Coordinated Vulnerability Disclosure: Providing legal Safe Harbour with minimal risks

Name: Benjamin Lim
Email: s2599925@ed.ac.uk
Programme of Study: Information Technology Law
Word Count: 9998

Contents

Introduction

1.1. Introduction to Vulnerability Disclosure

Companies today are eagerly launching new services to capture market share. Amidst this competitive landscape, it is increasingly common for applications and websites to contain undiscovered security vulnerabilities [1], which are flaws that were introduced unintentionally. When exploited by hackers, these security vulnerabilities could result in financial losses, customer data leaks, or downtime resulting in inconvenience to customers [2]. Throughout the dissertation, I will use the term 'hacker' to denote someone with malicious intent that possesses cybersecurity skills capable of intentionally causing harm.

Given the ubiquity of digital services, it is increasingly likely that a layperson or a security researcher may be the first to come across a vulnerability [3]. In this dissertation, the term 'layperson' will refer to a responsible member of society who chanced upon a vulnerability while the term 'security researcher' will refer to someone with good intentions and sufficient knowledge to actively search for vulnerabilities. Upon discovery, they could choose to privately disclose the vulnerability to the relevant organization owning the service. However, organizations may not take the report seriously [4], thus continuing to put others at risk should hackers chance upon the same vulnerability. I will use the term 'organization' to refer to private companies, government bodies or any formally organized group of people. Alternatively, upon discovery, they could also fully disclose the vulnerability to the public, putting 'pressure' on the relevant organization to fix it timeously since the public is now aware that the service is not secure and may avoid its use [5]. However, since the organization finds out at the exact same time as everyone else, it leaves a window of opportunity for hackers to exploit the vulnerability before a fix is released [6].

Coordinated Vulnerability Disclosure (CVD) gained momentum around the turn of the century [7]. Essentially, the CVD reporter would first privately disclose the vulnerability, giving organizations a head start in developing a fix, but set a reasonable timeline for public disclosure [8] so organizations cannot delay the fix indefinitely and continue exposing others to that risk. We will use the term 'CVD reporter' to refer to a collection of both laypersons and security researchers who disclose vulnerabilities to the organization. CVD strikes a good balance between private disclosure and public disclosure, increasing service

1 Jakub Vostoupal and others, 'The legal aspects of cybersecurity vulnerability disclosure: To the NIS 2 and beyond' (2024) 53 Computer Law & Security Review 105988 <https://www.sciencedirect.com/science/article/pii/S0267364924000554>, pp. 3

2 'Encouraging vulnerability treatment: Overview for policy makers' [2021] (307) IDEAS Working Paper Series from RePEc, pp. 5

3 National Telecommunications and Information Administration, *Vulnerability Disclosure Attitudes and Actions* (2016) <https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf>, pp. 4

4 Ali Ahmed, Amit Deokar, and Ho Cheung Brian Lee, 'Vulnerability disclosure mechanisms: A synthesis and framework for market-based and non-market-based disclosures' (2021) 148 Decision Support Systems 113586 <https://www.sciencedirect.com/science/article/pii/S0167923621000968>, pp. 2

5 Ahmed, Deokar, and Lee (n 4), pp. 2

6 Mingyi Zhao, Aron Laszka, and Jens Grossklags, 'Devising Effective Policies for Bug-Bounty Platforms and Security Vulnerability Discovery' (2017) 7 Journal of Information Policy 372, pp. 28

7 Uldis Ķinis, 'From Responsible Disclosure Policy (RDP) towards State Regulated Responsible Vulnerability Disclosure Procedure (hereinafter – RVDP): The Latvian approach' (2018) 34(3) Computer Law & Security Review 508 <https://www.sciencedirect.com/science/article/pii/S0267364917303606>, pp. 514

8 Marleen Weulen Kranenbarg, Thomas Holt, and Jeroen van der Ham, 'Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure' (2018) 7(1) Crime Science, pp. 1

quality at little cost [9]. Organizations will usually publish a CVD policy detailing the scope of the program, contact details where reports can be sent, and a disclosure timeline [10]. Many organizations have benefited from such an arrangement [11], which has led to the rise of bug bounty programs in recent years which goes one step further by offering cash rewards for vulnerability reports, thus enticing active participation from security researchers [12]. Some have even described it as crowdsourced security testing where organizations only pay for 'valid vulnerabilities discovered' [13], as opposed to hiring security consultants where fees are fixed regardless of whether the consultants managed to find any vulnerabilities.

1.2. Tackling the issue of Safe Harbour in CVD programs

Amidst the successes of a CVD program, it is poignant to note that CVD reporters may not be adequately protected and may be liable to legal repercussions in breach of *inter alia* Computer Misuse Act (CMA) and copyright laws [14]. Thus, laypersons who have incidentally chanced upon vulnerabilities may be reluctant to step forward due to potential legal implications. Security researchers may be overwhelmed by jurisdictional challenges, lack of resources to handle complex legal issues and the uncertainty introduced by broad sweeping statements, all of which highlight the need for safe harbour and will be explored in the second chapter.

Chapter three will take us through a chronological journey of various attempts at providing guidance and legislating safe harbour in CVD programs, starting off with the Dutch National Cyber Security Centre (NCSC) and prosecutor's guidelines, the US Digital Millennium Copyright Act (DMCA), the French Digital Republic Act (FDRA), the UK Cybersecurity Act and Product Security and Telecommunications Infrastructure (PSTI) regulation, and finally the ongoing transposition of the Network and Information Systems Directive 2 (NIS2). We will explore the legal principles of intent, proportionality and subsidiarity which many legislations subscribe to, using it as a foundation for the future chapters.

In chapter four, we will examine case law to understand how the courts determine the intention of the CVD reporter and provide practical guidance in crafting a Safe Harbour clause that closely mirrors the court's stance, reducing the risks of an excessively permissible clause being exploited by hackers.

Following that, we will analyse the principle of proportionality in chapter five, evaluating cases where the *actus reus* is disproportional to the *mens rea*. Similarly, we will be proposing guidance on crafting a comprehensive clause to ensure that such disproportional actions cannot qualify for Safe Harbour protection.

We will end off in chapter six with an academic analysis of the principle of subsidiarity, which dictates that issues should be resolved at a local level where possible. Involvement of the press should be the last resort after communications have broken down. Premature involvement may suggest prioritization of fame or recognition over altruistic intentions.

This dissertation will primarily focus on leg-

9 Mingyi Zhao, Jens Grossklags, and Peng Liu, 'An Empirical Study of Web Vulnerability Discovery Ecosystems' (CCS '15, Association for Computing Machinery 2015) <https://doi.org/10.1145/2810103.2813704>, sect. 4.3.1

10 'Encouraging vulnerability treatment: Overview for policy makers' (n 2), pp. 24

11 Zhao, Laszka, and Grossklags (n 6), pp. 2

12 John Jackson, *Corporate Cybersecurity: Identifying Risks and the Bug Bounty Program* (1st, 2022), sect. 1.8

13 Suresh Malladi and Hemang Subramanian, 'Bug Bounty Programs for Cybersecurity: Practices, Issues, and Recommendations' (2020) 37(1) IEEE Software 31, pp. 31-32

14 European Union Agency for Cybersecurity, *Coordinated vulnerability disclosure policies in the EU* (2022) <https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu>, pp. 62

islation and case law in the UK and EU but will occasionally bring in examples from other jurisdictions when equivalents are not found in the UK or EU to highlight lacunas and possible pitfalls. While the CMA might not directly apply in the EU, it is largely aligned with the Council of Europe Convention on Cybercrime especially in the offence of illegal access and system interference [15], which are the relevant offences that CVD is likely to contravene. It is hoped that the practical guidance provided in this dissertation will benefit organizations implementing CVD policies under the NIS2 directive.

Understanding the need for Safe Harbour in CVD

Before venturing into recommendations for constructing safe harbour clauses, we must first examine why safe harbour is required to begin with. In this chapter, we will show how CVD activity could be illegal, how it's inherent legal complexity may disadvantage CVD reporters, and how organizations can benefit from increased certainty with safe harbour clauses. This demonstrates that safe harbour is required to protect both CVD reporters and organizations from legal risks.

2.1. Illegality of CVD Activity

Section 1 of the CMA proscribes intentional acts to gain unauthorized access to computer systems [1]. According to the UK Crown Prosecution Service (CPS) guidance on prosecuting CMA cases, the *actus reus* of the offence is the physical act of gaining unauthorized access [2]. Knowledge that the access is unauthorized and the continued effort despite that constitutes the *mens rea* of the offence [3]. Unfortunately, such prosecutory guidelines do not leave room for any 'higher social purposes'. A good Samaritan might intentionally leap over a fence fully knowing that the access is unauthorized with full intention to trespass the property so that he can save a child from a burning building. In the digital realm, security researcher Rob Dyke, discovered and reported leaked credentials to Apperta Foundation, a UK non-profit supported by the National Health Service (NHS) [4]. While he was initially thanked by the organization for 'responsible reporting', the organization later filed a police report for 'Computer Misuse' [5]. The *prima facie* intention of his act was to potentially gain unauthorized access to Apperta's credentials, however the 'higher social purpose' was to highlight the exposure of those credentials so they could be secured. Given current CPS guidelines, such acts would contravene Section 1 of the CMA and be liable to possible prosecution. Hans Schröder, a fifteen-year-old who visited Habbo, an online chatroom, had to contact the Zendesk helpdesk for a request [6]. During the process, he inadvertently used a different email address and found that the account on Habbo was 'automatically linked' to the Zendesk account with no verification performed [7]. This sparked an idea where he used a Zendesk employee's email to

15 Society for Computers & Law, 'Cybercrime and the UK' (30 June 2005) <https://www.scl.org/766-cybercrime-and-the-uk/> accessed 2 August 2025

1 Computer Misuse Act 1990, sect. 1

2 The Crown Prosecution Service, 'Computer Misuse Act' (3 August 2023) <https://www.cps.gov.uk/legal-guidance/computer-misuse-act> accessed 1 June 2025

3 The Crown Prosecution Service (n 2)

4 Bleeping Computer LLC, 'Engineer reports data leak to nonprofit, hears from the police' (25 March 2021) <https://www.bleepingcomputer.com/news/security/engineer-reports-data-leak-to-nonprofit-hears-from-the-police/> accessed 15 June 2025

5 Bleeping Computer LLC (n 4)

6 Chris van't Hof, *Helpful Hackers: How the Dutch Do Responsible Disclosure* (1st, 2016), pp. 78-79

7 van't Hof (n 6), pp. 78-79

create an account on Habbo, giving him access to privileged data including tickets raised by other Habbo users and their details such as IP addresses [8]. He called Habbo the next day to report the vulnerability [9]. While Schröder might have been motivated by curiosity, he understood the gravity of the situation and immediately exhibited ethical behaviour. Even though he did not leak or use the privileged data in any way, he was subjected to a police investigation for Computer Misuse as well [10]. In both cases, no charges were subsequently filed but the stress of being subjected to a police investigation and the legal costs incurred in seeking legal advice on the crimes that they were charged with cannot be overlooked. Safe Harbour provisions can protect future Dykes and Schröders from unnecessary stress, costs incurred and potential criminal charges purely from trying to do a good deed.

At this juncture, it is also pertinent to note that the discovery of most vulnerabilities may entail contravening the CMA [11] [12]. If Dyke did not download the code repository to confirm his hunch, he would never have known if it contained leaked credentials. If Schröder had not tried to register a Habbo account with a Zendesk employee's email, he would never have known if it was possible, or if he would be blocked from doing so. Allowing hypothetical scenarios to be submitted would be untenable as organizations will likely receive many unrealistic simulations and eventually pay no heed to such reports. This scenario played out in the Netherlands where a security researcher, Oscar Koeroo gained access to a webpage which contained controls for water pumps at the town of Veere [13]. Koeroo hypothesized that it might be possible to reverse the direction of the pumps and flood the town [14]. Upon notifying the administrator of the system, the administrator immediately dismissed his hypothesis, claiming that it was 'not possible' as the pumps were on a 'separate network' and because 'their operation is very specific' [15]. Koeroo only gained some credibility after he revealed the vendor of the software used to control the pumps and after he worked with a manager of a separate facility to switch off the heating for an hour, providing 'hard evidence' that this type of an attack was possible [16]. Thus, this debunks the argument that CVD can be done effectively without contravening the CMA and that Safe Harbour is not required.

The lack of Safe Harbour protection will have a 'chilling effect' [17] [18], discouraging CVD reporters from stepping forward due to potential legal implications, leaving society at risk should these vulnerabilities be independently

8 van't Hof (n 6), pp. 78-79

9 van't Hof (n 6), pp. 78-79

10 van't Hof (n 6), pp. 78-80

11 NIS Cooperation Group, *Guidelines on Implementing National Coordinated Vulnerability Disclosure Policies* (2023) <https://ec.europa.eu/newsroom/dae/redirection/document/99973>, pp. 5

12 British Standards Institute, *TC: Tracked Changes. Information technology. Security techniques. Vulnerability disclosure* (2015) <https://discovered.ed.ac.uk/permalink/44UOE_INST/1viuo5v/cdi_bsi_primary_000000000030413565>, para. 9.4.2

13 van't Hof (n 6), pp. 49

14 van't Hof (n 6), pp. 49

15 van't Hof (n 6), pp. 49

16 van't Hof (n 6), pp. 52

17 British Standards Institute (n 12), para. 5.5.4

18 'Encouraging vulnerability treatment: Overview for policy makers' (n 2), pp. 27

19 Centre for European Policy Studies, *Software Vulnerability Disclosure in Europe* (2018) <https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges/>, pp. 10

discovered by a hacker. Studies have shown that 5% to 20% of vulnerabilities are rediscovered within a year [19], hence this represents a material risk. This scenario played out in the REvil ransomware attack. Security researchers had responsibly disclosed the vulnerability to the organization 3 months earlier, but before the organization could fully remediate the vulnerability, hackers independently discovered the same vulnerability, causing 'one of the most significant ransomware attacks in history' [20].

2.2. CVD reporters are ill-equipped to handle inherent legal complexity

Complicating the issue is the fact that 17% of CVD reporters claim to be 'accidental finders' or laypersons while 50% identify as security researchers working independently [21]. Schröder would probably be considered an 'accidental finder' while Koeroo falls into the category of a security researcher, having a day job in IT and engaging in CVD in his free time [22]. The statistics are not surprising as companies hire security researchers to improve their own products internally and have little incentive to task them with finding vulnerabilities in other products on their dime. Thus, most CVD reporters do not have a legal background nor easy access to legal advice from in-house legal counsel. The legal technicalities surrounding most CVD policies are complex [23]. Walshe posits that understanding 'rights and obligations' in each contract is not sufficient and CVD reporters will also need to understand the 'order of precedence' when policies conflict [24]. This is especially apparent with bug bounty platforms, which some organizations use to reduce the administrative burden of correspondence and handling payments to CVD reporters globally. These platforms have their own code of conduct [25] which may conflict with those set by the organization's CVD policy.

Elazar notes that many policies contain 'vague or generic references to the law' [26]. One such possible statement could be found in what was Twitter's bug bounty program in which it is mentioned that CVD reporters must 'comply with all applicable laws in connection with [their] participation in this program' [27]. It is thus left as an exercise to the legally untrained CVD reporter to determine which types of laws are relevant, whether he should be concerned with laws in his home jurisdiction or those in what was Twitter's jurisdiction [28] among other concerns. Such cross border issues 'aggravate legal risks' to CVD reporters [29]. Hostile policies are a factor in discouraging 60% of survey respondents from voluntarily engaging in CVD programs [30] and causing 4% of respondents to turn a blind

[20] Lily Newman, 'The Unfixed Flaw at the Heart of REvil's Ransomware Spree' (8 June 2021) <https://www.wired.com/story/revil-ransomware-kaseya-flaw-fix-disclosure-april/> accessed 8 July 2025

[21] National Telecommunications and Information Administration (n 3), pp. 4

[22] van't Hof (n 6), pp. 51

[23] 'Encouraging vulnerability treatment: Overview for policy makers' (n 2), pp. 28

[24] Thomas Walshe and Andrew Simpson, 'Towards a Greater Understanding of Coordinated Vulnerability Disclosure Policy Documents' (2023) 4(2) Digital Threats: Research and Practice 1 <https://www.sciencedirect.com/science/article/pii/S0925753523001868>, pp. 29:17

[25] hackerone, 'Code of Conduct' <https://www.hackerone.com/policies/code-of-conduct> accessed 6 June 2025

[26] Walshe and Simpson (n 24), pp. 29:18

[27] Aron Laszka and others, 'The Rules of Engagement for Bug Bounty Programs' (Springer-Verlag 2018) <https://doi.org/10.1007/978-3-662-58387-6_8>, pp. 154

[28] Diane Rowland, Uta Kohl, and Andrew Charlesworth, *Information Technology Law* (5th, 2016), pp. 40

[29] 'Encouraging vulnerability treatment: Overview for policy makers' (n 2), pp. 28

[30] National Telecommunications and Information Administration (n 3), pp. 6

eye to vulnerabilities they inadvertently discovered [31], leaving them for hackers to find.

2.3. Organizations benefit from increased certainty

A well-crafted Safe Harbour policy can be beneficial to the organization as well. Most organizations stipulate the choice of law when negotiating commercial contracts as it provides greater certainty through known precedents that can be relied upon [32]. A case of interest, R v Walker, transpired in New Zealand courts where the judge concluded that Walker's actions were 'motivated by curiosity' rather than 'criminal intent or malice' even though Walker profited over $36,000 and caused $13,000 in damages from the hacking incident [33] [34]. For completeness, it should be noted that Walker was under the age of 18 and on the autism spectrum, nonetheless Maurushat believes that his age and health condition was not a factor in the decision [35]. Such precedents in remote jurisdictions demonstrate how a well-crafted Safe Harbour policy which clearly defines the scope of the program can protect organizations from unforeseen risks. Studies have shown that participants on the HackerOne bug bounty platform hail from more than 70 countries [36], thus this represents a real risk. Given a choice, organizations would have excluded activities which cause financial loss from Safe Harbour protection rather than leaving it to the discretion of courts in remote jurisdictions.

Having justified the need for a Safe Harbour clause, it is important to point out that a poorly crafted clause can expose the organization to risks where malicious actions are indemnified under the clause, allowing hackers to participate in the program and act with impunity without any legal repercussions. The courts will not intervene in a 'bad bargain' [37]. If an organization mistakenly omits a clause to prohibit automated scanning activity and subsequently suffers an outage due to persistent scanning from CVD reporters, the organization will not be able to seek recourse from the CVD reporters. Conversely, an overly restrictive policy limits the vulnerabilities that CVD reporters can find, leaving many more to be discovered by hackers who exploit them for personal gain outside the boundaries of the CVD program. In subsequent chapters, we will delve into recommendations that will guide organizations in crafting clauses that strike a balance between benefiting from CVD activity while reducing the risks.

Contextualizing approaches at promoting Safe Harbour for CVD

Having explained the need for a safe harbour clause in the previous chapter, we can shift our focus onto how we can implement safe harbour in a CVD program. We will not be starting from scratch, instead we will analyse previous attempts at implementing safe harbour by states and the legal principles underpinning eligibility for safe harbour. These legal principles of intention, proportionality and subsidiarity will serve as a foundation on which we will propose recommendations in the subsequent chapters.

---

31 National Telecommunications and Information Administration (n 3), pp. 5

32 Leonard Manning, 'Choice of Law for Commercial Contracts' (1961) 2(2) Boston College Law Review <https://bclawreview.bc.edu/articles/2967/files/63f315c09dc7c.pdf>, pp. 241

33 Alana Maurushat, *Disclosure of Security Vulnerabilities* (1st, 2013) pp. 43

34 *R v Walker* [2008] New Zealand High Court Hamilton CRI2008-0750711 1201

35 Maurushat (n 33) pp. 43-44

36 Zhao, Laszka, and Grossklags (n 6), pp. 30

37 *Chappell v Nestle* [1960] AC 87, pp. 114

3.1. Dutch NCSC and Prosecution Guidelines (2013)

The idea of providing safe harbour to CVD reporters was first mooted in the Dutch NCSC Guidelines for Responsible Disclosure (Dutch GRD) back in 2013, coming hot on the heels of the Groene Hart hack [1]. The incident involved an individual who had cracked the password to a hospital's file server and downloaded numerous medical records [2]. He then took screenshots, reported the vulnerability to the hospital and to relevant authorities, published details about the vulnerability before finally deleting the downloaded files [3]. The guidelines were 'surprisingly practical for an official document', forbidding CVD reporters from *inter alia* 'social engineering' or 'brute force' attacks and encouraging organizations not to pursue legal action in return [4]. At the same time, the prosecution service issued a circular on prosecuting cases of 'ethical' hacking [5], formulating the three tests that would eventually gain widespread acceptance [6]. Firstly, the intent of the individual needed to include an 'overriding general public interest', secondly, the individual's actions needed to be proportional to the objective and lastly, the individual had to adhere to the principle of subsidiarity [7].

This guidance has remained largely unchanged in the 2018 version, however, there has been a greater emphasis on prosecutorial discretion, and the approach seems to be to offer safe harbour at a state level if the CVD reporter is eligible, regardless of whether the organization chooses to offer safe harbour [8]. This approach benefits the Dutch public as the prosecution service makes the final determination whether to prosecute. If an organization acts unreasonably and chooses to make a police report even when the CVD reporter has fully abided by the guidelines, the prosecution service can choose not to take further action. However, one downside is that the organization can still pursue civil action for *inter alia* copyright infringement.

3.2. US DMCA Good Faith exemption (2015)

The issue of copyright infringement during vulnerability enumeration was addressed just a few years later in the US with the 2015 DMCA exemption for 'Good Faith Security Research', which considers security research as 'noninfringing fair use' of software [9]. This occurred just months after security researchers in the US, risking legal action, demonstrated a vulnerability which allows hackers to remotely control a car over the Internet [10]. The manufacturer eventually released a security update to fix the issue [11].

1 van't Hof (n 6), pp. 106-107

2 van't Hof (n 6), pp. 94

3 van't Hof (n 6), pp. 94

4 van't Hof (n 6), pp. 107-108

5 'Encouraging vulnerability treatment: Overview for policy makers' (n 2), pp. 29

6 van't Hof (n 6), pp. 108-109

7 van't Hof (n 6), pp. 109

8 Dutch National Cyber Security Centre, *Coordinated Vulnerability Disclosure: the Guideline* (2018) <https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline>, pp. 9-10

9 USCopyright Office, Library of Congress, 'Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies' (28 October 2015) <https://cdn.loc.gov/copyright/1201/2015/fedreg-publicinspectionFR.pdf> accessed 15 June 2025, pp. 48

10 Samuel Gibbs, 'Jeep owners urged to update their cars after hackers take remote control' (21 July 2015) <https://www.theguardian.com/technology/2015/jul/21/jeep-owners-urged-update-car-software-hackers-remote-control> accessed 28 June 2025

11 Gibbs (n 10)

Unfortunately, there exist no such exemption in both the UK and EU even today [12], and Apperta was able to take civil action against Dyke in 2021. Section 296ZA of the Copyright, Designs and Patents Act (CDPA) as well as Article 6(1) of the InfoSoc Directive both prohibit the circumvention of any technological protection mechanisms controlling access to copyrighted works [13] [14]. The discovery of a vulnerability in copyrighted software will entail successful circumvention of protection mechanisms preventing unauthorized access. It is therefore difficult to argue that those were not protection mechanisms because in that case, the access would not be unauthorized. A closer reading of Section 296ZA(2) of the CDPA may reveal some *prima facie* exemption for 'research into cryptography', however scholars have cautioned that the law remains ambiguous [15], and the exception may apply only when research is being done to understand how it works or for interoperability reasons [16] but may not apply when research is done with a purpose of breaking it, as doing so 'prejudicially affect[s] the copyright owner' [17]. Thus, security research aimed at breaking protection mechanisms would likely contravene copyright laws in the UK and EU.

3.3. French Digital Republic Act (2016)

The Dutch may have been the first to provide safe harbour at a state level, but they are definitely not the last. The FDRA [18] is worthy of mention as it uses a different approach that may be able to address the downside of organizations pursuing civil action. Article 47 of the FDRA exempts persons, who inform the national authority of vulnerabilities in good faith, from Article 40 of the French Criminal Procedure Code [19]. Firstly, the exemption is codified in law and provides stronger certainty than finicky prosecutorial discretion. Apart from that, Article 47 of the FDRA also requires that the national authority preserves the confidentiality of the CVD reporter [20], thus ensuring that organizations cannot find out the identity and thus subsequently take civil action against the CVD reporter. This level of protection is not seen even in the Dutch GRD, in which it is mentioned that the NCSC cannot 'guarantee that the owner will not take legal action' [21].

However, providing safe harbour in legislation is no easy feat. Latvia attempted to codify safe harbour as an amendment to their criminal law, but the amendment failed to pass due to objections from the police and interior ministry, who believed that 'sufficient and grounded risk analysis' was not performed and that the amendment might lead to 'unexpected and un-

12 Centre for European Policy Studies (n 19), pp. 47

13 Copyright, Designs and Patents Act 1988, sect. 296ZA

14 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (InfoSoc Directive) [2001] OJ L167/10, art. 6(1)

15 Joseph Godfrey, 'Who's afraid of reverse engineering?' (2024) 1 Intellectual Property Quarterly 50, pp. 6

16 Centre for European Policy Studies (n 19), pp. 47

17 Peter Groves, 'The copyright owner's rights (1)' <https://sites.google.com/site/ipsojurepages/copyright/the-copyright-owner-s-rights-1> accessed 15 June 2025

18 Law No 2016-1321 of October 7, 2016, for a Digital Republic, France

19 Law No 2016-1321 of October 7, 2016, for a Digital Republic, France, art. 47

20 Law No 2016-1321 of October 7, 2016, for a Digital Republic, France, art. 47

21 Dutch National Cyber Security Centre (n 8), pp. 14

22 Ķinis (n 7), pp. 521-522

predicted consequences' [22]. Closer to home, there have been calls to reform the UK CMA [23] and to introduce amendments to the PSTI Bill [24] without much success. The amendment aimed to protect security researchers from 'spurious legal action' [25], but was withdrawn citing concerns of unintentional loopholes and law enforcement concerns [26], similar to the case in Latvia.

3.4. Cybersecurity Act (2019) and UK PSTI Regulations (2023)

Thus far, we have explored legislations permitting CVD at a state level. The Cybersecurity Act takes a different approach, targeting vendors who aim to qualify for the Cybersecurity Certification scheme and mandating they put in place a CVD process which allows 'previously undetected cybersecurity vulnerabilities' to be 'reported and dealt with' [27] [28]. On a similar note, Schedule 1 of the UK PSTI Regulations 2023 also mandates that vendors of Internet connected products have a 'point of contact' for reporting security issues and that 'status updates' must be provided until resolution of the reported issue [29], which expounds on the principle of subsidiarity. As explained in the previous paragraph, attempts at introducing safe harbour amendments to the PSTI failed to pass.

Although these regulations only target vendors offering IT products and services, they do have a sizable impact. Surveys have shown that up to 55% of companies utilize off-the-shelf technology solutions [30], hence regulations which mandate vendors to support a CVD program have a wider effect as the CVD reporters can report vulnerabilities directly to these vendors even if the organization deploying the solution does not have a CVD program. Had such legislation been in place, Koeroo could have directly reported the vulnerability in the pump software to the vendor Aquaview [31], perhaps experiencing a smoother reporting process compared to liaising with the administrator of the facility which may not be as conversant with the inner workings of the software.

3.5. NIS2 Directive (2022)

The NIS2 directive introduced in 2022 includes a 'framework for coordinated vulnerability disclosure' that was not found in its predecessor

23 Alex Scroxton, 'Lords move to protect cyber researchers from prosecution' (20 June 2022) <https://www.computerweekly.com/news/252521716/Lords-move-to-protect-cyber-researchers-from-prosecution> accessed 28 June 2025

24 HL Deb 6 June 2022, vol 822, col 1051

25 CyberUp, 'Campaign responds to withdrawal of amendment to update Computer Misuse Act' (9 January 2025) <https://www.cyberupcampaign.com/news/campaign-responds-to-withdrawal-of-amendment-to-update-computer-misuse-act> accessed 28 June 2025

26 HL Deb 28 January 2025, vol 843, col 182

27 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 54(1)(m)

28 Yoon Sang Pil and Roger Lee, *Big Data, Cloud Computing, and Data Science Engineering* (1st, Switzerland, 2023), pp. 125

29 The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023, Schedule 1, para. 2

30 Baker McKenzie, *2021/2022 Digital Transformation & Cloud Survey: A Wave of Change* (2021) <https://www.bakermckenzie.com/-/media/files/insight/publications/2021/12/2021-digital-transformation--cloud-survey--a-wave-of-change.pdf>, pp. 15

31 van't Hof (n 6), pp. 49

[32]. Article 12 of the NIS2 directive requires that member states designate a 'coordinator' that facilitates the reporting process between the CVD reporter and the organization [33]. Following in the FDRA's footsteps, the coordinator is required to preserve the CVD reporter's anonymity should it be requested [34]. CVD reporters who are most risk adverse can take advantage of the anonymity, while those who are willing can waive anonymity and receive public recognition for their good deed. While the FDRA mandates the preservation of anonymity [35], and appears to be *prima facie* different from having the choice of anonymity, the *de facto* effect may not be different as French CVD reporters could still pierce the veil of anonymity by stepping out and claiming credit should they wish to do so. Finally, Recital 60 of the NIS2 directive exhorts member states to address the 'potential exposure to criminal liability' experienced by security researchers to the extent possible [36]. NIS2 has left the ball in the court for member states to decide whether to mandate safe harbour. In the next section, we will explore Belgium's transposition of the NIS2 directive and understand the decisions they have made.

3.6. NIS2 Directive: Belgian transposition (2024)

Article 23 of Belgium's transposition of the NIS2 framework, which was passed in 2024, states that 'whistleblowers' are deemed not to infringe various articles of the Criminal Code pertaining to computer misuse as long as they fulfil the following criteria [37] [38]. They must not have acted with the intention to cause harm [39]. They must provide a 'simplified notification' within 24 hours and a 'full notification' within 72 hours of discovering the vulnerability [40]. They must not have gone 'beyond what was necessary and proportionate' to verify the existence of the vulnerability [41]. Finally, they must not publicly disclose the vulnerability without consent of the relevant authority [42]. This is very much similar to the principles of intent, proportionality and subsidiarity first proposed by the Dutch guidelines, albeit with an extra clause requiring timely reporting of vulnerabilities. The requirement for timely reporting can be viewed as an extension of subsidiarity. CVD reporters acting in good faith should aim to report vulnerabilities as soon as possible so they could be patched to prevent

32 Sandra Schmitz and Stefan Schiffner, 'Responsible Vulnerability Disclosure under the NIS 2.0 Proposal' (2021) 12(5) Journal of Intellectual Property, Information Technology and Electronic Commerce Law, pp. 455

33 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L333/80, art. 12

34 Dir 2022/2555 (n 33)

35 Law No 2016-1321 of October 7, 2016, for a Digital Republic, France, art. 47

36 Dir 2022/2555 (n 33), recital. 60

37 Royal Decree implementing the law of 26 April 2024 establishing a framework for the cybersecurity of network and information systems of general interest for public security, Belgium, art. 23

38 Charlotte Somers and Koen Vranckaert, 'Ethical hacking under the Belgian NIS2-law: still a safe haven?' (29 April 2025) <https://www.law.kuleuven.be/citip/blog/ethical-hacking-under-the-belgian-nis2-law-still-a-safe-haven/> accessed 21 May 2025

39 Royal Decree implementing the law of 26 April 2024 establishing a framework for the cybersecurity of network and information systems of general interest for public security, Belgium, art. 23(1)

40 Royal Decree implementing the law of 26 April 2024 establishing a framework for the cybersecurity of network and information systems of general interest for public security, Belgium, art. 23(2)

41 Royal Decree implementing the law of 26 April 2024 establishing a framework for the cybersecurity of network and information systems of general interest for public security, Belgium, art. 23(3)

42 Royal Decree implementing the law of 26 April 2024 establishing a framework for the cybersecurity of network and information systems of general interest for public security, Belgium, art. 23(4)

hackers from taking advantage. Delayed reporting cast doubts on the true intent of the CVD reporter as it raises the possibility that the individual might have exploited the vulnerability for a period of time or might have attempted to sell the vulnerability on the black market prior to disclosure [43] [44].

3.7. Promoting Safe Harbour: Role of Organizations with respect to States

In this chapter, we have observed how multiple jurisdictions have adopted the same few principles of intent, proportionality and subsidiarity, forming a legal framework to determine if a CVD reporter has acted in good faith. Netherlands, France and Belgium have put in place safe harbour exceptions albeit through differing methods such as prosecutorial discretion or through legislation. Latvia and the UK have attempted to amend legislation to promote safe harbour but face challenges from legislators. Finally, other member states are also considering their options with Hungary, Germany and Austria favouring prosecutorial discretion and Portugal, Greece and Slovenia favouring amendment of criminal laws [45]. In the interest of brevity, we have not explored every jurisdiction in detail, but have distilled the common principles of intent, proportionality and subsidiarity which will guide us crafting recommendations in the following chapters.

Even though this chapter examines efforts undertaken by states, it remains relevant to organizations because once NIS2 is fully in force, even organizations without a CVD program may find themselves at the receiving end of a vulnerability report forwarded from the coordinating agency [46] [47]. It is more important now than ever for organizations to understand how the courts evaluate if certain actions are eligible for safe harbour protection and develop a CVD policy that is aligned with that position. A CVD policy guides CVD reporters on acceptable behaviour and also prepares staff to receive and process CVD reports [48]. Now that the floodgates are opening, organizations should start placing markers to guide excess water flow away from them, instead of reacting only when the water reaches them.

As discussed in the previous chapter, an overly relaxed policy may allow hackers free reign with no legal recourse. Under NIS2, an overly strict policy provides a false sense of security [49]. If a particular action is prohibited in the organization's program but permitted as good faith under the NIS2 transposition, CVD reporters can still make the report through the coordinating agency [50], leaving the organization befuddled and scrambling to address vulnerabilities in areas outside what they originally planned for. Thus, the following chapters will utilize these common principles, with the support of case law, to provide sound recommendations that prepare organizations for the CVD requirement in the upcoming NIS2 transposition.

43 'Encouraging vulnerability treatment: Overview for policy makers' (n 2), pp. 18

44 Jaziar Radianti, Eliot Rich, and Jose J Gonzalez, 'Vulnerability Black Markets: Empirical Evidence and Scenario Simulation' (HICSS '09, Institute of Electrical and Electronics Engineers 2009) <https://doi.org/10.1109/HICSS.2009.504>, pp. 1

45 European Union Agency for Cybersecurity (n 14), pp. 74

46 Vostoupal and others (n 1), pp. 7

47 Zhao, Laszka, and Grossklags (n 6), pp. 29

48 Centre for European Policy Studies (n 19), pp. 5-6

49 European Union Agency for Cybersecurity (n 14), pp. 58-59

50 European Union Agency for Cybersecurity (n 14), pp. 58-59

Preventing hackers with malicious intent from abusing Safe Harbour

4.1. Understanding how Safe Harbour clause can supercede the CMA

In Chapter 2 of the dissertation, we briefly explored how the CPS guidelines on prosecuting the CMA [1] does not account for 'higher social purposes' when considering the intent of a CVD reporter. Intent is a core concept in law and can be traced back to the twelfth century [2]. The latin expression *non facit reum nisi mens sit rea*, which can be interpreted to mean that an offence must be predicated on 'wrongful intent' [3], provides an ethical basis to argue that the intention of the subject should be taken into consideration when determining Safe Harbour eligibility.

We can allow for this 'higher social purpose' through the implementation of a Safe Harbour clause which authorizes CVD reporters [4] to enumerate vulnerabilities under a 'limited liability waiver' [5], rendering it authorized access and hence legal under Section 1 of the CMA [6]. Critics may argue that such an approach may work for the issue of copyright infringement during security research and organization can promise not to undertake civil action, but private law cannot possibly take precedence over public law. A private organization cannot possibly grant a 'license to kill' [7], or a license to hack in this case. In Burrows v Rhodes, it was concluded that 'an express promise of indemnity ... for the commission of [an illegal] act is void' [8], with the reasoning stated to be based on 'grounds of public policy' [9]. However, a closer inspection reveals that the proposed license to hack is limited in scope to the property owned by that organization and property rights would be encroached if we do not allow for the organization to exercise free will over their property [10]. Homeowners who have misplaced their keys can authorize a locksmith to break into their own homes [11]. In the digital realm, organizations authorize security consultants to conduct security assessments against their products [12]. This is no public policy concerns with permitting either of these activities. Hence, such an approach is arguably sound and avoids the thorny issue of CVD reporters being unwittingly prosecuted due to lack of prosecu-

1 The Crown Prosecution Service (n 2)

2 Eugene Chesney, 'Concept of Mens Rea in the Criminal Law' (1939) 29(5) Journal of Criminal Law and Criminology <https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=2828&context=jclc>, pp. 630

3 Chesney (n 2), pp. 627

4 Vostoupal and others (n 1), pp. 13

5 European Union Agency for Cybersecurity (n 14), pp. 64

6 Computer Misuse Act 1990, sect. 1

7 Michael L Nash, 'A killer contract' (2006) 156(7212) New Law Journal <https://plus.lexis.com/api/permalink/24e91ede-5218-4ef7-92fb-b0b42174bf21/?context=1001073>, pp. 3

8 *Burrows v Rhodes and Another* [1899] All ER 117, pp. 124

9 *Burrows v Rhodes and Another* (n 8), pp. 125

10 Katrina M Wyman, 'The New Essentialism in Property' (2017) 9(2) Journal of Legal Analysis <https://plus.lexis.com/api/permalink/db676c55-6195-403e-bd83-913f2838ab68/?context=1001073>, pp. 188

11 DSB Locksmith, 'How Do Locksmiths Know it's Your House?' <https://dsblocksmith.co.uk/how-do-locksmiths-know-its-your-house/> accessed 11 July 2025

12 reg 2019/881 (n 27), art. 52(7)

13 Centre for European Policy Studies (n 19), pp. 45

torial discretion in certain jurisdictions such as France [13]. However, it is also poignant to note that by doing so, the organization has waived the protection accorded by the CMA, and will thus have to draft a watertight clause to minimize risks to itself.

4.2. Recommendation 1: Registration and acceptance of terms

One method of risk minimization is to require CVD reporters register and accept the terms of the program before embarking on any vulnerability enumeration, thus ensuring that CVD reporters are fully aware of the scope and denying the defence that important details were not disclosed at the material time. In Thornton v Shoe Lane Parking, the court stated that since the terms were printed on a ticket and available only after accepting the offer, they could not form part of the contract [14]. Most bug bounty platforms require CVD reporters to create an account and accept the terms before they can submit a vulnerability report [15]. However, some organizations accept submissions over email [16] [17], creating a situation where it is unclear if the CVD reporter has read and agreed to the policy or if he obtained the email address via other means such as word of mouth. Registration is also important since it represents the acceptance of a bilateral contract where both parties are identified instead of a unilateral contract open to anyone [18] [19]. Case law dictates that revocation of a unilateral contract cannot occur after performance has begun [20]. If an organization wanted to modify the terms of the CVD program, it would be near to impossible to track down everyone who had viewed the CVD policy webpage. However, if registration is in place, it would be trivial to send them an email informing them of the change of terms.

It is poignant to note here that Article 12(1) of NIS2 requires that coordinators allow persons to report vulnerabilities to them anonymously should they choose to [21]. While this may *prima facie* seem to contradict the recommendation, scholars have explained that anonymity is requested because some CVD reporters fear prosecution due to the lack of proper Safe Harbour clauses [22]. This creates a Catch-22 situation where CVD reporters must register to contractually bind organizations to providing Safe Harbour but yet are reluctant to do so in fear that organizations may turn their backs and take legal actions against their now revealed identity. Nonetheless, this is not an impasse. CVD reporters comfortable with the Safe Harbour provided can choose to register and report directly to the organization, benefiting from recognition and possible reward, while the more cautious can still choose to preserve their anonymity and report through the coordinator [23].

14 *Thornton v Shoe Lane Parking Ltd* (1971) 2 QB 163, pp. 169

15 Bugcrowd, 'Reporting a Bug' <https://docs.bugcrowd.com/researchers/reporting-managing-submissions/reporting-a-bug/> accessed 7 June 2025

16 Jisc Services Limited, 'Vulnerability disclosure policy' <https://www.jisc.ac.uk/about-us/vulnerability-disclosure-policy> accessed 7 June 2025

17 Thirona, 'Coordinated Vulnerability Disclosure Policy' <https://thirona.eu/coordinated-vulnerability-disclosure-policy/> accessed 7 June 2025

18 Cristina Del-Real and María José Rodriguez Mesa and, 'From black to white: the regulation of ethical hacking in Spain' (2023) 32(2) Information & Communications Technology Law 207 <https://doi.org/10.1080/13600834.2022.2132595>, pp.212

19 'Encouraging vulnerability treatment: Overview for policy makers' (n 2), pp. 26

20 *Errington v Errington & Woods* (1952) 1 KB 290, pp. 295

21 Dir 2022/2555 (n 33), art. 12(1)

22 Vostoupal and others (n 1), pp. 9

23 European Union Agency for Cybersecurity (n 14), pp. 58-59

4.3. Recommendation 2: Restricting participation based on age and track record

CVD reporters run the gamut from youths interested in a future in cybersecurity to laypersons like Schröder who happened to chance upon a vulnerability [24]. When inexperience encounters a field demanding specialized knowledge, the doctrine of oblique intent becomes increasingly relevant. Oblique intent is concerned with situations where the subject may not have 'acted with purpose' but performed an action with highly foreseeable results [25]. To illustrate, a person dropping a heavy object off a balcony onto a busy sidewalk may have done it out of mischief, but it is highly foreseeable that such conduct will cause serious injury, thus leaving him liable. However, in a specialized field like cybersecurity, it may not be immediately apparent to a layperson if running a command that was copied off the Internet could cause data loss or catastrophic damage. In DPP v Lennon, a case that occurred outside the bounds of a CVD program, a 16-year-old youth downloaded a 'mail-bombing program' off the Internet with the intention of 'causing a bit of a mess up' but ended up completely overwhelming the email servers of his former employer, resulting in £18,000 of damage [26] [27]. Criminalizing mischief or recklessness can be contentious with various jurisdictions in favour and others not much so [28]. From an organization's stance, avoiding the issue altogether by restricting CVD participation may be least risky.

Excluding minors from participating can be effective in reducing the probability of encountering such acts of mischief. In the Netherlands, it was observed that most computer misuse cases in court involved youths under 23 and even warranted the creation of an awareness program to help these youths understand 'their rights and duties' [29]. While some independent CVD programs do not stipulate a minimum age for participation [30], bug bounty platforms do require that participants 'have reached the age of majority' to be eligible for monetary compensation [31], indirectly reducing incidents of mischief on their platforms. A more inclusive approach is to restrict participation based on track record. Bug bounty platforms achieve this by keeping track of each CVD reporter's submissions and allowing organizations to invite only those who have met a certain criterion to their private programs [32]. Studies have shown that private programs achieve a 'higher percentage of valid reports', with an average of 52% compared to 20% for public programs since 2015 [33]. To replicate this, organizations running an independent program can probably limit the scope of their public CVD program to low-risk assets and invite those who have proven themselves to join a separate private CVD program.

---

24 van't Hof (n 6), pp. 78-79

25 Shlomit Wallerstein, 'Oblique Intent in English and Jewish Law' (2014) 3(2) Oxford Journal of Law and Religion 258 <https://plus.lexis.com/api/document?collection=analytical-materials-uk&id=urn:contentItem:5CDV-CMH1-F0NG-61KY-00000-00&context=1001073>, pp. 258

26 Stefan Fafinski, *Computer Misuse: Response, Regulation and the Law* (1st, 2009), pp. 61-62

27 *DPP v Lennon* [2005] Wimbledon Magistrates Court, unreported

28 John Child (ed), *Reforming the Computer Misuse Act 1990: CLRNN1 Report* (Criminal Law Reform Now Network 2020), para. 3.45

29 European Union Agency for Cybersecurity (n 14), pp. 52

30 Jisc Services Limited (n 16)

31 Bugcrowd, 'Standard Disclosure Terms' <https://www.bugcrowd.com/resources/hacker-resources/standard-disclosure-terms/> accessed 7 June 2025

32 Bugcrowd, 'Viewing and Accepting Invitations' <https://docs.bugcrowd.com/researchers/invites/viewing-and-accepting-engagement-invitations/> accessed 7 June 2025

33 Zhao, Laszka, and Grossklags (n 6), pp. 5

4.4. Recommendation 3: Clear delineation of permissible actions

As explained in the previous section, the participation of youths and laypersons in CVD programs may entail risks due to lack of maturity or experience. However, experience can also be dangerous in the wrong hands. Hackers may pose risks as they can use their wealth of experience to argue that the organization has implemented the technology in an illogical or unconventional fashion. Hence, they should not be liable for their alleged benign actions. They may even argue that any damages should be attributed to poor practices from the organization. In R v Cuthbert, the defendant, who was a cybersecurity professional in his day job, executed an unauthorized 'directory traversal' on a charity website [34] [35]. Cuthbert attempted to justify his actions by claiming the website had 'slow response' and 'poor graphics', leading him to suspect that it was a phishing website [36]. Cybersecurity professionals were divided, with some 'alarm[ed]' that the act of directory traversal would be considered unauthorized access while others pointed out that directory traversal was not an effective test to detect a phishing website [37], and thus the *actus reus* was not aligned to his claimed *mens rea*.

Clear delineation of permissible actions under the CVD program is of paramount importance to avoid such situations where it is uncertain whether the CVD reporter ought to have known that his actions would be permitted or prohibited. A generic CVD policy taken from a template exhorting CVD reporters not to 'take advantage of the vulnerability or problem you have discovered' [38] leaves much uncertainty. It is probable that such policies are written by the organization's legal team without input from the cybersecurity team. Without detailed domain knowledge, keeping it generic leaves room for interpretation and argument. However, doing so increases uncertainty for all parties and may not always work in favour of the organization, as evidenced in R v Walker [39] [40].

CVD policies drafted by the cybersecurity team without input from the legal team may not fare better. Without an understanding of the legal framework underpinning safe harbour [41], these polices might resemble a laundry list of prohibited actions. There is a possibility that certain clauses were omitted or misclassified because the policy was not crafted in a structured manner. For example, the data exfiltration, social engineering and physical security prohibition in JISC's CVD policy would be more appropriate under the testing instead of the reporting section [42]. Possible prohibitions under the reporting section that may have been missed include not sharing information about the vulnerability to anyone else during the disclosure process and not submitting duplicate reports in a bid to expedite the process. Interestingly, the University of York's CVD policy exhibits an identical misclassification of prohibitions [43], indicating possible referencing by either party. More concerning

34 *R v Cuthbert* [2005] Horseferry Road Magistrates Court, unreported

35 Society for Computers & Law, 'Computer Misuse Prosecutions' (1 November 1999) <https://www.scl.org/821-computer-misuse-prosecutions/> accessed 13 June 2025

36 Society for Computers & Law, 'Computer Misuse Prosecutions' (n 35)

37 Society for Computers & Law, 'Computer Misuse Prosecutions' (n 35)

38 Thirona (n 17)

39 Maurushat (n 33) pp. 43

40 *R v Walker* (n 34)

41 Ķinis (n 7), pp. 518

42 Jisc Services Limited (n 16)

43 University of York, 'Vulnerability disclosure policy' <https://www.york.ac.uk/it-services/about/policies/vulnerability-disclosure/> accessed 7 June 2025

is the fact that an important document promising safe harbour protection has probably not been vetted by the legal team, who likely would have caught the misclassified clause.

Evidently, as legislators in Latvia [44] and the UK [45] have found out, drafting a watertight safe harbour policy is a complex endeavour requiring close cooperation from both the legal and the cybersecurity team. The principle of intent discussed in this chapter is primarily legal in nature. In the next chapter, we will delve deeper into the cybersecurity domain as we attempt to determine which actions are proportional to achieving certain selected aims.

Ensuring CVD reporters do not take disproportional actions

In the previous chapter, we have determined the various scenarios in which *mens rea* qualifies for safe harbour protection. However, *mens rea* must align with the *actus reus*. Due to the varied types of possible actions, we shall look towards the CMA to help with classifying them.

Section 1 of the CMA prohibits unauthorized access [1]. Unauthorized access is usually surgical in nature. To illustrate, a journalist found exposed Social Security Numbers (SSNs) on a state website [2]. An individual just had to visit one specific page and hit F12 to view the source code, revealing the SSNs [3]. Recommendation 4 will focus on incidents like these and evaluate if the actions taken to demonstrate proof of privileged access are proportionate.

Section 3 of the CMA is broader in scope compared to Section 1 and prohibits acts which 'impair the operation' and acts which 'prevent or hinder access' to a service [4]. Finding that surgical strike may entail considerable scanning which exceeds acceptable usage limits. Continuing from our previous example, finding the page with exposed SSNs requires either chancing upon it or scanning thousands of irrelevant pages for possible sensitive data. This scanning traffic has the potential to overwhelm the service and deny other legitimate visitors access unless appropriate limits are put in place, which we will examine in recommendation 5.

Lastly, unlike intention, actions leave traces and affect the service targeted by the CVD reporter. In recommendation 6, we will explore the opportunity to introduce traceability and evidentiary requirements to reduce disputes where the organization's account of the actions taken differs from the CVD reporter's claim.

5.1. Recommendation 4: Demonstrating proof of privileged access

In R v Mangham, the defendant gained access to Facebook's servers and made copies of a selection of emails as well as part of Facebook's source code [5]. Although he did not share the emails and source code with anyone and did not attempt to seek any financial gain from it [6], he was nonetheless found guilty. Maurushat believes that the decision to prosecute may have been due to him making a copy of the source code, which is one of the company's greatest

44 'Encouraging vulnerability treatment: Overview for policy makers' (n 2), pp. 30

45 HL Deb 28 January 2025, vol 843, col 182

1 Computer Misuse Act 1990, sect. 1

2 Carly Page, 'F12 isn't hacking: Missouri governor threatens to prosecute local journalist for finding exposed state data' (15 October 2021) <https://techcrunch.com/2021/10/15/f12-isnt-hacking-missouri-governor-threatens-to-prosecute-local-journalist-for-finding-exposed-state-data/> accessed 1 July 2025

3 Page (n 2)

4 Computer Misuse Act 1990, sect. 3

5 *Mangham v Court of Appeal Criminal Division* [2012] EWCA 973, para. 4

6 *Mangham v Court of Appeal Criminal Division* (n 5), para. 11

asset [7]. Hence, we can probably conclude that making copies of valuable data are likely to be treated as disproportional based on precedent.

In our next case, the defendant happened to overhear a login code and password while visiting his healthcare provider, Diagnostiek voor U [8] [9]. He subsequently informed an acquaintance who tried using the credentials and searched the system for his own name [10]. When the results came back empty, he searched for the names of a few other friends, found some medical records, printed them and redacted the names with a marker pen [11]. He then informed the healthcare provider over a phone call [12]. The prosecutor attempted to argue that his aim could have been achieved in a 'far less intrusive manner' [13]. Suggestions made by the prosecutor included stopping once they had logged into the system and not venturing to open or view any documents, or if they wanted to confirm that it was possible to open a file, seeking permission from the subject whose file they were attempting to open [14]. However, the judge rejected the prosecutor's argument, concluding that opening the files was necessary to prove the flaw exists and that the defendant had acted responsibly by redacting the names.

These two cases give us a good understanding on where the courts stand regarding proportionality of actions. The courts place great emphasis on accuracy of reporting and is even willing to allow personal data of a few individuals to be copied as long as they are adequately protected or anonymized by the CVD reporter. This is also contingent on the fact that the CVD reporter has tried to retrieve his own data first but is unable to find his own data in the system. This finding is important because some CVD policies currently forbid users from 'interacting with accounts' they do not own [15] [16]. This position is not aligned with the court's position and once NIS2 transposition is complete, these organizations may start receiving CVD reports with other's personal data through the coordinator.

One possible method in reducing risk is to plant fake files or accounts on the systems in scope and instruct CVD reporters to retrieve those planted values instead of actual accounts [17] [18]. This method avoids issues with General Data Protection Regulation (GDPR) and thus are low risk, albeit at the cost of complexity of planting fake data. JISC also has a novel approach where CVD reporters are asked to use the 'touch /root/uniqueid' command to create a new file in a privileged location to demonstrate privileged access. Such an approach avoids the complexity of planting files on all systems. Instead, the team only has to cleanup files created on successful exploit attempts. An alternative might be to create a fully separate 'staging environment' that is a replica of the actual website but filled with test data instead of ac-

7 Maurushat (n 33), pp. 42

8 Case 01/820892-12 *PPS v Brenno de Winter* ECLI:NL:RBOBR:2013:BZ1157

9 van't Hof (n 6), pp. 84

10 van't Hof (n 6), pp. 84

11 van't Hof (n 6), pp. 84

12 van't Hof (n 6), pp. 84

13 van't Hof (n 6), pp. 90

14 van't Hof (n 6), pp. 90

15 UK Finance Limited, 'Responsible disclosure policy' <https://www.ukfinance.org.uk/about-us/our-commitments/responsible-disclosure-policy> accessed 7 June 2025

16 Laszka and others (n 27), pp. 144

17 Laszka and others (n 27), pp. 143

18 Heather Simpson, 'Give it a go: Capture the flag for $20K USD in our bug bounty program' (4 August 2022) <https://about.gitlab.com/blog/capture-the-flag-in-our-bug-bounty-program/> accessed 1 July 2025

tual customer data [19] [20]. If the above-mentioned methods are not feasible, then CVD reporters should be instructed to access their own data where possible and only access a small number of other customer's data as a last resort. In such cases, CVD reporters should be instructed to redact and protect that information, aligning with the court's decision in the Diagnostiek voor U case. According to Belgian legislation, this action could be reconciled with the GDPR by considering the CVD reporter a data controller subcontracted by the organization to process small volumes of personal data [21].

Many CVD programs also exclude a range of vulnerabilities such as reflected cross-site scripting, cross-site request forgery, username enumeration among others due to 'low severity' [22] [23]. While it might *prima facie* seem arbitrary, evaluating them in the context of unauthorized access elucidates the fact that these vulnerabilities usually do not directly provide any privileged access when exploited. In most cases, they require additional social engineering such as sending a phishing email containing the payload to a victim who must then click the link [24] [25]. It may be prudent for organizations to group these prohibited actions together and provide an overarching rationale, so that CVD reporters can better comprehend the reasoning.

5.2. Recommendation 5: Setting limits on acceptable resource usage

Having addressed unauthorized access, we shall now turn our attention towards ensuring that CVD activity does not overwhelm computing resources. There are generally two different types of high-volume activities that can be differentiated based on their intent. The first is 'load testing', usually characterized by repeated traffic whose sole intent is to exhaust available resources, so that the CVD reporter can file a report claiming that the service is not robust and unable to withstand high traffic volumes. Although outside the bounds of a CVD program, this occurred in DPP v Lennon in which the defendant sent over 5 million emails with similar content, taking down the email service [26] [27]. These types of activities are usually excluded from the scope of the CVD program because organizations only require enough capacity to handle legitimate traffic. Engaging in a never-ending arms race to increase capacity just to be faced with an even larger volume of traffic does not contribute to improving security.

The second type of high-volume activity is characterized by varying traffic whose intent is to map out resources in an effort to discover vulnerabilities. The SSN exposure example earlier in the chapter [28] is one such activity where a different page is requested every single time and

19 Laszka and others (n 27), pp. 142

20 Grant McCracken, 'All You Need to Know About Bug Bounty Testing Environments' (12 October 2016) <https://www.bugcrowd.com/blog/all-you-need-to-know-bug-bounty-testing-environments/> accessed 7 June 2025

21 European Union Agency for Cybersecurity (n 14), pp. 66

22 Walshe and Simpson (n 24), pp. 29:10

23 Esko-Graphics BV, 'Esko CVD Rules' <https://www.esko.com/it/cvd-rules> accessed 5 July 2025

24 Open Worldwide Application Security Project, 'Cross Site Request Forgery (CSRF)' <https://owasp.org/www-community/attacks/csrf> accessed 5 July 2025

25 Open Worldwide Application Security Project, 'Cross Site Scripting (XSS)' <https://owasp.org/www-community/attacks/xss> accessed 5 July 2025

26 Fafinski (n 26), pp. 61-62

27 *DPP v Lennon* (n 27)

28 Page (n 2)

checked if it contains sensitive data. In a similar case, an Australian security expert, Webster found that the URL to his superannuation account contained his identity number and that by simply incrementing that number and reloading the page, he was able to access data belonging to other individuals [29]. Within a few minutes, the script he wrote managed to save data belonging to 500 accounts [30]. This vulnerability is known as an Insecure Direct Object Reference (IDOR) [31] and can be tricky to regulate as it depends heavily on the security researcher's experience. Webster probably knew that identity numbers were generated incrementally, and he had a good chance of guessing many valid identity numbers within mere minutes, and hence not subjecting the organization to an unreasonable volume of scanning traffic. However, a less experienced security researcher, when confronted with a completely randomly generated Universally Unique Identifier (UUID) might not recognize that fact and spend hours incrementing the value without success, consuming the organization's resource usage unnecessarily.

One method that some organizations use to tackle this issue is clear delineation in Recommendation 3. By stating that denial of service (DoS) scenarios are not accepted, and by clarifying that certain UUIDs have been securely generated and is out of bounds of the CVD program should suffice in addressing such behaviour. The former is relatively common, the CVD program of both JISC and Thirona prohibit DoS or brute force attacks [32] [33]. However, the latter is considerably rarer and perhaps only found in mature programs where much thought has been put into drafting program exclusions.

5.3. Recommendation 6: Traceability and evidentiary requirements

We have demonstrated in chapter 2 that CVD activity borders on the cusp of illegality. Furthermore, such activity does not exist in a silo but in an actual environment with legitimate users, other CVD reporters and hackers all accessing the systems and leaving traces at any given time. In such a complex environment, traceability is key to ensure that someone else's actions do not get mistakenly attributed to a CVD reporter, potentially disqualifying him from safe harbour. In the Groene Hart incident described in chapter 3, the vulnerable server was accessed on a second occasion using the same leaked password where a larger volume of data was downloaded [34]. While the defendant admitted to the first attempt and argued that it was for an ethical purpose, he denied accessing it a second time and there was 'no hard forensic evidence' linking the defendant to the second incident [35]. The prosecutor attempted to convince the court that since only hospital staff and the defendant knew the password, it can be attributed to the defendant based on 'a balance of probabilities' [36]. Nonetheless, the court ruled that there was 'insufficient evidence' linking the defendant to the second attempt [37]. Thus, it is beneficial for organizations and CVD reporters to build in traceability into the process and maintain evidence in

29 Maurushat (n 33), pp. 10

30 Maurushat (n 33), pp. 10

31 Open Worldwide Application Security Project, 'Insecure Direct Object Reference Prevention Cheat Sheet' <https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html> accessed 4 July 2025

32 Jisc Services Limited (n 16)

33 Thirona (n 17)

34 van't Hof (n 6), pp. 125

35 van't Hof (n 6), pp. 125

36 van't Hof (n 6), pp. 125

37 van't Hof (n 6), pp. 129-130

the event of a dispute.

Organizations can require CVD reporters to use a 'specific user agent or header' to differentiate their traffic for easier traceability [38] [39]. This requirement may also have the added benefit of filtering out reports from less experienced CVD reporters who may not have the knowledge to customize automated scanning tools to use these user agents or headers. Nonetheless, these additional requirements may also introduce 'additional friction' discouraging participation [40], thus organizations will have to weigh the benefits. A less intrusive approach favoured by some organizations is to require that CVD reporters provide their IP address so that the relevant logs could be analysed to view the reporter's activity [41]. While these methods work for security researchers, laypersons who have chanced upon a vulnerability will likely not have the knowledge to fulfil these requirements. Making these requirements optional but encouraged strikes a balance between allowing laypersons to submit CVD reports while ensuring that security researcher's activity is well documented and visible to the organization.

Ensuring issues are resolved timeously while respecting subsidiarity

With the intention and the act of vulnerability discovery addressed, we can now turn our attention to the disclosure and coordination process. Friction between CVD reporters and organizations boil down to differences in priorities. CVD reporters are usually eager for vulnerabilities to be patched timeously to reduce risks to the public and so they can receive recognition for their finding. However, organizations have a profit motive and hence may prioritize new product development instead of patching vulnerabilities in existing products. They may also be more inclined to keep the issue under wraps to avoid possible reputational impact. We will explore the issue of timely resolution in recommendation 7. Finally, recommendation 8 will cover disclosure mechanisms and ensuring appropriate credit is accorded to the CVD reporter.

6.1. Recommendation 7: Defined timeline and escalation process

In chapter 1, we briefly discussed how CVD gives organizations a head start in patching vulnerabilities before the public is notified. Organizations will thus need to include a reasonable timeline for resolution in their CVD policies, while keeping in constant communication with the CVD reporter to avoid any surprises [1]. Setting a reasonable timeline can be a complex endeavour. Smaller outfits may lack internal security expertise, or the vulnerability report may include complex or multiple vulnerabilities which would logically take more time to fix [2]. An overly generous timeline is also risky as hackers may independently find the same vulnerability, which occurred in the REvil ransomware attack [3] discussed in chapter 2. Thus, it is important for the organization to understand its capacity when drafting a timeline for their CVD policy and be ready to negotiate with CVD reporters if more time is needed. When Phillips needed more time to remediate the thousands of vulner-

38 Jackson (n 12), pp. 153

39 Inti, 'Understanding testing requirements' <https://kb.intigriti.com/en/articles/5412984-understanding-testing-requirements> accessed 5 July 2025

40 Jackson (n 12), pp. 153

41 Jisc Services Limited (n 16)

1 'Encouraging vulnerability treatment: Overview for policy makers' (n 2), pp. 39

2 Black Duck Editorial Staff, 'Responsible disclosure on a timetable' (27 February 2017) <https://www.blackduck.com/blog/responsible-disclosure-on-a-timetable.html> accessed 8 July 2025

3 Newman (n 20)

abilities reported to them, they worked with the coordinator and the security researcher to delay the public disclosure beyond the stipulated 90 days [4], culminating in a positive outcome for all involved.

However, CVD may not always be smooth sailing and communication breakdowns may occur, especially since CVD reporters usually do not have a long-standing working relationship with an organization. Thus, it is important to understand the escalation process available to CVD reporters in seeking recourse. In the Groene Hart hack previously discussed, the defendant printed out personal data 'in the presence of journalists' [5] [6]. The court ruled that involving the media so early in the process 'was entirely unnecessary' since there was no evidence that the log-in code was known to anyone else at that stage [7]. This decision is important as it implies that the court may permit CVD reporters to escalate the issue and involve the media later in the process such as when communication has broken down or if there is reason to believe that hackers already have knowledge of the same vulnerability. Thus, it is of paramount importance that organizations maintain close communication [8] and prioritize the issue especially if it is suspected that others may also know of the vulnerability.

6.2. Recommendation 8: Clear disclosure mechanism and outcome

Better late than never. While CVD reporters might be more forgiving and patient in awaiting a positive outcome, the situation may turn sour if they realize that the outcome they expect to receive is not aligned with that provided by the organization. Some CVD programs like JISC permit the CVD reporter to publicly disclose the vulnerability and claim credit after it has been fixed [9]. However, others such as DJI retain 'sole discretion' in deciding the extent of public disclosure [10]. DJI's nuanced statement today is the product of a disclosure gone wrong back in 2017, when Finisterre, a prominent security researcher, was unwilling to accept the terms of a non-disclosure agreement (NDA) [11]. The conflict resulted in threats of legal action and Finisterre eventually walked away without agreeing to the terms, forfeiting the $30K bounty, choosing instead to publicly disclose the vulnerability and his negative experience with the organization [12]. This case highlights the importance of stating the disclosure mechanism upfront so that both the organization and security researchers are aligned on the expected outcome of the CVD process [13].

Nonetheless, even when both parties have agreed on public disclosure, conflicts may still

4 Black Duck Editorial Staff (n 2)

5 *PPS v de Winter* (n 8)

6 van't Hof (n 6), pp. 91

7 van't Hof (n 6), pp. 91

8 'Encouraging vulnerability treatment: Overview for policy makers' (n 2), pp. 17

9 Jisc Services Limited (n 16)

10 DJI, 'DJI Bug Bounty Program Policy' <https://web.archive.org/web/20250701041931/https://security.dji.com/policy?lang=en_US> accessed 29 July 2025

11 Chris Bing, 'How DJI fumbled its bug bounty program and created a PR nightmare' (30 November 2017) <https://cyberscoop.com/dji-bug-bounty-drone-technology-sean-melia-kevin-finisterre/> accessed 8 July 2025

12 Kevin Finisterre, 'Why I walked away from $30,000 of DJI bounty money' (20 November 2017) <https://web.archive.org/web/20171120000359/http://www.digitalmunition.com/WhyIWalkedFrom3k.pdf> accessed 8 July 2025

13 'Encouraging vulnerability treatment: Overview for policy makers' (n 2), pp. 25

occur over the extent of disclosure. In 2015, security researchers from ERNW found vulnerabilities in FireEye's security software. After the vulnerabilities were addressed, they were unable to reach a consensus regarding the extent of disclosure [14]. FireEye claimed that the report revealed 'extensive technical details' about the inner workings of their software, while ERNW claimed that 'some level of contextual detail' is required to understand the vulnerability for the purposes of education [15]. Eventually, FireEye filed an injunction to prevent disclosure of their proprietary information in the report [16]. This case is rather uncommon as the security researchers were not acting independently but under the direction of their employer. ERNW provides cybersecurity consultancy [17], hence they would likely place much greater emphasis on public disclosure which boosts their firm's reputation and industry recognition, even at the expense of forfeiting possible bug bounty.

Other than industry partners, the field of academia is another where emphasis is skewed towards publishing and public disclosure over financial reward. In NXP v Radboud University, researchers from the university found vulnerabilities in an algorithm used by an NXP chip and planned to publish the research at a conference [18]. NXP attempted to block the publication citing copyright infringement through 'knowingly circumvent[ing] effective technical measures', violation of 'duty of care' as all organizations using the chip will be harmed by the publication, and finally violation of computer hacking laws [19]. However, the court ruled in favour of the university, concluding that the algorithm was '[never] made public or intended to be made public' and hence not eligible for copyright [20]. Furthermore, the court also stated that blocking the publication would go against the right of freedom of expression under Article 10 of the European Convention of Human Rights, restrict the dissemination of scientific information [21] and that society would benefit from the knowledge that the chips are insecure so that they can take measures to mitigate the risks [22].

These three cases illustrate that even though the main aim of CVD activity is for vulnerabilities to be disclosed and patched for the benefit of society, CVD reporters may have differing motivations and priorities. Organizations will need to be flexible in negotiating terms especially when dealing with prominent researchers, cybersecurity consultancies or academia. DJI offered Finisterre some concessions to 'try to reach a deal' [23] while FireEye 'sought a face-to-face meeting' to come to an agreement with ERNW [24]. While it did not succeed in these highly publicised cases, there is good reason to believe that many other cases may have been amicably resolved behind closed doors with the public none the wiser. Nonetheless, if organizations are adamant on having the last say, they should follow in the footsteps of DJI and craft a clause to ensure they have 'sole discretion' in deciding

14 Kim Zetter, 'A Bizarre Twist in the Debate Over Vulnerability Disclosures' (11 September 2015) <https://www.wired.com/2015/09/fireeye-enrw-injunction-bizarre-twist-in-the-debate-over-vulnerability-disclosures/> accessed 8 July 2025

15 Zetter (n 14)

16 Zetter (n 14)

17 Zetter (n 14)

18 Case 171900 *NXP BV v Radboud Universiteit Nijmegen* ECLI:NL:RBARN:2008:BD7578, pp. 1

19 *NXP BV v Radboud Universiteit Nijmegen* (n 18), para. 3.2

20 *NXP BV v Radboud Universiteit Nijmegen* (n 18), para. 4.10

21 *NXP BV v Radboud Universiteit Nijmegen* (n 18), para. 4.13

22 *NXP BV v Radboud Universiteit Nijmegen* (n 18), para. 4.17

23 Bing (n 11)

24 Zetter (n 14)

disclosure terms [25]. Lastly, it should be noted that even though NIS2 mandates the maintenance of a European vulnerability database, disclosure and registration is 'on a voluntary basis' and hence organizations are allowed to restrict the extent of disclosure [26].

Conclusion

The field of CVD is in its infancy, with many organizations not putting serious thought into drafting their CVD policies. Policies with vague and generic references to law are commonplace, creating strife among CVD reporters and discouraging CVD activity due to potential legal implications. In some cases, organizations have even backtracked on their initial promise [1]. However, with increased regulatory interest and the upcoming transposition of the NIS2 directive, CVD programs will likely catch the attention of legal teams who will have to work closely with their cybersecurity counterparts in the drafting and implementation of these programs. This is not an isolated phenomenon, the field of data privacy has 'dramatically transformed' post-GDPR from an internal cybersecurity function concerned with securing organization's data in the interests of the organization, into a compliance function that safeguards customer's data from misuse by the organization [2]. Given that both CVD and data privacy provide greater societal benefits and experience a conflict of interest when organizations prioritize profits over its customer's welfare, there is reason to believe that the field of CVD might go down a similar path.

In this dissertation, we chronologically explored various attempts to promote safe harbour in the UK and EU, starting with the Dutch NCSC and prosecution guidelines and culminating in the NIS2 directive. The legal principles of intent, proportionality and subsidiarity were observed to be a common factor used by these legislative instruments to evaluate if a CVD reporter should be eligible for safe harbour. We then utilized these legal principles and evaluated relevant cases to determine recommendations that organizations can adopt to ensure that their CVD policy is aligned with the court's position.

Organizations should consider mandating registration and acceptance of terms before embarking on CVD activity and consider restricting participation based on age or track record. Other recommendations include planting fake files or accounts for CVD reporters to demonstrate proof of privileged access and requiring the usage of specific user agents or headers for increased traceability. Organizations should also clearly delineate the scope of the program, permissible actions, disclosure timeline and mechanisms. Such clarity ensures that CVD reporters with good intentions do not accidentally overstep the boundaries and are aware and satisfied with the disclosure outcomes from the onset. Finally, organizations should also maintain close contact with CVD reporters and be willing to exercise a degree of flexibility in dealing with CVD reporters with differing motivations.

CVD brings about positive benefits to the organization and the society at large. The provision of safe harbour encourages CVD activity and hence many states have attempted to promote safe harbour through various means such as prosecutorial discretion or legislative amendments. As some countries with failed attempts have realized, providing safe harbour while minimizing risks is not an easy feat, requiring input from experts in both the legal and technology domain. This dissertation has attempted to take the first step in bridging that gap, providing recommendations that organizations can utilize to craft safe harbour policies that minimize risks and are aligned with the upcoming NIS2 transposition.

---

25 DJI (n 10)

26 Dir 2022/2555 (n 33), art. 12(2)

1 Bleeping Computer LLC (n 4)

2 GDPR Advisor, 'The Evolving Role of Data Protection Officers in the Post-GDPR Landscape' <https://www.gdpr-advisor.com/the-evolving-role-of-data-protection-officers-in-the-post-gdpr-landscape/> accessed 13 July 2025

Bibliography

Cases

Burrows v Rhodes and Another [1899] All ER 117.

Chappell v Nestle [1960] AC 87.

DPP v Lennon [2005] Wimbledon Magistrates Court, unreported.

Errington v Errington & Woods (1952) 1 KB 290.

Mangham v Court of Appeal Criminal Division [2012] EWCA 973.

R v Cuthbert [2005] Horseferry Road Magistrates Court, unreported.

R v Walker [2008] New Zealand High Court Hamilton CRI2008-0750711 1201.

Case 171900 *NXP BV v Radboud Universiteit Nijmegen* ECLI:NL:RBARN:2008:BD7578.

Case 01/820892-12 *PPS v Brenno de Winter* ECLI:NL:RBOBR:2013:BZ1157.

Thornton v Shoe Lane Parking Ltd (1971) 2 QB 163.

Legislation

Computer Misuse Act 1990.

Copyright, Designs and Patents Act 1988.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L333/80.

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (InfoSoc Directive) [2001] OJ L167/10.

Law No 2016-1321 of October 7, 2016, for a Digital Republic, France.

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.

Royal Decree implementing the law of 26 April 2024 establishing a framework for the cybersecurity of network and information systems of general interest for public security, Belgium.

The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023.

Treaties

Official Report, House of Lords.

Reports

Baker McKenzie, *2021/2022 Digital Transformation & Cloud Survey: A Wave of Change* (2021) <https://www.bakermckenzie.com/-/media/files/insight/publications/2021/12/2021-digital-transformation--cloud-survey--a-wave-of-change.pdf>.

British Standards Institute, *TC: Tracked Changes. Information technology. Security techniques. Vulnerability disclosure* (2015) <https://discovered.ed.ac.uk/permalink/44UOE_INST/1viuo5v/cdi_bsi_primary_000000000030413565>.

Centre for European Policy Studies, *Software Vulnerability Disclosure in Europe* (2018) <https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges/>.

Dutch National Cyber Security Centre, *Coordinated Vulnerability Disclosure: the Guideline* (2018) <https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline>.

European Union Agency for Cybersecurity, *Coordinated vulnerability disclosure policies in the EU* (2022) <https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu>.

National Telecommunications and Information Administration, *Vulnerability Disclosure Attitudes and Actions* (2016) <https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf>.

NIS Cooperation Group, *Guidelines on Implementing National Coordinated Vulnerability Disclosure Policies* (2023) <https://ec.europa.eu/newsroom/dae/redirection/document/99973>.

Books

J Child (ed), *Reforming the Computer Misuse Act 1990: CLRNN1 Report* (Criminal Law Reform Now Network 2020).

Fafinski S, *Computer Misuse: Response, Regulation and the Law* (1st, 2009).

Jackson J, *Corporate Cybersecurity: Identifying Risks and the Bug Bounty Program* (1st, 2022).

Maurushat A, *Disclosure of Security Vulnerabilities* (1st, 2013).

Pil YS and Lee R, *Big Data, Cloud Computing, and Data Science Engineering* (1st, Switzerland, 2023).

Rowland D, Kohl U, and Charlesworth A, *Information Technology Law* (5th, 2016).

van't Hof C, *Helpful Hackers: How the Dutch Do Responsible Disclosure* (1st, 2016).

Articles

Ahmed A, Deokar A, and Lee HCB, 'Vulnerability disclosure mechanisms: A synthesis and framework for market-based and non-market-based disclosures' (2021) 148 Decision Support Systems 113586 <https://www.sciencedirect.com/science/article/pii/S0167923621000968>.

Chesney E, 'Concept of Mens Rea in the Criminal Law' (1939) 29(5) Journal of Criminal Law and Criminology <https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=2828&context=jclc>.

Del-Real C and and MJRM, 'From black to white: the regulation of ethical hacking in Spain' (2023) 32(2) Information & Communications Technology Law 207 <https://doi.org/10.1080/13600834.2022.2132595>.

'Encouraging vulnerability treatment: Overview for policy makers' [2021] (307) IDEAS Working Paper Series from RePEc.

Godfrey J, 'Who's afraid of reverse engineering?' (2024) 1 Intellectual Property Quarterly 50.

Ķinis U, 'From Responsible Disclosure Policy (RDP) towards State Regulated Responsible Vulnerability Disclosure Procedure (hereinafter – RVDP): The Latvian approach' (2018) 34(3) Computer Law & Security Review 508 <https://www.sciencedirect.com/science/article/pii/S0267364917303606>.

Kranenbarg MW, Holt T, and van der Ham J, 'Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure' (2018) 7(1) Crime Science.

Malladi S and Subramanian H, 'Bug Bounty Programs for Cybersecurity: Practices, Issues, and Recommendations' (2020) 37(1) IEEE Software 31.

Manning L, 'Choice of Law for Commercial Contracts' (1961) 2(2) Boston College Law Review <https://bclawreview.bc.edu/articles/2967/files/63f315c09dc7c.pdf>.

Nash ML, 'A killer contract' (2006) 156(7212) New Law Journal <https://plus.lexis.com/api/permalink/24e91ede-5218-4ef7-92fb-b0b42174bf21/?context=1001073>.

Schmitz S and Schiffner S, 'Responsible Vulnerability Disclosure under the NIS 2.0 Proposal' (2021) 12(5) Journal of Intellectual Property, Information Technology and Electronic Commerce Law.

Vostoupal J and others, 'The legal aspects of cybersecurity vulnerability disclosure: To the NIS 2 and beyond' (2024) 53 Computer Law & Security Review 105988 <https://www.sciencedirect.com/science/article/pii/S0267364924000554>.

Wallerstein S, 'Oblique Intent in English and Jewish Law' (2014) 3(2) Oxford Journal of Law and Religion 258 <https://plus.lexis.com/api/document?collection=analytical-materials-uk&id=urn:contentItem:5CDV-CMH1-F0NG-61KY-00000-00&context=1001073>.

Walshe T and Simpson A, 'Towards a Greater Understanding of Coordinated Vulnerability Disclosure Policy Documents' (2023) 4(2) Digital Threats: Research and Practice 1 <https://www.sciencedirect.com/science/article/pii/S2925753523001868>.

Wyman KM, 'The New Essentialism in Property' (2017) 9(2) Journal of Legal Analysis <https://plus.lexis.com/api/permalink/db676c55-6195-403e-bd83-913f2838ab68/?context=1001073>.

Zhao M, Laszka A, and Grossklags J, 'Devising Effective Policies for Bug-Bounty Platforms and Security Vulnerability Discovery' (2017) 7 Journal of Information Policy 372.

Secondary Sources

Bing C, 'How DJI fumbled its bug bounty program and created a PR nightmare' (30 November 2017) <https://cyberscoop.com/dji-bug-bounty-drone-technology-sean-melia-kevin-finisterre/> accessed 8 July 2025.

Black Duck Editorial Staff, 'Responsible disclosure on a timetable' (27 February 2017) <https://www.blackduck.com/blog/responsible-disclosure-on-a-timetable.html> accessed 8 July 2025.

Bleeping Computer LLC, 'Engineer reports data leak to nonprofit, hears from the police' (25 March 2021) <https://www.bleepingcomputer.com/news/security/engineer-reports-data-leak-to-nonprofit-hears-from-the-police/> accessed 15 June 2025.

Bugcrowd, 'Reporting a Bug' <https://docs.bugcrowd.com/researchers/reporting-managing-submissions/reporting-a-bug/> accessed 7 June 2025.

— 'Standard Disclosure Terms' <https://www.bugcrowd.com/resources/hacker-resources/standard-disclosure-terms/> accessed 7 June 2025.

Bugcrowd, 'Viewing and Accepting Invitations' <https://docs.bugcrowd.com/researchers/invites/viewing-and-accepting-engagement-invitations/> accessed 7 June 2025.

CyberUp, 'Campaign responds to withdrawal of amendment to update Computer Misuse Act' (9 January 2025) <https://www.cyberupcampaign.com/news/campaign-responds-to-withdrawal-of-amendment-to-update-computer-misuse-act> accessed 28 June 2025.

DJI, 'DJI Bug Bounty Program Policy' <https://web.archive.org/web/20250701041931/https://security.dji.com/policy?lang=en_US> accessed 29 July 2025.

DSB Locksmith, 'How Do Locksmiths Know it's Your House?' <https://dsblocksmith.co.uk/how-do-locksmiths-know-its-your-house/> accessed 11 July 2025.

Esko-Graphics BV, 'Esko CVD Rules' <https://www.esko.com/it/cvd-rules> accessed 5 July 2025.

Finisterre K, 'Why I walked away from $30,000 of DJI bounty money' (20 November 2017) <https://web.archive.org/web/20171120000359/http://www.digitalmunition.com/WhyIWalkedFrom3k.pdf> accessed 8 July 2025.

GDPR Advisor, 'The Evolving Role of Data Protection Officers in the Post-GDPR Landscape' <https://www.gdpr-advisor.com/the-evolving-role-of-data-protection-officers-in-the-post-gdpr-landscape/> accessed 13 July 2025.

Gibbs S, 'Jeep owners urged to update their cars after hackers take remote control' (21 July 2015) <https://www.theguardian.com/technology/2015/jul/21/jeep-owners-urged-update-car-software-hackers-remote-control> accessed 28 June 2025.

Groves P, 'The copyright owner's rights (1)' <https://sites.google.com/site/ipsojurepages/copyright/the-copyright-owner-s-rights-1> accessed 15 June 2025.

hackerone, 'Code of Conduct' <https://www.hackerone.com/policies/code-of-conduct> accessed 6 June 2025.

Inti, 'Understanding testing requirements' <https://kb.intigriti.com/en/articles/5412984-understanding-testing-requirements> accessed 5 July 2025.

Jisc Services Limited, 'Vulnerability disclosure policy' <https://www.jisc.ac.uk/about-us/vulnerability-disclosure-policy> accessed 7 June 2025.

McCracken G, 'All You Need to Know About Bug Bounty Testing Environments' (12 October 2016) <https://www.bugcrowd.com/blog/all-you-need-to-know-bug-bounty-testing-environments/> accessed 7 June 2025.

Newman L, 'The Unfixed Flaw at the Heart of REvil's Ransomware Spree' (8 June 2021) <https://www.wired.com/story/revil-ransomware-kaseya-flaw-fix-disclosure-april/> accessed 8 July 2025.

Open Worldwide Application Security Project, 'Cross Site Request Forgery (CSRF)' <https://owasp.org/www-community/attacks/csrf> accessed 5 July 2025.

— 'Cross Site Scripting (XSS)' <https://owasp.org/www-community/attacks/xss> accessed 5 July 2025.

— 'Insecure Direct Object Reference Prevention Cheat Sheet' <https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html> accessed 4 July 2025.

Page C, 'F12 isn't hacking: Missouri governor threatens to prosecute local journalist for finding exposed state data' (15 October 2021) <https://techcrunch.com/2021/10/15/f12-isnt-hacking-missouri-governor-threatens-to-prosecute-local-journalist-for-finding-exposed-state-data/> accessed 1 July 2025.

Scroxton A, 'Lords move to protect cyber researchers from prosecution' (20 June 2022) <https://www.computerweekly.com/news/252521716/Lords-move-to-protect-cyber-researchers-from-prosecution> accessed 28 June 2025.

Simpson H, 'Give it a go: Capture the flag for $20K USD in our bug bounty program' (4 August 2022) <https://about.gitlab.com/blog/capture-the-flag-in-our-bug-bounty-program/> accessed 1 July 2025.

Society for Computers & Law, 'Computer Misuse Prosecutions' (1 November 1999) <https://www.scl.org/821-computer-misuse-prosecutions/> accessed 13 June 2025.

— 'Cybercrime and the UK' (30 June 2005) <https://www.scl.org/766-cybercrime-and-the-uk/> accessed 2 August 2025.

Somers C and Vranckaert K, 'Ethical hacking under the Belgian NIS2-law: still a safe haven?' (29 April 2025) <https://www.law.kuleuven.be/citip/blog/ethical-hacking-under-the-belgian-nis2-law-still-a-safe-haven/> accessed 21 May 2025.

The Crown Prosecution Service, 'Computer Misuse Act' (3 August 2023) <https://www.cps.gov.uk/legal-guidance/computer-misuse-act> accessed 1 June 2025.

Thirona, 'Coordinated Vulnerability Disclosure Policy' <https://thirona.eu/coordinated-vulnerability-disclosure-policy/> accessed 7 June 2025.

USCopyright Office, Library of Congress, 'Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies' (28 October 2015) <https://cdn.loc.gov/copyright/1201/2015/fedreg-publicinspectionFR.pdf> accessed 15 June 2025.

UK Finance Limited, 'Responsible disclosure policy' <https://www.ukfinance.org.uk/about-us/our-commitments/responsible-disclosure-policy> accessed 7 June 2025.

University of York, 'Vulnerability disclosure policy' <https://www.york.ac.uk/it-services/about/policies/vulnerability-disclosure/> accessed 7 June 2025.

Zetter K, 'A Bizarre Twist in the Debate Over Vulnerability Disclosures' (11 September 2015) <https://www.wired.com/2015/09/fireeye-enrw-injunction-bizarre-twist-in-the-debate-over-vulnerability-disclosures/> accessed 8 July 2025.

Other works

Laszka A and others, 'The Rules of Engagement for Bug Bounty Programs' (Springer-Verlag 2018) <https://doi.org/10.1007/978-3-662-58387-6_8>.

Radianti J, Rich E, and Gonzalez JJ, 'Vulnerability Black Markets: Empirical Evidence and Scenario Simulation' (HICSS '09, Institute of Electrical and Electronics Engineers 2009) <https://doi.org/10.1109/HICSS.2009.504>.

Zhao M, Grossklags J, and Liu P, 'An Empirical Study of Web Vulnerability Discovery Ecosystems' (CCS '15, Association for Computing Machinery 2015) <https://doi.org/10.1145/2810103.2813704>.