 March 2025.

International Standards Organization, 'IEC 62304:2006 Medical device software — Software life cycle processes' (1 January 2006) <https://www.iso.org/standard/38421.html> accessed 9 March 2025.

Joos T, 'Want to safely use Windows 10 after Microsoft ends support? Meet 0Patch' (13 September 2024) <https://www.pcworld.com/article/2456251/windows-10-will-no-longer-receive-updates-from-october-2025-change-that-with-this-tool.html> accessed 6 March 2025.

Kolsek M, 'The "EventLogCrasher" 0day For Remotely Disabling Windows Event Log, And a Free Micropatch For It' (31 January 2024) <https://blog.0patch.com/2024/01/the-eventlogcrasher-0day-for-remotely.html> accessed 6 March 2025.

La Quadrature du Net, 'All-out mobilization against the French "war-on-drugs" law' <https://www.laquadrature.net/en/warondrugslaw/> accessed 5 April 2025.

Lacoma T, 'Google's Nest Secure Has Fully Shut Down: We've Got Answers if You're Worried' (24 April 2024) <https://www.cnet.com/home/security/googles-nest-secure-has-fully-shut-down-weve-got-answers-if-youre-worried/> accessed 8 March 2025.

Liu Z, 'The Meltdown and Spectre CPU Bugs, Explained' (14 February 2019) <https://www.alertlogic.com/blog/meltdown-spectre-cpu-bugs-explained/> accessed 18 March 2025.

— 'Intel CPUs Suffer Performance Hit From New Spectre-v2 Mitigations' (11 March 2022) <https://www.tomshardware.com/news/intel-cpus-performance-hit-spectre-v2-migitations> accessed 18 March 2025.

Martin A, 'Apple turns off iCloud encryption feature in UK following reported government legal order' (21 February 2025) <https://therecord.media/apple-encryption-feature-off-britain> accessed 5 April 2025.

Microsoft Security Response Center, 'Customer Guidance for WannaCrypt attacks' (13 May 2017) <https://msrc.microsoft.com/blog/2017/05/customer-guidance-for-wannacrypt-attacks/> accessed 4 March 2025.

RTCA, Inc, 'Software Considerations in Airborne Systems and Equipment Certification' (1 December 1992) <https://antena.fe.uni-lj.si/literatura/Razno/Avionika/rtca/Rtca%20Do-178B.pdf> accessed 9 March 2025.

Schwartz O, 'In 2016, Microsoft's Racist Chatbot Revealed the Dangers of Online Conversation' (25 November 2019) <https://spectrum.ieee.org/in-2016-microsofts-racist-chatbot-revealed-the-dangers-of-online-conversation> accessed 7 April 2025.

Scroxton A, 'CrowdStrike update chaos explained: What you need to know' (29 July 2024) <https://www.computerweekly.com/feature/CrowdStrike-update-chaos-explained-What-you-need-to-know> accessed 9 March 2025.

Shirriff K, 'Intel's $475 million error: the silicon behind the Pentium division bug' (1 December 2024) <https://www.righto.com/2024/12/this-die-photo-of-pentium-shows.html> accessed 8 March 2025.

Smalley S, 'Swedish authorities seek backdoor to encrypted messaging apps' (25 February 2025) <https://therecord.media/sweden-seeks-backdoor-access-to-messaging-apps> accessed 5 April 2025.