

MATTIS VAN 'T SCHIP

THE INTERDEPENDENCE OF THINGS

Digital product interdependencies and
European cybersecurity law



Institute for Computing
and Information Sciences

**RADBOD
UNIVERSITY
PRESS**

The Interdependence of Things

Digital product interdependencies and European cybersecurity law

Proefschrift ter verkrijging van de graad van doctor
aan de Radboud Universiteit Nijmegen
op gezag van de rector magnificus prof. dr. J.M. Sanders,
volgens besluit van het college voor promoties
in het openbaar te verdedigen op

woensdag 16 september 2026
om 12:30 uur precies

door
Mattis van 't Schip
geboren op 15 januari 1997
te Leiden

Promotoren:

prof. dr. B.P.F. Jacobs

prof. mr. F.J. Zuiderveen Borgesius

prof. mr. P.T.J. Wolters

Manuscriptcommissie:

prof. dr. mr. A.U. Janssen

prof. dr E. Kosta (Tilburg University)

prof. dr. G.P. Mifsud Bonnici (Rijksuniversiteit Groningen)

dr. L.D. Urquhart (The University of Edinburgh, Verenigd Koninkrijk)

dr. mr. O.L. van Daalen (Universiteit van Amsterdam)

The Interdependence of Things

Digital product interdependencies and European cybersecurity law

Dissertation to obtain the degree of doctor
from Radboud University Nijmegen
on the authority of Rector Magnificus prof. dr. J.M. Sanders,
according to the decision of the Doctorate Board
to be defended in public on

Wednesday, September 16, 2026
at 12.30 pm

by

Mattis van 't Schip
born on January 15, 1997
in Leiden (the Netherlands)

Supervisors:

prof. dr. B.P.F. Jacobs

prof. dr. F.J. Zuiderveen Borgesius

prof. dr. P.T.J. Wolters

Manuscript Committee:

prof. dr. A.U. Janssen

prof. dr E. Kosta (Tilburg University)

prof. dr. G.P. Mifsud Bonnici (University of Groningen)

dr. L.D. Urquhart (The University of Edinburgh, United Kingdom)

dr. O.L. van Daalen (University of Amsterdam)

Table of Contents

List of Tables	v
----------------	---

List of Figures	vii
-----------------	-----

1	Introduction	1
1	The entangled digital product	1
2	The aims and motivation of this dissertation	4
3	Digital product interdependencies	6
3.1	Digital product(ion)	6
3.2	The Internet of Things stack	8
3.3	Critical properties of digital product interdependencies	10
4	Policy approaches	13
4.1	Supply chain cybersecurity	13
4.2	Digital sovereignty	15
5	Legal framework	16
5.1	Improving cybersecurity through legal frameworks	16
5.2	European cybersecurity law: an overview	18
6	Outline and methodology	21
6.1	Outline of the chapters	21
6.2	Methodology	24
2	The Regulation of Supply Chain Cybersecurity in the NIS2 Directive in the Context of the Internet of Things	33
1	Introduction	34
2	Supply chain cybersecurity	36
2.1	The multi-tiered supply chain	37
2.2	The developing field of supply chain cybersecurity	39
3	The NIS2 supply chain cybersecurity approach	43
3.1	The scope of NIS2	43
3.2	Supply chain cybersecurity provisions	44
3.3	The novelty of supply chain cybersecurity regulation	47
4	NIS2 Cyber Supply Chain Risk Management	51
4.1	Addressing cyber resilience within cybersecurity	51
4.2	Collaborative cybersecurity investments	52
4.3	Standardisation	53
5	Supply chain cybersecurity beyond NIS2: perfecting the approach . .	53
5.1	What is supply chain cybersecurity?	53
5.2	The right responsibility in the wrong hands	55
6	Conclusion	57

3	Measuring Up to (Reasonable) Consumer Expectations: Providing an Empirical Basis for Holding IoT Manufacturers Legally Responsible	63
1	Introduction	64
2	Background and Related Work	65
2.1	Expectations of IoT security and privacy	65
2.2	Reasonable expectations in law	66
2.3	The role of other stakeholders	67
3	Method	67
3.1	Measuring consumer expectations: the ideal and the learned .	68
3.2	Survey procedure	70
3.3	Vignette design	70
3.4	Choice of vignette factors	71
3.5	Ethics	73
3.6	Participants	73
3.7	Vignette and response quality	74
3.8	Data analysis	75
4	Results	75
4.1	Expectations of manufacturers	75
4.2	The user's role	79
4.3	Personal experiences	81
5	Discussion	82
5.1	Recommendations	85
5.2	Limitations	86
6	Conclusion	86
4	The Cyber Resilience Act and Open-Source Software: A Fine Balancing Act	97
1	Introduction	98
2	Open-source software	100
2.1	The development and ideologies of open-source software . . .	101
2.2	Open-source software and cybersecurity	103
3	The Cyber Resilience Act and open-source software cybersecurity . .	105
3.1	The Cyber Resilience Act in short	105
4	Assessing the commerciality of a project	109
5	Specific provisions for open-source software within the Cyber Resilience Act	111
5.1	Open-source software stewards	111
5.2	Proprietary manufacturers using open-source software	113
6	Cybersecurity and open-source software: a problem solved?	114
7	The future of open-source software under EU law	115
8	Conclusion	116

5	The Internet of Forgotten Things: European cybersecurity regulation and the cessation of Internet of Things manufacturers	121
1	Introduction	122
2	Manufacturer cessation and its risks in the context of the Internet of Things	123
2.1	The shapes of manufacturer cessation	124
2.2	Shapes of product end-of-support	125
3	Update obligations and manufacturer cessation: exemplification of a legal problem	127
3.1	The Cyber Resilience Act	128
3.2	Sale of Goods Directive	129
4	Moving away from manufacturer longevity based on existing digital policy	130
4.1	Cyber Resilience Act	132
4.2	Digital Operational Resilience Act	132
4.3	Data Governance Act	133
4.4	Interoperability policies	134
5	Designing IoT in the face of manufacturer cessation	137
5.1	Interoperability	138
5.2	Open source code publication and development	143
5.3	Suggestions for future research	145
6	Conclusion	146
6	Regulating Smart Device Support Periods: User Expectations and the European Cyber Resilience Act	153
1	Introduction	154
2	Background and Related Work	155
2.1	EU support duration regulations	156
2.2	Consumer expectations and perspectives of IoT security and product lifespans	157
3	Method	158
3.1	Survey Design	158
3.2	Recruitment and participants	160
3.3	Survey procedure	161
3.4	Data analysis	163
4	Results	164
4.1	Individual use of smart devices	164
4.2	Lifetime expectations of smart devices	167
4.3	Perceptions of software updates and security over devices' lifetime	169
5	Discussion	172
5.1	Device lifetimes	173
5.2	Software Updates and Security over devices' lifespan	173
5.3	Recommendations	174
5.4	Limitations	175
6	Conclusion	176

7	The Vulnerability of Consumers under the Cyber Resilience Act	185
1	Introduction	186
2	Human vulnerability under interdisciplinary scholarship	187
3	Human vulnerability under recent EU law	189
3.1	The Unfair Commercial Practices Directive	190
3.2	General Data Protection Regulation	192
3.3	AI Act	193
3.4	The legal landscape for human vulnerability	195
4	Vulnerable consumers under the Cyber Resilience Act	195
4.1	The basis of the Cyber Resilience Act	196
4.2	Universal vulnerability under the Cyber Resilience Act	197
4.3	Layered vulnerability under the Cyber Resilience Act	199
5	The Cyber Resilience Act as a platform for mitigating vulnerability .	200
6	Conclusion	201
8	Conclusion	205
1	Interdependence	205
1.1	Heterogeneity	206
1.2	Cybersecurity risks	207
2	The limits of European cybersecurity law in the context of interdependencies	208
3	Answering the research question	211
4	Outlook for the future	214
4.1	Limitations	214
4.2	The future is interdisciplinary	215
A	Appendix	219
	References	231
	Literature	231
	Legislation	252
	Case law	255
	Acknowledgements	257
	Summary	259
	Samenvatting	261
	Curriculum Vitae	265

List of Tables

Tables of Chapter 1

<i>Table 1</i>	Author contribution table	21
----------------	-------------------------------------	----

Tables of Chapter 2

<i>Table 1</i>	The lack of supply chain cybersecurity provisions in current EU cybersecurity legislation	50
----------------	---	----

Tables of Chapter 3

<i>Table 1</i>	Overview of vignette factors and levels.	69
<i>Table 2</i>	Distribution of age and region in the sample	74

Tables of Chapter 4

<i>Table 1</i>	The scope of the Cyber Resilience Act for open-source software	110
----------------	--	-----

Tables of Chapter 5

<i>Table 1</i>	Dimensions of interoperability	141
----------------	--	-----

Tables of Chapter 6

<i>Table 1</i>	Selection of devices in vignettes	160
<i>Table 2</i>	Demographic overview	161
<i>Table 3</i>	Prevalence and brands of smart device categories owned and used by respondents	165

Tables of Appendix

<i>Table 1</i>	Regression models for Chapter 3	220
<i>Table 2</i>	Regression models for Chapter 6	227
<i>Table 3</i>	Factors taken into account by respondents when estimating devices' lifetimes	228
<i>Table 4</i>	Final codebook analysis of open text responses	230

List of Figures

Figures of Chapter 1

<i>Figure 1</i>	The iceberg of digital products	11
-----------------	---	----

Figures of Chapter 2

<i>Figure 1</i>	Multi-tier supply chain	38
<i>Figure 2</i>	NIS2: general scope for supply chain cybersecurity provisions	45
<i>Figure 3</i>	The supply chain cybersecurity process in the NIS2 Directive	47
<i>Figure 4</i>	NIS2: allocation of responsibilities	56

Figures of Chapter 3

<i>Figure 1</i>	Ratings of likelihood and appropriateness of manufacturer responses to security events	76
<i>Figure 2</i>	Ratings of likelihood and appropriateness of manufacturer responses to privacy events	77
<i>Figure 3</i>	Ratings of user response suitability across security and privacy events and previous manufacturer responses	79

Figures of Chapter 5

<i>Figure 1</i>	Addressing IoT manufacturer cessation under current EU digital policies	131
-----------------	---	-----

Figures of Chapter 6

<i>Figure 1</i>	Sum of past use and intended future use duration across respondents' smart devices	164
<i>Figure 2</i>	Duration of device usage before stopped being used	166
<i>Figure 3</i>	Expected lifetimes for different smart and conventional device categories	167
<i>Figure 4</i>	Changes to smart devices after software support ends as expected by respondents	170
<i>Figure 5</i>	Respondents' own experiences with changes to their devices after the end of update support	171
<i>Figure 6</i>	Responses to the question: "Does the particular device you are currently using still receive software updates, as far as you know?"	172

Figures of Appendix

<i>Figure 1</i>	Respondents' concerns relating to security and privacy risks with their smart devices	221
<i>Figure 2</i>	Respondents' mitigation behaviors relating to their security and privacy concerns with their smart devices	221

1.

Introduction

"Comme notre imagination n'est puissamment frappée que de ce qui est grand, il appartient à la philosophie de la nature de s'arrêter à ce qui est petit."

Alexander von Humboldt, 'Personal narrative of travels to the equinoctial regions of the New Continent during the years 1799-1804'

1 The entangled digital product

In 2024, a software developer discovered that a piece of software on his computer was demanding more computing power than before—significantly more. Out of curiosity, he started investigating and coincidentally uncovered a cyberattack that had been in the making for three years. Inside a software package called XZ Utils, an attacker had implemented a virtual backdoor which would allow remote access to the hundreds of millions of computers that depend on XZ Utils.¹ Luckily, the investigating software developer used an early test version—which was not released to the general public yet—and quickly reported the vulnerability to the maintainers of XZ Utils. A disastrous cyberattack was prevented by a mix of sheer coincidence and technical skill.

In the months after, researchers discovered that the attacker implemented the backdoor after voluntarily working on the XZ Utils package for more than three years. The source code of XZ Utils is publicly available ('open source'), meaning that anyone can contribute to the code if they want to. On a first contribution, the code is usually checked by more senior contributors. To circumvent such verification, the attacker contributed to the code for three years, gaining a level of trust that allowed them to secretly implement the backdoor—and gain access to virtually every computer and server on the internet.²

Certainly, the average consumer will never hear about XZ Utils. But if they use a computer with Windows or Linux, it is very likely that XZ Utils is present on their system—hidden behind countless different pieces of software which depend on countless other pieces of software. In essence, the XZ Utils case is like having an

1 Kevin Roose, 'Did One Guy Just Stop a Huge Cyberattack?' The New York Times (3 April 2024) <<https://www.nytimes.com/2024/04/03/technology/prevent-cyberattack-linux.html>> accessed 13 October 2025.

2 Bruce Schneier, 'Backdoor in XZ Utils That Almost Happened' (Schneier on Security, 11 April 2024) <<https://www.schneier.com/blog/archives/2024/04/backdoor-in-xz-utils-that-almost-happened.html>> accessed 2 November 2025.

infection; where XZ Utils caused an increase in power consumption, an infection may raise your body temperature. And where XZ Utils was hidden beneath the surface of countless software packages, an infection is caused by a few harmful bacteria among the trillions in our bodies.

The XZ Utils attack never materialised at scale, but highlights an invisible world behind everyday digital products—a world going beyond software. Recently, a similar large attack occurred at the hardware level: the Israeli military remotely set off explosive charges that they had implemented in beepers used by Hezbollah.³ The Hezbollah members had bought the beepers years prior and, naturally, were unable to vet every entity involved in the production process of the beepers. Somewhere along this process, Israeli intelligence services had set up a shell company which covertly integrated the explosive charges; for the rest, the beepers remained fully functional.⁴ The explosions demonstrated that, even for hardware components that are physically present, the end user has virtually no control or knowledge over the countless components included in their end product.

These interdependencies entail risks both for software and hardware components. This is especially problematic for modern Internet of Things (IoT) devices, which combine hardware and software components from long production chains. Traditionally, a vacuum cleaner was a mere piece of hardware, already a culmination of various components, such as the brush and the power buttons. IoT devices integrate an additional layer: software. The ‘smart’ vacuum is not just a piece of hardware—it is an interactive product that exchanges, generates, and analyses data. All of these functionalities introduce respective software components to the product. The consumer can only trust that the manufacturer securely assembles a set of secure components.

Unfortunately, frequent cybersecurity incidents are giving consumers sufficient reason to distrust the security of IoT devices. In 2017, the German government told parents who had bought a ‘My Friend Cayla’ doll to dispose of it immediately.⁵ In the months prior, hackers discovered that Cayla was an ideal tool for eavesdropping on domestic conversations. The Cayla doll contained a microphone and speaker, so that children could speak to Cayla, who then, after data processing on its manufacturer’s servers, could respond. Hackers discovered that the data stream between the doll and the manufacturer was vulnerable, meaning that they could retrieve what the child—or anyone else in the room—said.

3 Sheera Frenkel, Ronen Bergman and Hwaida Saad, ‘How Israel Built a Modern-Day Trojan Horse: Exploding Pagers’ *The New York Times* (18 September 2024) <<https://www.nytimes.com/2024/09/18/world/middleeast/israel-exploding-pagers-hezbollah.html>> accessed 20 January 2025.

4 Raffi Berg, ‘Ex-Israeli Agents Reveal How Hezbollah Pager Attacks Were Carried Out’ (23 December 2024) <<https://www.bbc.com/news/articles/cwy3l02wxqdo>> accessed 5 February 2026.

5 ‘German Parents Told to Destroy Cayla Dolls over Hacking Fears’ *BBC News* (17 February 2017) <<https://www.bbc.com/news/world-europe-39002142>> accessed 28 October 2024.

IoT devices, like the Cayla doll, therefore compromise what was once considered a private, domestic space. Parents unknowingly built a virtual backdoor into their home when they bought the Cayla doll. Unfortunately, the Cayla manufacturer had forgotten to lock the door—and this is not an isolated incident. In fact, there are public search engines available for seeking out insecure internet-connected devices, such as security cameras.⁶ This insecurity—this breach of the private space—is particular to IoT products. Conventional counterparts, such as a regular doll, or a security camera without an internet connection, do not pose such cybersecurity and privacy risks. This contrast demonstrates that the expansion of a product’s interdependencies can introduce new concerns, such as cybersecurity.⁷

Digital products are now entanglements of software and hardware components. This dissertation addresses the legal obligations related to the cybersecurity risks arising out of this entanglement, which I conceptualise as ‘digital product interdependencies’. The XZ Utils, Hezbollah, and Cayla cases highlight the cybersecurity risks embedded in these interdependencies: end users are at risk of cyberattacks that compromise their personal environment, while producers risk data leaks, ransomware, or the complete halt of their production line because of cyber attacks cascading on from their suppliers.⁸

Policy makers are increasingly aware of these risks. In a recent speech, EU Commission President Von der Leyen spoke of ‘Europe’s independence moment’ for various sectors, such as technology.⁹ The need for such independence surfaced, for example, when Microsoft stopped the email services of the chief prosecutor at the International Criminal Court in the Netherlands, supposedly because of US sanctions against him for his intention to prosecute Israeli government officials for alleged war crimes in Gaza.¹⁰ In response to such risks, EU policy makers now invest in ‘digital sovereignty’, that is, to become technologically independent from foreign states and/or bad actors by stimulating the production and use of EU-based digital services.

Cybersecurity is a key pillar of the EU’s digital sovereignty strategy.¹¹ As digital sovereignty concerns emerged over the past decade, the EU equally introduced a broad

6 <<https://www.shodan.io>> last accessed 10 February 2026.

7 European Union Agency for Cybersecurity and others, Guidelines for Securing the Internet of Things – Secure Supply Chain for IoT (European Network and Information Security Agency 2020).

8 See, for instance, the impact on the Jaguar Land Rover supply chain after a cyberattack: Jasper Jolly and Dan Milmo, ‘Inside the Jaguar Land Rover Hack: Stalled Smart Factories, Outsourced Cybersecurity and Supply Chain Woes’ *The Guardian* (20 September 2025) <<https://www.theguardian.com/business/2025/sep/20/jaguar-land-rover-hack-factories-cybersecurity-jlr>> accessed 22 September 2025.

9 European Commission, ‘2025 State of the Union Address by the President’ <https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH_25_2053> accessed 10 October 2025.

10 Microsoft’s president denies such claims, see: ‘Microsoft Didn’t Cut Services to International Criminal Court, Its President Says’ *POLITICO* (4 June 2025) <<https://www.politico.eu/article/microsoft-did-not-cut-services-international-criminal-court-president-american-sanctions-trump-tech-icc-amazon-google/>> accessed 29 October 2025.

11 Rocco Bellanova, Helena Carrapico and Denis Duez, ‘Digital/Sovereignty and European Security Integration: An Introduction’ (2022) 31 *European Security* 337, 349.

array of cybersecurity legislation. The main aim of cybersecurity legislation is to bolster the cybersecurity of digital products, including IoT products. In the NIS2 Directive, for example, the EU introduces obligations for ‘supply chain security’, the cybersecurity of entities and processes involved in a production chain.¹² In a similar vein, the Cyber Resilience Act, the EU’s overarching cybersecurity law for products placed on its market, requires that security is taken into account during every step of the design, production, and after-sales processes.¹³ Furthermore, product manufacturers must perform due diligence when integrating third-party components.¹⁴ The emergence of these provisions may suggest that EU cybersecurity law already addresses risks arising out of digital product interdependencies, but much remains uncertain. It is this uncertainty that this dissertation aims to resolve.

2 The aims and motivation of this dissertation

The incessant expansion of digital product interdependencies, such as in IoT devices, is giving rise to urgent cybersecurity problems. In this dissertation, I therefore examine whether European cybersecurity law addresses these problems. I answer the following question:

To what extent does EU cybersecurity law address the cybersecurity challenges raised by the increasing interdependencies in digital products, as exemplified by Internet of Things devices? How could cybersecurity law adapt to these challenges in the future?

With the phrase ‘to what extent’, I do not mean to provide an empirical assessment of how well current European cybersecurity law addresses the various risks. Instead, this part of the research question refers to whether and how European cybersecurity law currently covers the various cybersecurity risks of digital product interdependencies. The thesis covers entities and situations that fall outside the traditional scope of this legal framework, such as open-source software providers and insolvent companies. The thesis investigates such ‘edge cases’ across European cybersecurity law, offering a thorough overview of this area of law. This analysis demonstrates potential legal uncertainties, as the edge cases may bring risks that the various cybersecurity laws do not yet fully address.

The ‘how could’ question is more normative, referring to the future: if current law does not suffice in certain areas, which regulatory revisions could ensure that EU cybersecurity law addresses these shortcomings? I describe the legal analysis in more detail in the methodology section 6.2 below.

EU cybersecurity law is a relatively nascent field. Since 2016, the European Union ramped up its legislative efforts regarding cybersecurity,¹⁵ with the incursion of the

12 Art 21(2)(d) NIS2.

13 Art 13(1) CRA.

14 Art 13(5) CRA.

15 See on the rise of cybersecurity as a policy area at the EU: AM Arnbak, ‘Securing Private Communications: Protecting Private Communications Security in EU Law: Fundamental Rights,

first NIS Directive.¹⁶ This means that academic work on the legislation introduced since 2016 has developed only over the past decade.

At the same time, digital products are becoming increasingly interdependent with the advent of technologies such as cloud computing and artificial intelligence. The cybersecurity risks that came along with this development are also relatively novel. Cloud computing may lead to unforeseen data and access breaches because of centralised data storage and connection dependencies,¹⁷ while AI providers suffer from problems like the malicious alteration of training data and broader authenticity concerns.¹⁸

Taken together, an academic gap exists both for EU cybersecurity law and for the cybersecurity risks of digital product interdependencies. While EU cybersecurity law is certainly receiving scholarly attention in general, work on digital product interdependencies remains scarce. Overall, legal scholarship on EU cybersecurity law either addresses more general questions,¹⁹ or points to regulatory adaptations required because of certain novel technologies.²⁰ Legal scholars have not yet investigated the role of European cybersecurity law for digital product interdependencies. This legal-academic gap equals a lack of scholarly attention to digital product interdependencies

Functional Value Chains and Market Incentives' (PhD thesis, Universiteit van Amsterdam 2015) ch 2; Lee A Bygrave, 'The Emergence of EU Cybersecurity Law: A Tale of Lemons, Angst, Turf, Surf and Grey Boxes' (2025) 56 Computer Law & Security Review 106071.

16 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS1 Directive).

17 See on the relation between cloud providers and cybersecurity law: Christopher Millard (ed), *Cloud Computing Law* (2nd edn, Oxford University Press 2021) ch 11.

18 Bart Jacobs, 'The Authenticity Crisis' (2024) 53 Computer Law & Security Review 105962; Henrik Nolte, Miriam Rateike and Michèle Finck, 'Robustness and Cybersecurity in the EU Artificial Intelligence Act' Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency (ACM 2025).

19 For a human rights perspective, see Pier Giorgio Chiara, 'Towards a Right to Cybersecurity in EU Law? The Challenges Ahead' (2024) 53 Computer Law & Security Review 105961; Ot Van Daalen, *From Encryption to Quantum Computing: The Governance of Information Security and Human Rights*, vol 38 (TMC Asser Press 2025). For perspectives focused more on individual legislative acts, see Sandra Schmitz-Berndt and Pier Giorgio Chiara, 'One Step Ahead: Mapping the Italian and German Cybersecurity Laws against the Proposal for a NIS2 Directive' (2022) 3 International Cybersecurity Law Review 163; Niels Vandezande, 'Cybersecurity in the EU: How the NIS2-Directive Stacks up against Its Predecessor' (2024) 52 Computer Law & Security Review 105890; Bygrave (n 15); S Nusselder, 'Scrutinising the Interplay between Data Protection and Cybersecurity: A Paradox Shrouded Behind the "State-of-the-Art"' (2025) 11 European Data Protection Law Review 145; Pratham Ajmera, 'Cybersecurity in the Internet of Things: Trends and Challenges in a Nascent Field' (2025) 59 Computer Law & Security Review 106204.

20 See, inter alia: Pier Giorgio Chiara, 'The IoT and the New EU Cybersecurity Regulatory Landscape' [2022] International Review of Law, Computers & Technology 1; Elisabetta Biasin and Erik Kamenjašević, 'Cybersecurity of Medical Devices: New Challenges Arising from the AI Act and NIS 2 Directive Proposals' (2022) 3 International Cybersecurity Law Review 163; Liane Colonna, 'The End of Open Source? Regulating Open Source under the Cyber Resilience Act and the New Product Liability Directive' (2025) 56 Computer Law & Security Review 106105.

generally.²¹ Digital products are often studied as singular, separate objects, instead of as ecosystems of interdependent components.

By studying digital product interdependencies under European cybersecurity law, this dissertation also offers societal benefits. The societal and personal risks emerging from digital product interdependencies are already evident in cases such as XZ Utils, the Hezbollah beepers, and the My Cayla doll. Hence, society at large will benefit from a regulatory framework which properly addresses these risks.

I address the central research question through six journal articles. In the following, I introduce the landscape that gave rise to the research conducted in these articles. I address the following main themes: digital product interdependencies, current policy work on supply chain cybersecurity and digital sovereignty, and EU cybersecurity law.

3 Digital product interdependencies

3.1 Digital product(ion)

Digitalisation is part of the fabric of daily life. More than 70% of people in the EU now use internet-connected devices (e.g., internet-connected TVs).²² Similarly, about 60% of EU citizens used social networks in 2023.²³ These percentages will probably increase over the coming years.

The omnipresence of digital products may seem so natural that one forgets how many aspects of daily life are now digitalised. Where a conventional doll was once an inanimate object, the My Cayla doll can reply to voice commands. Governments regularly host important press conferences on privately-owned social media platforms, while data-driven drones define the battleground in the war between Ukraine and Russia.²⁴

Across these use cases, digitalisation brings novel questions to the fore. Digitalisation—or a technological artefact—is not a neutral means to an end. The My Cayla case shows how societal and legal concerns can quickly arise out of the ‘mere’ integration of technology. Indeed, the concerns in the My Cayla Case are emblematic for digital product interdependencies.

21 Given certain exceptions, such as: Jennifer Cobbe, Chris Norval and Jatinder Singh, ‘What Lies beneath: Transparency in Online Service Supply Chains’ (2020) 5 *Journal of Cyber Policy* 65; Jennifer Cobbe, Michael Veale and Jatinder Singh, ‘Understanding Accountability in Algorithmic Supply Chains’ 2023 ACM Conference on Fairness Accountability and Transparency (ACM 2023).

22 Eurostat, ‘Internet-Connected Devices Are Widely Used in the EU’ (28 August 2025) <<https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20250828-2>> accessed 6 November 2025.

23 Eurostat, ‘59% of EU Individuals Using Social Networks in 2023’ (19 March 2024) <<https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20240319-1>> accessed 6 November 2025.

24 Yogita Limaye, ‘Fibre Optic Drones: The Terrifying New Weapon Changing the War in Ukraine’ BBC News (28 May 2025) <<https://www.bbc.com/news/articles/ckgn47e5qyno>> accessed 3 December 2025.

Digital product interdependencies are largely the result of supply chains. A supply chain includes the actors, processes, and assets that contribute to the production of a product.²⁵ Supply chains can involve hardware and/or software suppliers, but also actors that provide logistical operations, technical support, and sales. Taken together, the production of a digital product is a system of systems: the mining of natural resources (e.g., lithium for batteries), the assembly of hardware components, and the development of user applications all coalesce under one umbrella term: the supply chain. Hence, every product is the result of an almost unimaginable amount of collaborating actors and processes.

Digital product interdependencies consist of a wider palette than just those actors and processes involved in production—there are equal interdependencies embedded in the continued *functioning* of the product. Some academics visualise the dynamics of this latter process as a vertical ‘stack’ of layers, with each layer covering respective supply chains, market dynamics, and policies (e.g., for the realisation, maintenance, and continuous provision of a cloud service).²⁶ I shall illustrate an interdependent digital product using the stack visualisation in the next section (3.2).

One can imagine that the integration of all these smaller systems—which are individually already significant—poses unique challenges. In systems theory, academics speak of ‘emergence’: individual components only present risks when they are systematically combined.²⁷ The theory of emergence suggests that digital product interdependencies entail their own, unique risks, rather than merely bringing together the risks of individual components—the whole is greater than the sum of its parts.

In particular, this dissertation focuses on cybersecurity risks. Traditionally, cybersecurity concerns the protection of confidentiality, integrity, and availability.²⁸ The vulnerabilities present in software such as XZ Utils constitute precisely this type of risk: a virtual backdoor allowing remote access to hundreds of millions of computers worldwide—a significant breach of confidentiality. Cybersecurity measures also integrate societal concerns under the CIA-triad, such as awareness and employee training.²⁹ This means that cybersecurity is more than just a technical approach—it also considers the social dynamics of incidents like the My Cayla doll, such as the impact on children.

In sum, ‘digital product interdependencies’ is a term covering the components necessary both for the production and functioning of a digital product. Cybersecurity risks arise out of the entanglement of these components, as one insecure component can impact the entire interdependent ecosystem—including the end user.

25 European Union Agency for Cybersecurity and others, Guidelines for Securing the Internet of Things – Secure Supply Chain for IoT (n 7) 9.

26 Benjamin H Bratton, *The Stack: On Software and Sovereignty* (MIT Press 2015); Haroon Sheikh, ‘European Digital Sovereignty: A Layered Approach’ (2022) 1 *Digital Society* 25.

27 Cobbe, Norval and Singh (n 21).

28 Together, they are often coined as the ‘CIA triad’, see Spyridon Samonas and David Coss, ‘The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security’ (2014) 10 *Journal of Information System Security* 21.

29 Michael Veale and Ian Brown, ‘Cybersecurity’ (2020) 9 *Internet Policy Review* 14.

3.2 The Internet of Things stack

Thus far, I have offered quite an abstract description of digital product interdependencies, especially as no digital product—including its interdependencies—is the same. Here, I aim to ground this abstract definition of digital product interdependencies in a practical example: the stack of a smart vacuum.

In most of this dissertation, I primarily focus on Internet of Things (IoT) devices. This dissertation is part of the INTERSCT research project, which concerns the cybersecurity of the IoT in a broad sense.³⁰ In contrast to most digital products (e.g., a website), the IoT *combines* hardware and software. This leads to more interdependencies. Simply put, more interdependencies equals a larger attack surface—and thus more cybersecurity risks. The IoT therefore exemplifies the cybersecurity risks embedded in digital product interdependencies. Before coming to the smart vacuum stack, I will briefly describe the IoT.

A single definition for the IoT does not exist.³¹ Many terms exist for similar or equal concepts, such as ubiquitous computing, ‘smart devices’ (e.g., smart watch), or the Internet of Everything. This ambiguity is partially caused by the fact that IoT devices differ significantly. A smart car—a vehicle full of sensors and cameras—, a plant sensor that tracks humidity, and manufacturing machinery with sensors recording maintenance needs are all part of the IoT. This variety means that the IoT is an umbrella term covering a comprehensive cluster of devices.

In terms of functioning, IoT devices are often quite similar. They are hardware objects with the purpose of recording, transmitting, and/or exchanging data.³² Often, such data exchange happens with other similar devices, so that a motion sensor can signal the lights to turn on when you enter a room.

Within this diverse landscape, this dissertation largely focuses on smart devices bought by consumers, for instance for domestic usage. Common examples of such ‘smart home’ devices are security cameras, smart doorbells, and smart vacuums. Other prevalent IoT sectors, such as health or energy, are generally out of scope.³³

Since smart devices often share core functionalities—recording, transmitting, and/or exchanging data—they equally share their core components. For instance, data exchange requires some type of network architecture (e.g., WiFi), while data recording requires certain sensors for ‘perception’ (e.g., light sensors).

Academics schematise these various components, including their supply chains, related policies, and market dynamics, as a vertical ‘stack’ of layers. The concept of a

30 <<https://intersct.nl/>> last accessed 10 February 2026.

31 Nikolaos Goumagias and others, ‘Making Sense of the Internet of Things: A Critical Review of Internet of Things Definitions between 2005 and 2019’ (2021) 31 *Internet Research* 1583.

32 See also the definition of a ‘connected product’ under the EU Data Act, Article 2(5): ‘[...] an item that obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access’.

33 Some legislation, such as the NIS2 Directive, addresses these sectors directly. Hence, in my analysis of that legislation, I do occasionally refer to health or energy-related IoT devices.

‘technology stack’ is rather common. For example, computer scientists refer to the ‘OSI model’, which organises various components of network communication as a stack of layers.

In 2015, Bratton extended the notion of the stack towards non-technical areas in the context of political geography.³⁴ In Bratton’s sense, the stack of computation concerns a broader palette of layers, including more abstract concepts such as the city and humans. Whereas Bratton focused on computation broadly,³⁵ Sheikh conceptualised a stack primarily for digital products, consisting of seven layers (from bottom to top): resources; chips; networks; the cloud; intelligence; applications; and connected devices.³⁶ Each layer brings various actors and infrastructures to the fore. I will illustrate how those layers manifest interdependencies—both in terms of production and functioning of the product—as exemplified by the smart vacuum.

The smart vacuum combines the purpose of a traditional vacuum—cleaning floors—with autonomous navigation, so that it can freely navigate through the house while simultaneously cleaning the floor.

To perform this core function, the vacuum contains a variety of sensors, each capable of detecting movement, obstacles, and surroundings. Commonly, smart vacuums rely on light detection (Lidar), which requires laser components.³⁷ Using these sensors, the vacuum can navigate through the house and create an interactive room layout. In addition, the vacuum operates on energy from a battery, which requires regular charging. While Sheikh’s taxonomy does not directly point to these hardware components, he does mention that each digital product requires natural resources—such as lithium for batteries—within the ‘resource layer’.³⁸ The extraction of natural resources involves various organisations, such as mining companies.

The smart vacuum records environment data and shares such data with its manufacturer and/or with the end user, for instance in a mobile application. Data transmission happens in the ‘network layer’. Often, IoT devices use the internet (e.g., WiFi networks) for data sharing. However, other options exist for more local connections, such as Bluetooth, Zigbee, and Z-Wave.³⁹ These communication protocols depend on network infrastructure, such as undersea cables for data transmission and 5G infrastructure for wireless communication. Consequently, the smart vacuum depends on a range of communication technologies—ultimately extending to core network infrastructure.

Data sharing often happens indirectly through the ‘cloud’. Cloud providers (e.g., Amazon Web Services, Microsoft Azure) offer large-scale computing power for data analysis and storage. For instance, a smart vacuum manufacturer may store the

34 Bratton (n 26).

35 *ibid* 1.

36 Sheikh (n 26).

37 Lidar is short for ‘light detection and ranging’.

38 Sheikh (n 26) 7–8.

39 Eyhab Al-Masri and others, ‘Investigating Messaging Protocols for the Internet of Things (IoT)’ (2020) 8 IEEE Access 94880.

sensor data on the cloud and analyse that data to improve house mapping systems. The cloud's computing power originates in a data centre consisting of an enormous amount of servers.⁴⁰ As with any computer, the servers depend on their own hardware components sourced from various companies.⁴¹ Moreover, cloud servers use an array of software, such as for data analysis and authentication. And, as with the hardware, software components are a stack of layers relying on numerous other software packages. Altogether, the cloud layer adds countless interdependencies to the smart vacuum's stack.

Finally, the end user can interact with the smart vacuum. The technologies in the 'application layer' allow this interaction. The smart vacuum, for example, will have a mobile companion application in which the end user, after authentication, can view the map, add and edit rooms, and check whether the bin is full. As a result, the mobile companion application is a software package relying on third-party software for the respective functionalities. Through this integration, the application layer also adds numerous interdependencies to the smart vacuum.

This dissertation largely focuses on the risks associated with software interdependencies, but the smart vacuum naturally also contains various hardware components, including a brush, filter, and a speaker. With all these components beneath the surface, the smart vacuum itself is the tip of an intricate iceberg. Figure 1 illustrates some of the components contained in this digital product iceberg.

In sum, digital products rely on a stack of different layers, ranging from natural resources to the applications. Each layer involves a range of components. Unfortunately, this overview only scratches the surface of the smart vacuum stack—and it may already feel beyond comprehension. This is only natural: taken together, digital product interdependencies are becoming a highly complex and multi-headed monster.

3.3 Critical properties of digital product interdependencies

The cybersecurity risks of digital product interdependencies are diverse and multi-faceted. However, in general terms, they can be reduced to three central properties: first, digital product interdependencies are *complex*, because of the countless components involved; second, interdependencies are *opaque*: end users, but even collaborating entities are hardly aware of the scale of their network; third, *control* over this network—and the end product—is asymmetric and centralised in a few choke points.

The overview of the smart vacuum stack demonstrated the complexity of digital product interdependencies. There are countless entities collaborating for the production and functioning of a smart vacuum; each entity relies on its own suppliers, who respectively have their own suppliers, and so forth. Merely identifying all these entities is already a complex task.⁴²

40 Hence, cloud computing is often referred to as 'someone else's computer'.

41 Millard (n 17) ch 3.

42 Cobbe, Norval and Singh (n 21).

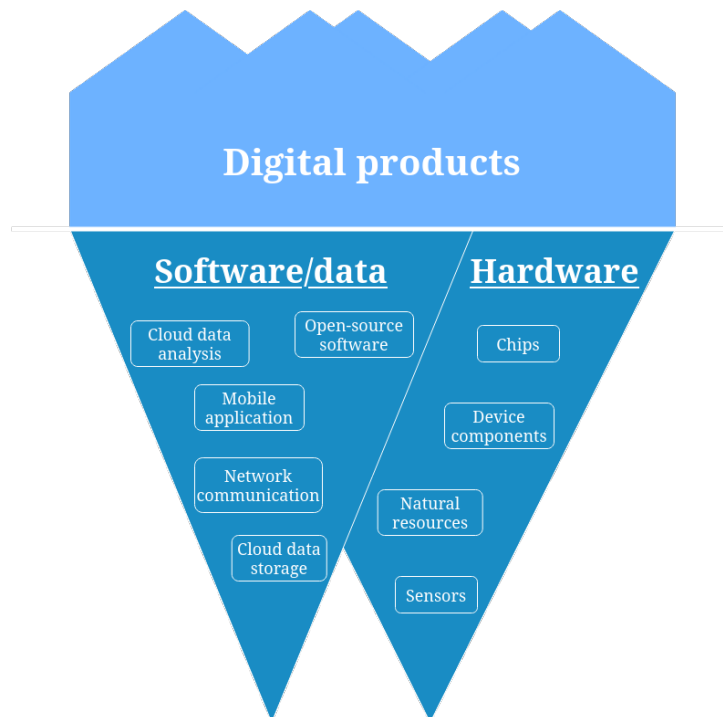


Figure 1: The iceberg of digital products. The end user only sees the product itself, the tip of the iceberg. The iceberg is not exhaustive, but illustrates some of the components contained in digital products.

But as complex as identification is, it remains a preliminary step. After identifying members, the next step is to ensure that they achieve an adequate level of cybersecurity and can be held responsible. Each additional member brings their own vulnerabilities, whether they originate in the people working for that organisation or the systems that they use. For example, Target stores in the US were hacked after the hackers found a weak password in air-conditioning systems supplied by a third party.⁴³ Since those systems were connected to the Target network, the hackers gained access to payment data within the cash registers. Target may have been aware of their co-operation with the air conditioning supplier, but seemingly not with the additional cybersecurity measures required.

Moreover, as Chapter 4 shows, notions such as ‘software’ mask already complex sectors. A software supplier can publish their code publicly, so that anyone may download and modify it, or sell it, without any access to the underlying code.⁴⁴ This software could be a final product, or a component integrated in other software packages. Similarly, a hardware supplier could sell a single screw, or an entire car chassis. Each actor carries organisation-dependent risks, in turn requiring

⁴³ Brian Krebs, ‘Target Hackers Broke in Via HVAC Company’ (Krebs on Security, 5 February 2014) <<https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/>> accessed 20 June 2022.

⁴⁴ Jaap-Henk Hoepman and Bart Jacobs, ‘Increased Security through Open Source’ (2007) 50 Communications of the ACM 79.

distinct mitigation measures.⁴⁵ Broad terms such as ‘software’ and ‘hardware’ hide heterogeneous actors which require specific attention—a complex ask when connected to the scale of digital product interdependencies.

Digital product interdependencies are often opaque—both to end users and those within the interdependent network.⁴⁶ For instance, years after a critical vulnerability in software similar to XZ Utils, many software developers still used the vulnerable version.⁴⁷ This is not just a problem of small software developers. In fact, Iranian hackers exploited the vulnerability to gain access to a US federal agency—a year after the vulnerability became public.⁴⁸ The main cause of this seemingly unprofessional conduct is the sheer scale of digital product interdependencies: this vulnerable component is merely one of countless other software integrations. If identification of components becomes impossible, so does mitigating their individual risks. Complexity and opaqueness coalesce: the sheer number of dependencies masks their existence—and associated risks.

Individual services are also opaque, especially to the end user. Recent EU consumer investigations found widespread use of ‘dark patterns’, such as fake discounts, a lack of contact details, and deceptive product labels on Shein, a Chinese webshop.⁴⁹ In a similar investigation, the European Consumer Organisation BEUC found that Temu, another Chinese e-commerce platform, did not provide ‘sufficient traceability of the traders’ on the platform; this opaqueness made it difficult for consumers to realise which organisation they actually purchased their products from.⁵⁰ On these platforms, opaqueness is not just a by-effect of complexity—it may indeed be its purpose.

In this opaque and complex chain, control is concentrated in the hands of a few large technology companies. The relation between interdependent chain participants is often asymmetric: one entity holds a disproportionate amount of control over the product’s functioning.⁵¹ Recently, ‘smart bed’ customers suddenly found their beds stuck in an upright position, not because the manufacturer used faulty screws or

45 Jillian K Kwong and Keri Pearlson, ‘Supply Chain Cybersecurity and Small and Medium-Sized Enterprises (SMEs): Exploring Shortcomings in Third Party Risk Management of SMEs’ Proceedings of the 57th Hawaii International Conference on System Sciences 6656.

46 Cobbe, Norval and Singh (n 21) 69.

47 Bill Toulas, ‘Over 30% of Log4j Apps Use a Vulnerable Version of the Library’ (Bleeping-Computer) <<https://www.bleepingcomputer.com/news/security/over-30-percent-of-log4j-apps-use-a-vulnerable-version-of-the-library/>> accessed 6 November 2025.

48 Edward Graham, ‘Iranian Hackers Compromised a Federal Agency’s Network, CISA and FBI Say’ (Nextgov.com, 16 November 2022) <<https://www.nextgov.com/cybersecurity/2022/11/iranian-hackers-compromised-federal-agencys-network-cisa-and-fbi-say/379832/>> accessed 5 February 2026.

49 ‘Commission and National Authorities Urge SHEIN to Respect EU Consumer Protection Laws’ (European Commission - European Commission) <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1331> accessed 27 November 2025.

50 BEUC, ‘Taming Temu’ <<https://www.beuc.eu/enforcement/taming-temu>> accessed 27 November 2025.

51 Jennifer Cobbe, ‘Governance and Interdependence in Data-Driven Supply Chains’ Global Governance by Data: Infrastructures of Algorithmic Rule (2026).

bolts, but because of an outage at Amazon Web Services.⁵² This example demonstrates that cloud platforms, such as Amazon Web Services, hold significant control over the end product. Large technology companies often control these ‘choke points’—products or services, such as the cloud, without which the entire product could not function. And where an end user can easily replace a faulty screw or bolt, technology companies retain exclusive control over their products or services. As a result, control over the functioning of the digital end product shifts into the hands of a few technology companies.

This asymmetry is a symptom of the wider development of servitisation, whereby manufacturers offer *services* rather than *products*. For instance, BMW offered drivers a monthly subscription to ‘unlock’ seat heating.⁵³ If the consumer no longer pays the monthly subscription, they lose access to this functionality. This ‘software-as-a-service’ business model differs from the traditional buyer-seller relation where the buyer owned the product after purchasing it.⁵⁴ This model is prevalent across digital products, such as in cloud services. This is a worrying trend from a dependence perspective, as the end user is never fully in control over the service: if the monthly subscription ends, their access ends. I will return to questions surrounding asymmetric control in Chapter 5, where I discuss the position of the end user when a manufacturer controlling a choke point ceases their operations.

4 Policy approaches

The problems of digital product interdependencies are steadily emerging, as evidenced by the patterns centred around complexity, opaqueness, and control. The emergence of these problems has not been without academic and political attention. Two topics are mainly rising on both the academic and political agenda: supply chain cybersecurity and digital sovereignty.

4.1 Supply chain cybersecurity

Supply chain cybersecurity is a strategic response to the rise of supply chain attacks. In these attacks, malicious actors focus on the weakest member in a chain, so that they can subsequently infiltrate the chain through their initial target. Supply chain attacks are therefore always twofold: there is an initial attack on a supplier and a subsequent attack on the assets of a second, main target.⁵⁵

52 Sopan Deb, ‘Smart Beds Helped Them Sleep on a Cloud. Then the Cloud Crashed.’ The New York Times (24 October 2025) <<https://www.nytimes.com/2025/10/24/business/amazon-aws-outage-eight-sleep-mattress.html>> accessed 31 October 2025.

53 Andrew J Hawkins, ‘BMW Drops Plan to Charge a Monthly Fee for Heated Seats’ (The Verge, 7 September 2023) <<https://www.theverge.com/2023/9/7/23863258/bmw-cancel-heated-seat-subscription-microtransaction>> accessed 19 November 2025.

54 Millard (n 17) ch 2.

55 European Union Agency for Cybersecurity and others, ENISA Threat Landscape for Supply Chain Attacks (A Malatras and others eds, European Network and Information Security Agency 2021).

In the introduction, I illustrated two recent supply chain attacks: the XZ Utils case, a software supply chain attack, and the Hezbollah case, a hardware attack. These attacks are not rare. In 2007, for instance, Israeli jets bombed a Syrian nuclear installation. The Syrian radar that was meant to prevent the attack malfunctioned shortly before. In later years, defence experts suggested that attackers intentionally shut down the radar; a chip made by a European company was remotely disabled just before the attack.⁵⁶ A few years later, the Snowden revelations showed that the NSA routinely manipulated routers and servers manufactured by a US company for espionage purposes.⁵⁷ These diverse cases show that supply chain attacks are increasingly common.

In fact, supply chain attacks are not just conducted by highly specialised intelligence services. A relatively common supply chain attack focuses on software repositories.⁵⁸ In these attacks, threat actors look for the most popular software packages on a repository; this popularity indicates that many other software developers have integrated them. Given this popularity, the initial infiltration can quickly cascade to many other software packages, like in the XZ Utils attack. However, unlike the XZ Utils attack, recent repository attackers merely attempted to obtain some cryptocurrency, which experts considered a ‘relatively unsophisticated approach’.⁵⁹ This lack of sophistication suggests that supply chain attacks are increasingly common across different types of attackers, from stately actors to more ‘unsophisticated’ actors with criminal intentions.

In response to these attacks, academics and policy makers call for ‘supply chain cybersecurity’, a strategic effort to address cyberattacks cascading through supply chains.⁶⁰ Academics increasingly focus on conceptualising and crafting practical requirements for these strategies,⁶¹ while policy makers at the European Agency

56 Sally Adee, ‘The Hunt For The Kill Switch’ (2008) 45 IEEE Spectrum 34; Olav Lysne, *The Huawei and Snowden Questions* (Springer International Publishing 2018) ch 1.

57 Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (First Edition, Metropolitan Books/Henry Holt 2014).

58 Ax Sharma, ‘Self-Propagating Supply Chain Attack Hits 187 Npm Packages’ (BleepingComputer) <<https://www.bleepingcomputer.com/news/security/self-propagating-supply-chain-attack-hits-187-npm-packages/>> accessed 18 September 2025; Gyana Swain, ‘Wave of Npm Supply Chain Attacks Exposes Thousands of Enterprise Developer Credentials’ (InfoWorld, 28 August 2025) <<https://www.infoworld.com/article/4047739/wave-of-npm-supply-chain-attacks-exposes-thousands-of-enterprise-developer-credentials.html>> accessed 18 September 2025; Jeff Burt, ‘Typosquat Supply Chain Attack Targets Go Developers’ (DevOps.com, 5 February 2025) <<https://devops.com/typosquat-supply-chain-attack-targets-go-developers/>> accessed 18 September 2025.

59 Gyana Swain, ‘Massive Npm Supply Chain Attack Hits 18 Popular Packages with 2B Weekly Downloads’ (CSO Online, 9 September 2025) <<https://www.csoonline.com/article/4053725/massive-npm-supply-chain-attack-hits-18-popular-packages-with-2b-weekly-downloads.html>> accessed 18 September 2025.

60 Myles D Garvey, Jim Samuel and Andrey Kretinin, ‘An Ontology of Supply Chain Cybersecurity’ in Steven Carnovale and Sengun Yeniyurt (eds), *Cyber security and supply chain management: risks, challenges and solutions* (World Scientific 2021) 106.

61 See, inter alia, Hugh Boyes, ‘Cybersecurity and Cyber-Resilient Supply Chains’ [2015] *Technology Innovation Management Review* 7; Steven Carnovale and Sengun Yeniyurt (eds), *Cyber Security and Supply Chain Management: Risks, Challenges and Solutions* (World Scientific 2021); Steven A Melnyk and others, ‘New Challenges in Supply Chain Management: Cybersecurity across the

on Cybersecurity examine the frequency and nature of supply chain attacks in threat landscape reports.⁶² This work indicates that risks arising out of supply chain interdependencies are increasingly on the academic and political agenda.

4.2 Digital sovereignty

Supply chains are also part of geopolitical concerns. The European Commission held in 2020 that ‘the [cybersecurity] threat landscape is compounded by geopolitical tensions [...] over control of technologies across the whole supply chain.’⁶³

Diplomatic clashes over the role of China in 5G network infrastructure exemplify these geopolitical concerns.⁶⁴ 5G infrastructure is a vital component of the network layer—IoT devices, for instance, can use this infrastructure for wireless communication.⁶⁵ Most 5G network infrastructure stems from Chinese manufacturers, such as Huawei. This important role of China in the production and functioning of 5G worried American and European policy makers, who believed that China would exploit the infrastructure for espionage purposes. As a result, American and European policy makers are restricting or banning Chinese providers from their telecommunication infrastructure, a move strongly condemned by the Chinese government.⁶⁶ This ongoing diplomatic clash highlights how digital product interdependencies are becoming contested geopolitical landscapes.

In the 2025 State of the Union, EU Commission President Von der Leyen spoke of ‘Europe’s independence moment’, referring to an increase in digital and territorial sovereignty. Digital sovereignty refers to the need for the EU to become technologically independent from other states through social, economic, geopolitical and legal

Supply Chain’ (2022) 60 *International Journal of Production Research* 162; Alessandro Creazza and others, ‘Who Cares? Supply Chain Managers’ Perceptions Regarding Cyber Supply Chain Risk Management in the Digital Transformation Era’ (2022) 27 *Supply Chain Management: An International Journal* 30.

62 European Union Agency for Cybersecurity and others, *ENISA Threat Landscape for Supply Chain Attacks* (n 55); European Union Agency for Cybersecurity and others, *ENISA Threat Landscape 2021 – April 2020 to Mid-July 2021* (M Theocharidou and others eds, European Network and Information Security Agency 2021).

63 European Commission and High Representative of the Union for Foreign Affairs and Security Policy, ‘The EU’s Cybersecurity Strategy for the Digital Decade’ (2020) JOIN(2020) 18 1.

64 Karsten Friis and Olav Lysne, ‘Huawei, 5G and Security: Technological Limitations and Political Responses’ (2021) 52 *Development and Change* 1174, 1177–1179; Roxana Radu and Cedric Amon, ‘The Governance of 5G Infrastructure: Between Path Dependency and Risk-Based Approaches’ (2021) 7 *Journal of Cybersecurity* 1.

65 Aymen I Zreikat and others, ‘The Integration of the Internet of Things (IoT) Applications into 5G Networks: A Review and Analysis’ (2025) 14 *Computers* 250.

66 David Shepardson, ‘US Agency Votes to Tighten Restrictions on Chinese Tech Companies Deemed Threats’ *Reuters* (28 October 2025) <<https://www.reuters.com/business/media-telecom/us-agency-votes-tighten-restrictions-chinese-tech-companies-deemed-threats-2025-10-28/>> accessed 2 February 2026; Foo Yun Chee, ‘EU Plan to Phase-out High-Risk Tech Draws Fire from China’s Huawei’ *Reuters* (21 January 2026) <<https://www.reuters.com/business/media-telecom/eu-phase-out-high-risk-tech-targets-huawei-chinese-companies-2026-01-20/>> accessed 2 February 2026.

policies.⁶⁷ In his technology stack, Sheikh shows that American companies dominate virtually the entire cloud layer; the EU plays a marginal role at best.⁶⁸ As the 5G discussion shows, this lack of European presence is not limited to the cloud layer. If the EU truly strives for digital sovereignty, it cannot ignore digital product interdependencies.

As part of its digital sovereignty agenda, the EU is implementing a regulatory strategy coined by Farrand et al. as ‘regulatory mercantilism’.⁶⁹ The initial aim of this regulatory strategy is to confine technology production to the physical territory of the Union. If this proves too difficult, the EU aims to impose its norms through regulatory influence on the production process.⁷⁰ The field of EU cybersecurity law exemplifies such regulatory influence.

5 Legal framework

Over the past few years, the EU has taken significant steps in advancing cybersecurity law. This field of law is closely aligned with supply chain cybersecurity and digital sovereignty efforts;⁷¹ this alignment suggests that the development of European cybersecurity law may help in mitigating risks arising out of digital product interdependencies. Before analysing this potential, I will shortly discuss how the law can contribute to improving cybersecurity practices in general.

5.1 Improving cybersecurity through legal frameworks

This dissertation analyses how emerging legal frameworks may address risks associated with digital product interdependencies. In other words, I believe that a legal framework is capable of tackling those risks—and more capable than, for instance, leaving the solution to the market. I will briefly set out why a legal response is necessary and fruitful in the context of cybersecurity risks in general and with regards to digital product interdependencies.

In general, proper cybersecurity investments demand regulatory incentives. In legal-economic terms, cybersecurity offers positive externalities. In other words, regulatory incentives lead to cybersecurity investments that positively impact on third parties. For instance, an organisation may adopt cybersecurity measures that protect their customers from the negative consequences of a data breach, such as identity theft. Without regulatory incentives, organisations will likely prioritise their own interests, possibly leading to negative consequences for third parties.⁷²

67 Bellanova, Carrapico and Duez (n 11); Daniel Lambach and Linda Monsees, ‘Beyond Sovereignty as Authority: The Multiplicity of European Approaches to Digital Sovereignty’ (2025) 4 *Global Political Economy* 71.

68 Sheikh (n 26) 12–14.

69 Benjamin Farrand, Helena Carrapico and Aleksei Turobov, ‘The New Geopolitics of EU Cybersecurity: Security, Economy and Sovereignty’ (2024) 100 *International Affairs* 2379.

70 *ibid* 2383.

71 Bellanova, Carrapico and Duez (n 11).

72 Bygrave (n 15) 2.

Another law and economics theory also points to the benefits of regulatory incentives: the least cost avoider theory. In simple terms, this theory holds that regulation should address the entity that suffers the least costs in achieving the regulatory goals. If a manufacturer is not held responsible for preventing harms arising out of the insecurity of their products, this burden falls on the end user. This was the status quo before the incursion of European cybersecurity law: manufacturers—or software developers—did not have sufficient incentives to provide strong cybersecurity measures when releasing their products and the end user did not have sufficient bargaining power to improve the manufacturer's stance.⁷³ The end user could only improve the cybersecurity of the product by taking manual measures, such as changing default passwords. If an end user fails to take these measures and suffers a cybersecurity breach, there are additional societal costs, such as when a hospital has to halt operations. The costs suffered by the manufacturer to improve the cybersecurity of their products is most likely much lower. Hence, the least cost avoider theory suggests that cybersecurity regulation incentivises the entity that suffers the least (societal) costs in taking cybersecurity measures.

Digital product interdependencies are complex due to their heterogeneity. Actors range across size, location, expertise, and digital adoption—a complex landscape which requires overarching principles and norms. A legal framework can help harmonise cybersecurity practices regardless of such diversity. In this context, supply chain cybersecurity experts, for example, call for legally mandated standardisation.⁷⁴ Standardised guidelines help organisations harmonise their cybersecurity practices throughout their chain, regardless of organisation-specific demands. Such guidelines also prevent holdout problems, where organisations aim to prevent costs by only acting when others do. Legal frameworks can—and do—mandate the development and implementation of such standards and harmonised practices.⁷⁵

Legal requirements for standardisation help to ensure that cybersecurity is a collective effort of interdependent actors. Political, legal or economic sanctions may only address single actors or organisations, thereby missing that the chain is only as strong as its weakest member. Harmonised cybersecurity practices entail that all partners attain an equal level of cybersecurity. All the fish in the pond, regardless of their size, are therefore more secure.

In summary, while a legal framework is not necessarily the most capable policy response to all risks, it offers unique benefits in the case of risks associated with digital product interdependencies. A legal framework encourages a harmonised, collective

73 R Anderson, 'Why Information Security Is Hard - an Economic Perspective' Seventeenth Annual Computer Security Applications Conference (IEEE Comput Soc 2001); Paul Rosenzweig, 'Cybersecurity and the Least Cost Avoider' [2013] Lawfare <<https://www.lawfaremedia.org/article/cybersecurity-and-least-cost-avoider>> accessed 28 November 2025.

74 Melnyk and others (n 61).

75 Irene Kamara, 'European Cybersecurity Standardisation: A Tale of Two Solitudes in View of Europe's Cyber Resilience' (2024) 37 Innovation: The European Journal of Social Science Research 1441.

effort—one that may lead to the lowest cost and to a scope that covers more than just the biggest fish in the pond.

5.2 European cybersecurity law: an overview

Over the past decade, the EU has introduced several legislative acts which aim to address the rise of cybersecurity incidents, including for—sometimes explicitly—digital product interdependencies and Internet of Things devices. In its 2020 Cybersecurity Strategy, the European Commission noted that ‘all *Internet-connected things* in the EU, [...] and *the whole supply chains which make them available*, need to be secure-by-design, resilient to cyber incidents, and quickly patched when vulnerabilities are discovered.’⁷⁶ One of the primary conduits for this aim is the introduction of ‘regulatory measures for an Internet of Secure Things’.⁷⁷ The regulatory measures that followed since the 2020 Cybersecurity Strategy form the central framework of this dissertation. Here, I introduce the most prominent pieces of legislation regarding cybersecurity: the Cyber Resilience Act; the NIS2 Directive; and the General Data Protection Regulation. I introduce other related acts in the following chapters where necessary, such as the Digital Operational Resilience Act and the Cybersecurity Act.⁷⁸

The Cyber Resilience Act (CRA) entered into force in 2024.⁷⁹ As product safety law, the CRA imposes rules on manufacturers and developers of ‘products with digital elements’, meaning both software and hardware and their remote data processing solutions.⁸⁰ The CRA thus applies to nearly all manufacturers and developers of IoT devices and device components.⁸¹

The CRA contains product cybersecurity requirements and general product safety requirements, such as providing technical documentation.⁸² Among the list of cybersecurity requirements are concepts such as maintaining data integrity and mitigating vulnerabilities.⁸³ Manufacturers have several obligations which revolve

76 European Commission and High Representative of the Union for Foreign Affairs and Security Policy (n 63) 5. Emphasis mine.

77 *ibid* 12.

78 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Digital Operational Resilience Act); 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).

79 Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) [2024] OJ L2024/2487.

80 Art 3(1) CRA.

81 Manufacturers of devices which are subject to a specific regulatory regime, such as medical devices, are exempted from the scope of the CRA. Art 2(2) CRA.

82 Art 13 CRA.

83 Annex I CRA.

around digital product interdependencies. For example, manufacturers must ensure security-by-design, meaning that every step of their production process must take cybersecurity into account.⁸⁴ Manufacturers must also conduct ‘due diligence’ when integrating third-party components in their product, in order to ensure that the security of their product is not compromised by those third-party components.⁸⁵

Market authorities enforce the provisions of the CRA. They must evaluate products upon suspicion of non-compliance and can even perform large-scale sweeps to check particular products.⁸⁶ In case of non-compliance with the CRA’s provisions, market authorities can mandate various corrective actions, including product withdrawal or recall. They can also hand out significant fines.⁸⁷

In sum, the CRA is the most pertinent piece of EU cybersecurity law, because of its broad scope and its role as the reference point for cybersecurity requirements in other legislation.⁸⁸

The Network and Information Security (NIS) Directive initially came into force in 2016, as the NIS1 Directive. With the NIS1 Directive, the EU legislators intended to create a harmonised level of cybersecurity across the Union, specifically in critical sectors (e.g., health). The NIS1 Directive, however, did not achieve its aims. The implementation of the Directive differed significantly between Member States.⁸⁹ Against this backdrop, the Commission revised NIS1 and introduced the NIS2 Directive.

NIS2 came into force in 2023 and, as with its predecessor, introduced cybersecurity rules for the ‘network and information systems’ which entities operating in certain critical sectors use.⁹⁰ Therefore, the NIS2 rules apply, for instance, to IoT devices used by entities in the health sector (e.g., by hospitals). The entities must ensure that they take adequate cybersecurity measures for those devices. Among the list of requirements, NIS2 explicitly requires ‘supply chain security’.⁹¹ In Chapter 2, I examine these requirements more comprehensively. The NIS2 Directive also introduces certain requirements for Member States, such as the adoption of national cybersecurity strategies.⁹²

84 Art 13(1) CRA.

85 Art 13(5) CRA.

86 Art 54 & 60 CRA.

87 Art 64 CRA.

88 See for instance Recital 32 CRA: ‘By protecting consumers and organisations from cybersecurity risks, the essential cybersecurity requirements laid down in this Regulation are also to contribute to enhancing the protection of personal data and privacy of individuals.’

89 Commission, ‘Impact Assessment Report Accompanying the Document Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity across the Union, Repealing Directive (EU) 2016/1148’ SWD (2020) 345 final.

90 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). Art 6(1) NIS2.

91 Art 21(2)(d) NIS2.

92 Art 7 NIS2.

Supervision and enforcement of the NIS2 Directive lies with different authorities, depending on the Member State and sector. For instance, supervision over health institutions lies with the existing supervisory authorities for the health sector, but now extending to cybersecurity. These authorities have various powers, including on-site inspections, ad hoc audits, and security scans.⁹³ Upon finding an infringement of NIS2, the authorities can order the entities to cease those activities, implement certain recommendations, or make their infringements public.⁹⁴ Moreover, board members are personally liable for improper cybersecurity risk management—a unique type of enforcement for European cybersecurity law.⁹⁵

The General Data Protection Regulation (GDPR) forms the primary legislative act related to the protection of personal data in the European Union.⁹⁶ The rules of the GDPR apply primarily to ‘controllers’, regarding the ‘processing’ of personal data.⁹⁷

Controllers are natural or legal persons who determine the means and purposes of personal data processing.⁹⁸ For example, if, for their smart watch, Apple decides how the watch collects data and for which purpose, Apple is the controller.

Under the GDPR, ‘personal data’ is an extensive notion, meaning ‘any information relating to an identified or identifiable natural person.’⁹⁹ Many types of data processed by an IoT device are personal data under the GDPR (e.g., heart rate measurements).

In the context of this dissertation, the GDPR comes to the fore when discussing cybersecurity requirements in the context of personal data protection.¹⁰⁰ A main principle of the GDPR is that controllers and ‘processors’, who process data on behalf of controllers,¹⁰¹ must ensure ‘appropriate security’, including for their direct co-operation.¹⁰² The appropriateness of the measures depends on the state of the art, the costs of implementation, and the risks associated with the specific type of processing to the rights and freedoms of data subjects.¹⁰³ This obligation therefore covers the data-related cybersecurity risks arising out of the interdependence between controllers and processors.

Furthermore, the GDPR contains rules related to ‘joint controllership’, where two or more entities determine the means and purposes of processing together.¹⁰⁴ In a recent case, the Court of Justice found that Facebook, for instance, is a joint controller with

93 Art 32(2) NIS2.

94 Art 32(4) NIS2.

95 Art 20(1) NIS2.

96 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

97 Art 2(1) GDPR. For definitions, see: Art 4(1) on personal data, Art 4(2) on processing, Art 4(7) on the controller and Art 4(8) on the processor.

98 Art 7 GDPR.

99 Art 1 GDPR.

100 Nusselder (n 19).

101 Art 4(8) GDPR.

102 Art 5(f) GDPR.

103 Art 32 GDPR.

104 Art 26 GDPR.

websites that embed the Facebook ‘like’ button.¹⁰⁵ This joint controllership must also comply with the GDPR in full, including with the security requirements.¹⁰⁶ In sum, the GDPR ensures that co-operating entities take the cybersecurity of their co-operation into account when processing personal data.

The CRA, NIS2, and GDPR cover various cybersecurity related aspects of digital products. Digital product interdependencies are regulated under this framework in various ways. The question remains if the overlap between this legislation is sufficient to address cybersecurity risks arising out of digital product interdependencies.

6 Outline and methodology

I answer the main research question of this dissertation through six journal articles, which were submitted to or published in various journals and conference proceedings. Chapters 3 and 6 are the work of co-authorship. Table 1 sets out my contribution to all the articles. In the outline below, I shortly summarise the work of each chapter, before coming to the methodology of this dissertation.

Table 1: Author contribution table

Chapter	Own contribution/role
Chapter 2	Sole author
Chapter 3	Legal-doctrinal analysis for ‘Background and related work’ section and policy recommendations in section ‘Recommendations’.
Chapter 4	Sole author
Chapter 5	Sole author
Chapter 6	Legal-doctrinal analysis for ‘Background and related work’ section and policy recommendations in section ‘Recommendations’.
Chapter 7	Sole author

6.1 Outline of the chapters

This main research question consists of several sub-questions, which this dissertation answers in the following order:

- What is the role of supply chain cybersecurity in European cybersecurity law, especially in relation to the Internet of Things? (Chapter 2)
- What do consumers expect how manufacturers will and should respond to emerging privacy and security risks with IoT devices? (Chapter 3)

¹⁰⁵ C-40/17 *Fashion ID v. Facebook Ireland* EU:C:2019:629.

¹⁰⁶ EDPB, ‘Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR’ 41.

- Does European cybersecurity law adequately strike a balance between regulating cybersecurity risks of open-source software and maintaining such software for a healthy software ecosystem? (Chapter 4)
- To what extent can manufacturers avoid responsibilities stemming from European cybersecurity law when they cease their operations and does a legal model exist to tackle such possible evasion? (Chapter 5)
- How long do consumers expect different smart device categories to last, and which factors influence these expectations? (Chapter 6)
- To what extent does European cybersecurity law mitigate human vulnerabilities when aiming to protect the ‘vulnerable consumer’? (Chapter 7)

One way of tackling interdependencies, as introduced in Section 4.1, is through supply chain cybersecurity. Therefore, Chapter 2 delves into the NIS2 Directive’s ‘supply chain security’ requirement. As research on supply chain cybersecurity remains scarce, this chapter builds an initial framework of requirements for adequate supply chain cybersecurity measures. Using this framework, the chapter subsequently questions whether the NIS2 Directive’s provisions on supply chain cybersecurity are adequate. The chapter concludes that NIS2 misses the mark, mainly due to a misallocation of responsibilities and a lateral role for supply chain cybersecurity under a broad array of cybersecurity requirements. Given this conclusion, Chapter 2 already points to some flaws of European cybersecurity law with regards to addressing digital product interdependencies.

Chapter 3 offers a social-empirical analysis of what consumers expect regarding the cybersecurity of Internet of Things devices. Consumer expectations have an important role in a range of consumer law, including in proving the defectiveness of a product under the Product Liability Directive. Our study confirms that consumers often expect the manufacturer to act when a cybersecurity incident occurs. The more severe an incident is, the more serious a consumer expects the manufacturer to respond, for instance by recalling a product. These expectations suggest that the manufacturer must ensure adequate post-purchase maintenance and support channels, so that they can respond adequately to cybersecurity incidents. In other words, the manufacturer cannot simply disregard the consumer after finalising the sale: they remain connected.

Chapter 4 investigates how the Cyber Resilience Act regulates open-source software, a cornerstone of the modern software ecosystem. Open-source software is a common target of supply chain attacks and—as the XZ Utils case shows—a vital interdependency for modern digital products. At the same time, open-source software differs significantly from commercial or ‘proprietary’ software: the code is openly accessible, downloadable, and extendable and generally the work of a small(er) team of developers. Given these unique characteristics, EU legislators struggled to find a regulatory approach that balanced the benefits of open-source software with its cybersecurity risks. The final result seems, *prima facie*, adequate for the Cyber Resilience Act. However, as the legislators constantly adapted the framework during the legislative process, the final regulatory approach is intertwined with the system of

the Cyber Resilience Act. It seems likely that the final word has not been spoken about the position of open-source software (developers) under EU digital policy.

Chapter 5, in turn, addresses how to regulate IoT manufacturers that cease to exist by choice or by force (e.g., bankruptcy, sudden disappearance). The chapter emphasises that IoT products often become obsolete when the manufacturer ceases their operations, leading to the absence of a central server or update mechanism. This results in problems for the end user, who is left with a largely defunct or vulnerable end product. European cybersecurity law barely addresses these problems, which emanate in digital product interdependencies such as cloud servers and software integrations. The main cause of this problem is that the law does not easily stretch beyond familiar or default concepts of interdependent actors. To improve the legal framework, Chapter 5 recommends that policy makers emphasise the development of interoperable and open-source digital product components, as they offer the end user more control over the functioning of their end product.

Given the risks identified for obsolete digital products, Chapter 6 follows with a social-empirical analysis of consumer expectations regarding product lifecycles, particularly for the Internet of Things. In terms of the overall research question, this chapter elucidates the cybersecurity risks of unsupported IoT devices and how these risks shape consumer perspectives. The analysis shows that consumers, in many cases, expect product lifetimes that go further than those proposed in the Cyber Resilience Act. The chapter hence recommends that policy makers take these consumer expectations into account when drafting guidelines on product support periods following the CRA.

Chapter 7 shifts this general consumer focus to *vulnerable* consumers, individuals who are at greater risk of abuse when, for instance, their data is breached. The preamble purports that the Cyber Resilience Act aims to address cybersecurity risks particularly for such vulnerable consumers, but there is seemingly no further role for consumer vulnerability in the legal act itself. Interdisciplinary research shows that human vulnerability calls for a flexible and personalised regulatory approach. In line with earlier articles, however, Chapter 7 concludes that the Cyber Resilience Act lacks this level of sophistication.

Given this overview, I must admit that this dissertation does not fully answer the central research question. The chapters cover individual elements of both digital product interdependencies (e.g., open-source software) and European cybersecurity law (e.g., the Cyber Resilience Act). Unfortunately, both fields are too comprehensive to cover entirely in one dissertation. What the dissertation aims to show, through these chapters, is which type of digital product interdependencies exist and which cybersecurity risks may arise out of those interdependencies. For the elements covered in each chapter, the conclusion is often the same: European cybersecurity law does not (fully) address the cybersecurity threats identified. Hence, while not an answer to the main research question in a broad sense, the dissertation does answer the question for these particular elements and establishes the need for future research. Chapter 8 offers a more detailed conclusion.

6.2 Methodology

This dissertation is primarily a legal-doctrinal analysis in that it describes the current legal framework and subsequently offers normative accounts of the quality of that framework and how to improve it.¹⁰⁷ Before delving into this method, I must mention that Chapters 3 and 6 differ from the legal-doctrinal approach: they offer social-empirical analyses of concepts originating in EU legislation; my contribution to these articles, however, remains legal-doctrinal.

For the descriptive part of my legal-doctrinal analysis, I studied legal texts and documents, ranging from legislation to soft law. Case law only played a minor role. European cybersecurity law is in a nascent state, which means that not many cases have yet made it to court. The European Court of Justice has ruled on only a few cases in the context of cybersecurity, predominantly centred around the General Data Protection Regulation.¹⁰⁸

In terms of the prescriptive analysis, this dissertation belongs to the field of ‘technology law’ or ‘law and technology’.¹⁰⁹ In this area, researchers combine the study of law with the study of technology, that is, technology may either be the subject of legal inquiry (i.e., similar to ‘environmental law’), or the driver (e.g., technology as regulation).

This dissertation identifies how certain risks—those arising out of interdependencies—associated with technological artefacts—the Internet of Things—fit within existing and emerging legal frameworks. If a legal gap exists, technology law scholars often recommend which regulatory response could bridge that gap. Proposals range from traditional legislative changes to regulation through product design.¹¹⁰ These proposals form the normative-prescriptive side of the legal-doctrinal analysis. Indeed, this dissertation proposes a mix of regulatory responses, ranging from broader, technology-neutral legislative adaptations to technology-specific changes, such as interoperability.

Next to legal-doctrinal research, this dissertation builds on multidisciplinary work. For this work, I greatly benefitted from my position at iHub, the interdisciplinary research group for digitalisation and society at Radboud University. At iHub, I gained diverse perspectives on the functioning and impact of digital product interdependencies. Out of these multidisciplinary perspectives, two fields return most often throughout this dissertation: supply chain management and information security studies.

The field of supply chain management studies stems primarily from business management research. In general, this research elucidates how supply chains function and which risks emerge from them. More specifically, I analysed studies related to

107 Sanne Taekema, ‘Theoretical and Normative Frameworks for Legal Research: Putting Theory into Practice’ [2018] *Law and Method*.

108 See more extensively on these cases: Nusselder (n 19).

109 Both terms are equally broad, see EJ Koops, ‘A Taxonomy for Descriptive Research in Law and Technology’ in E Palmerini and E Stradella (eds), *Law and technology: The challenge of regulating technological* (Pisa University Press 2013) 37.

110 Koops (n 109); Michael Guihot, ‘Coherence in Technology Law’ (2019) 11 *Law, Innovation and Technology* 311.

‘cyber supply chain risk management’ to understand the cybersecurity problems of digital product interdependencies.¹¹¹ Cyber supply chain risk management studies mainly point to the economic impact of these cybersecurity problems: if one manufacturer halts their production because of a cyber attack, numerous other interdependent entities are affected. Academics in this field therefore suggest various mitigation policies and strategies. I analysed these suggestions to reflect on legal conceptualisations of supply chain cybersecurity (see predominantly Chapter 2).

Information security studies informed the cybersecurity side of this dissertation. Security academics do not merely address technical risks—the field also covers aspects such as physical security and social engineering.¹¹² Information security studies thus provide a broad understanding of both ‘attack’ and ‘defence’, i.e. how a threat actor may conduct an attack and which policies may prevent (the effects of) such an attack. By understanding the exact nature of cybersecurity threats, I could reflect whether European cybersecurity law adequately addressed them.

Overall, this dissertation lies at the convergence of three areas: cybersecurity, digital product interdependencies, and European cybersecurity law. The overarching normative perspective is legal-doctrinal, supported by supply chain management and information security studies. Next to these main disciplines, some other disciplines are scattered throughout the following chapters, such as artificial intelligence and political science studies. Given this variety, and their sometimes brief role, I will not describe each discipline here. In the end, I must simply conclude that this dissertation is not unlike its subject: an interdependent product.

111 Sandor Boyson, ‘Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical IT Systems’ (2014) 34 *Technovation* 342.

112 Andrea M Matwyshyn, ‘CYBER!’ (2017) 2017 *BYU Law Review* 1109, 1156.

References

- Adee S, 'The Hunt For The Kill Switch' (2008) 45 IEEE Spectrum 34
- Ajmera P, 'Cybersecurity in the Internet of Things: Trends and Challenges in a Nascent Field' (2025) 59 Computer Law & Security Review 106204
- Al-Masri E and others, 'Investigating Messaging Protocols for the Internet of Things (IoT)' (2020) 8 IEEE Access 94880
- Anderson R, 'Why Information Security Is Hard - an Economic Perspective' *Seventeenth Annual Computer Security Applications Conference* (IEEE Comput Soc 2001)
- Arnbak AM, 'Securing Private Communications: Protecting Private Communications Security in EU Law: Fundamental Rights, Functional Value Chains and Market Incentives' (PhD thesis, Universiteit van Amsterdam 2015)
- Bellanova R, Carrapico H and Duez D, 'Digital/Sovereignty and European Security Integration: An Introduction' (2022) 31 European Security 337
- Berg R, 'Ex-Israeli Agents Reveal How Hezbollah Pager Attacks Were Carried Out' (23 December 2024) <<https://www.bbc.com/news/articles/cwy3l02wxqdo>> accessed 5 February 2026
- BEUC, 'Taming Temu' <<https://www.beuc.eu/enforcement/taming-temu>> accessed 27 November 2025
- Biasin E and Kamenjašević E, 'Cybersecurity of Medical Devices: New Challenges Arising from the AI Act and NIS 2 Directive Proposals' (2022) 3 International Cybersecurity Law Review 163
- Boyes H, 'Cybersecurity and Cyber-Resilient Supply Chains' [2015] Technology Innovation Management Review 7
- Boyson S, 'Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical IT Systems' (2014) 34 Technovation 342
- Bratton BH, *The Stack: On Software and Sovereignty* (MIT Press 2015)
- Brian Krebs, 'Target Hackers Broke in Via HVAC Company' (*Krebs on Security*, 5 February 2014) <<https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/>> accessed 20 June 2022
- Burt J, 'Typosquat Supply Chain Attack Targets Go Developers' (*DevOps.com*, 5 February 2025) <<https://devops.com/typosquat-supply-chain-attack-targets-go-developers/>> accessed 18 September 2025
- Bygrave LA, 'The Emergence of EU Cybersecurity Law: A Tale of Lemons, Angst, Turf, Surf and Grey Boxes' (2025) 56 Computer Law & Security Review 106071
- Carnovale S and Yeniyurt S (eds), *Cyber Security and Supply Chain Management: Risks, Challenges and Solutions* (World Scientific 2021)

Chee FY, 'EU Plan to Phase-out High-Risk Tech Draws Fire from China's Huawei' *Reuters* (21 January 2026) <<https://www.reuters.com/business/media-telecom/eu-phase-out-high-risk-tech-targets-huawei-chinese-companies-2026-01-20/>> accessed 2 February 2026

Chiara PG, 'The IoT and the New EU Cybersecurity Regulatory Landscape' [2022] *International Review of Law, Computers & Technology* 1

—, 'Towards a Right to Cybersecurity in EU Law? The Challenges Ahead' (2024) 53 *Computer Law & Security Review* 105961

Cobbe J, 'Governance and Interdependence in Data-Driven Supply Chains' *Global Governance by Data: Infrastructures of Algorithmic Rule* (2026)

Cobbe J, Norval C and Singh J, 'What Lies beneath: Transparency in Online Service Supply Chains' (2020) 5 *Journal of Cyber Policy* 65

Cobbe J, Veale M and Singh J, 'Understanding Accountability in Algorithmic Supply Chains' *2023 ACM Conference on Fairness Accountability and Transparency* (ACM 2023)

Colonna L, 'The End of Open Source? Regulating Open Source under the Cyber Resilience Act and the New Product Liability Directive' (2025) 56 *Computer Law & Security Review* 106105

Commission, 'Impact Assessment Report Accompanying the Document Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity across the Union, Repealing Directive (EU) 2016/1148' SWD (2020) 345 final

—, '2025 State of the Union Address by the President' <https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH_25_2053> accessed 10 October 2025

—, 'Commission and National Authorities Urge SHEIN to Respect EU Consumer Protection Laws' <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1331> accessed 27 November 2025

Creazza A and others, 'Who Cares? Supply Chain Managers' Perceptions Regarding Cyber Supply Chain Risk Management in the Digital Transformation Era' (2022) 27 *Supply Chain Management: An International Journal* 30

Deb S, 'Smart Beds Helped Them Sleep on a Cloud. Then the Cloud Crashed.' *The New York Times* (24 October 2025) <<https://www.nytimes.com/2025/10/24/business/amazon-aws-outage-eight-sleep-mattress.html>> accessed 31 October 2025

EDPB, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR'

European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 'The EU's Cybersecurity Strategy for the Digital Decade' (2020) JOIN(2020) 18

European Union Agency for Cybersecurity and others, *Guidelines for Securing the Internet of Things – Secure Supply Chain for IoT* (European Network and Information Security Agency 2020)

——, *ENISA Threat Landscape 2021 – April 2020 to Mid-July 2021* (M Theocharidou and others eds, European Network and Information Security Agency 2021)

——, *ENISA Threat Landscape for Supply Chain Attacks* (A Malatras and others eds, European Network and Information Security Agency 2021)

Eurostat, '59% of EU Individuals Using Social Networks in 2023' (19 March 2024) <<https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20240319-1>> accessed 6 November 2025

——, 'Internet-Connected Devices Are Widely Used in the EU' (28 August 2025) <<https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20250828-2>> accessed 6 November 2025

Farrand B, Carrapico H and Turobov A, 'The New Geopolitics of EU Cybersecurity: Security, Economy and Sovereignty' (2024) 100 *International Affairs* 2379

Frenkel S, Bergman R and Saad H, 'How Israel Built a Modern-Day Trojan Horse: Exploding Pagers' *The New York Times* (18 September 2024) <<https://www.nytimes.com/2024/09/18/world/middleeast/israel-exploding-pagers-hezbollah.html>> accessed 20 January 2025

Friis K and Lysne O, 'Huawei, 5G and Security: Technological Limitations and Political Responses' (2021) 52 *Development and Change* 1174

Garvey MD, Samuel J and Kretinin A, 'An Ontology of Supply Chain Cybersecurity' in Steven Carnovale and Sengun Yenyurt (eds), *Cyber security and supply chain management: risks, challenges and solutions* (World Scientific 2021)

'German Parents Told to Destroy Cayla Dolls over Hacking Fears' *BBC News* (17 February 2017) <<https://www.bbc.com/news/world-europe-39002142>> accessed 28 October 2024

Goumagias N and others, 'Making Sense of the Internet of Things: A Critical Review of Internet of Things Definitions between 2005 and 2019' (2021) 31 *Internet Research* 1583

Graham E, 'Iranian Hackers Compromised a Federal Agency's Network, CISA and FBI Say' (*Nextgov.com*, 16 November 2022) <<https://www.nextgov.com/cybersecurity/2022/11/iranian-hackers-compromised-federal-agencys-network-cisa-and-fbi-say/379832/>> accessed 5 February 2026

Greenwald G, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (First Edition, Metropolitan Books/Henry Holt 2014)

Guihot M, 'Coherence in Technology Law' (2019) 11 *Law, Innovation and Technology* 311

Hawkins AJ, 'BMW Drops Plan to Charge a Monthly Fee for Heated Seats' (*The Verge*, 7 September 2023) <<https://www.theverge.com/2023/9/7/23863258/bmw-cancel-heated-seat-subscription-microtransaction>> accessed 19 November 2025

Hoepman J-H and Jacobs B, 'Increased Security through Open Source' (2007) 50 *Communications of the ACM* 79

Jacobs B, 'The Authenticity Crisis' (2024) 53 *Computer Law & Security Review* 105962

Jolly J and Milmo D, 'Inside the Jaguar Land Rover Hack: Stalled Smart Factories, Outsourced Cybersecurity and Supply Chain Woes' *The Guardian* (20 September 2025) <<https://www.theguardian.com/business/2025/sep/20/jaguar-land-rover-hack-factories-cybersecurity-jlr>> accessed 22 September 2025

Kamara I, 'European Cybersecurity Standardisation: A Tale of Two Solitudes in View of Europe's Cyber Resilience' (2024) 37 *Innovation: The European Journal of Social Science Research* 1441

Koops EJ, 'A Taxonomy for Descriptive Research in Law and Technology' in E Palmerini and E Stradella (eds), *Law and technology: The challenge of regulating technological* (Pisa University Press 2013)

Kwong JK and Pearlson K, 'Supply Chain Cybersecurity and Small and Medium-Sized Enterprises (SMEs): Exploring Shortcomings in Third Party Risk Management of SMEs' *Proceedings of the 57th Hawaii International Conference on System Sciences* 6656

Lambach D and Monsees L, 'Beyond Sovereignty as Authority: The Multiplicity of European Approaches to Digital Sovereignty' (2025) 4 *Global Political Economy* 71

Limaye Y, 'Fibre Optic Drones: The Terrifying New Weapon Changing the War in Ukraine' *BBC News* (28 May 2025) <<https://www.bbc.com/news/articles/ckgn47e5qyno>> accessed 3 December 2025

Lysne O, *The Huawei and Snowden Questions* (Springer International Publishing 2018)

Matwyshyn AM, 'CYBER!' (2017) 2017 *BYU Law Review* 1109

Melnyk SA and others, 'New Challenges in Supply Chain Management: Cybersecurity across the Supply Chain' (2022) 60 *International Journal of Production Research* 162

'Microsoft Didn't Cut Services to International Criminal Court, Its President Says' *POLITICO* (4 June 2025) <<https://www.politico.eu/article/microsoft-did-not-cut-services-international-criminal-court-president-american-sanctions-trump-tech-icc-amazon-google/>> accessed 29 October 2025

Millard C (ed), *Cloud Computing Law* (2nd edn, Oxford University Press 2021)

Nolte H, Rateike M and Finck M, 'Robustness and Cybersecurity in the EU Artificial Intelligence Act' *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency* (ACM 2025)

Nusselder S, 'Scrutinising the Interplay between Data Protection and Cybersecurity: A Paradox Shrouded Behind the "State-of-the-Art"' (2025) 11 *European Data Protection Law Review* 145

Radu R and Amon C, 'The Governance of 5G Infrastructure: Between Path Dependency and Risk-Based Approaches' (2021) 7 *Journal of Cybersecurity* 1

Roose K, 'Did One Guy Just Stop a Huge Cyberattack?' *The New York Times* (3 April 2024) <<https://www.nytimes.com/2024/04/03/technology/prevent-cyberattack-linux.html>> accessed 13 October 2025

Rosenzweig P, 'Cybersecurity and the Least Cost Avoider' [2013] *Lawfare* <<https://www.lawfaremedia.org/article/cybersecurity-and-least-cost-avoider>> accessed 28 November 2025

Samonas S and Coss D, 'The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security' (2014) 10 *Journal of Information System Security* 21

Schmitz-Berndt S and Chiara PG, 'One Step Ahead: Mapping the Italian and German Cybersecurity Laws against the Proposal for a NIS2 Directive' (2022) 3 *International Cybersecurity Law Review* 163

Schneier B, 'Backdoor in XZ Utils That Almost Happened' (*Schneier on Security*, 11 April 2024) <<https://www.schneier.com/blog/archives/2024/04/backdoor-in-xz-utils-that-almost-happened.html>> accessed 2 November 2025

Sharma A, 'Self-Propagating Supply Chain Attack Hits 187 Npm Packages' (*BleepingComputer*) <<https://www.bleepingcomputer.com/news/security/self-propagating-supply-chain-attack-hits-187-npm-packages/>> accessed 18 September 2025

Sheikh H, 'European Digital Sovereignty: A Layered Approach' (2022) 1 *Digital Society* 25

Shepardson D, 'US Agency Votes to Tighten Restrictions on Chinese Tech Companies Deemed Threats' *Reuters* (28 October 2025) <<https://www.reuters.com/business/media-telecom/us-agency-votes-tighten-restrictions-chinese-tech-companies-deemed-threats-2025-10-28/>> accessed 2 February 2026

Swain G, 'Wave of Npm Supply Chain Attacks Exposes Thousands of Enterprise Developer Credentials' (*InfoWorld*, 28 August 2025) <<https://www.infoworld.com/article/4047739/wave-of-npm-supply-chain-attacks-exposes-thousands-of-enterprise-developer-credentials.html>> accessed 18 September 2025

—, 'Massive Npm Supply Chain Attack Hits 18 Popular Packages with 2B Weekly Downloads' (*CSO Online*, 9 September 2025) <<https://www.csoonline.com/article/4053725/massive-npm-supply-chain-attack-hits-18-popular-packages-with-2b-weekly-downloads.html>> accessed 18 September 2025

Taekema S, 'Theoretical and Normative Frameworks for Legal Research: Putting Theory into Practice' [2018] Law and Method

Toulas B, 'Over 30% of Log4J Apps Use a Vulnerable Version of the Library' (*Bleeping-Computer*) <<https://www.bleepingcomputer.com/news/security/over-30-percent-of-log4j-apps-use-a-vulnerable-version-of-the-library/>> accessed 6 November 2025

Van Daalen O, *From Encryption to Quantum Computing: The Governance of Information Security and Human Rights*, vol 38 (TMC Asser Press 2025)

Vandezande N, 'Cybersecurity in the EU: How the NIS2-Directive Stacks up against Its Predecessor' (2024) 52 Computer Law & Security Review 105890

Veale M and Brown I, 'Cybersecurity' (2020) 9 Internet Policy Review

Zreikat AI and others, 'The Integration of the Internet of Things (IoT) Applications into 5G Networks: A Review and Analysis' (2025) 14 Computers 250

2.

The Regulation of Supply Chain Cybersecurity in the NIS2 Directive in the Context of the Internet of Things

This article was published in the European Journal of Law & Technology on 2 May 2024. The text was last revised on 30 April 2024, with some minor textual corrections for inclusion in this dissertation.

Mattis van 't Schip, 'The Regulation of Supply Chain Cybersecurity in the NIS2 Directive in the Context of the Internet of Things' (2024) 15 European Journal of Law & Technology.

Since the publication of this article, the European Commission adopted the NIS2 Implementing Regulation, which offers more extensive guidance on the meaning of 'supply chain security' for cybersecurity practitioners who are implementing the NIS2 risk management measures.

Abstract

An increasing number of actors design, develop and produce modern ICT products in a collaborative network: a supply chain. From a cybersecurity perspective, each actor brings new vulnerabilities for the entire chain and, in turn, the ICT product created by the chain. This problem should be addressed by supply chain cybersecurity, a type of cybersecurity policy that aims to prevent disruption of a supply chain's digital assets by internal or external actors. The EU Network and Information Systems (NIS2) Directive, which was adopted in 2023, introduces rules on supply chain cybersecurity for the network and information systems (e.g., Internet of Things devices) of entities in critical sectors (e.g., energy providers, hospitals). This article shows that the NIS2 Directive aligns closely with established risk management guidelines. Thus, the Directive, at first glance, offers a proper response to supply chain cybersecurity problems. However, the supply chain cybersecurity provisions are a missed opportunity: the provisions build on a flawed and limited understanding of the intricacies of supply chain cybersecurity in practice.

1 Introduction

The proliferation of Internet of Things (IoT) devices in industry and everyday life gives rise to new security threats. IoT devices incorporate hardware and software elements; a ‘smart’ watch can indicate the current time, like a traditional watch, and can send and receive text messages. Attackers increasingly focus on IoT devices as entry points, as their network connection allows for easy access to other resources and devices within the network.¹ IoT devices often operate with constrained functionalities and resources, as manufacturers aim to continuously bring new products to the market.² As a result, devices become vulnerable; producers do not make significant security investments for each device and software may not be kept up to date.³

In recent years, attackers have shifted their focus to attacks on supply chains, with specific attention to insecure IoT devices. A supply chain is a collaborative network of actors that, together, create, design and develop products and services for consumers.⁴ Attackers exploit vulnerabilities in the systems of one actor to subsequently attack a second, main target in the same supply chain.⁵ For instance, in the SolarWinds attack, attackers infiltrated a piece of software used by multinational companies for network management.⁶ The attackers used this initial infiltration to access systems of SolarWinds users and install malware; an estimated 18,000 SolarWinds costumers installed the malware update, including the United States Department of Homeland Security and Microsoft.⁷

Supply chain attacks and IoT devices are closely linked.⁸ Many organisations employ IoT devices to transmit, record and exchange data between supply chain partners; the IoT is thus an important driver of modern supply chains.⁹

-
- 1 European Union Agency for Cybersecurity, *Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures* (European Network and Information Security Agency 2017).
 - 2 Sunil Cheruvu et al., *Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment* (Apress 2020) 10–12.
 - 3 European Union Agency for Cybersecurity (n 1) 22–23.
 - 4 See more extensively John T Mentzer et al., ‘Defining Supply Chain Management’ (2001) 22 *Journal of Business Logistics* 1, 4.
 - 5 European Union Agency for Cybersecurity and A Malatras et al. (eds), *ENISA Threat Landscape for Supply Chain Attacks* (European Network and Information Security Agency 2021).
 - 6 Saheed Oladimeji and Sean Michael Kerner, ‘SolarWinds Hack Explained: Everything You Need to Know’ (*TechTarget*, 29 June 2022) <<https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know>> accessed 17 January 2024.
 - 7 *ibid.*
 - 8 European Union Agency for Cybersecurity et al., *Guidelines for Securing the Internet of Things – Secure Supply Chain for IoT* (European Network and Information Security Agency 2020); Sandor Boyson, Thomas M Corsi and John-Patrick Paraskevas, ‘Defending Digital Supply Chains: Evidence from a Decade-Long Research Program’ (2022) 118 *Technovation* 102380; Tope Omitola and Gary Wills, ‘Towards Mapping the Security Challenges of the Internet of Things (IoT) Supply Chain’ (2018) 126 *Procedia Computer Science* 441.
 - 9 Martin Serror et al., ‘Challenges and Opportunities in Securing the Industrial Internet of Things’ (2021) 17 *IEEE Transactions on Industrial Informatics* 2985.

At the same time, the supply chain of IoT devices regularly includes hundreds of actors,¹⁰ which means the chain has a broad and diverse attack surface.¹¹ A single weak link in this surface can be sufficient for an attack on the supply chain that produces IoT devices. Recently, for instance, threat actors attacked Indian critical infrastructure multiple times, including an attack on the largest Indian power company.¹² Microsoft found that the infrastructure providers used IoT devices which operated on a web server called Boa.¹³ The maintainers of this web server discontinued the project in 2005; the web server, today, contains various critical vulnerabilities which threat actors could exploit. The IoT is thus also a major target of supply chain attacks.

As a response to supply chain attacks, organisations now develop supply chain cybersecurity strategies. Supply chain cybersecurity aims to prevent disruption of a supply chain's digital assets by internal or external actors.¹⁴ Until recently, EU cybersecurity legislation did not explicitly require organisations to adopt supply chain cybersecurity measures or policies.¹⁵

In January 2023, a revision for the EU Network and Information Security (NIS) Directive of 2016, the NIS2 Directive, came in effect.¹⁶ The Directive aims to harmonise cybersecurity across critical sectors in the EU. Therefore, the NIS2 Directive introduces a cybersecurity risk management framework which includes supply chain cybersecurity rules. These rules primarily address entities in critical sectors (e.g., hospitals, energy providers) that employ network and information systems, including IoT devices (e.g., smart watches for patients). Therefore, the NIS2 Directive aims to mitigate supply chain attacks on systems used within critical sectors.

This article answers the following question: to what extent can the NIS2 supply chain cybersecurity rules help mitigate the emergence of supply chain cybersecurity

10 '2021 Apple Supplier List' (2020) <<https://www.apple.com/supplier-responsibility/pdf/Apple-Supplier-List.pdf>> accessed 13 June 2023.

11 European Union Agency for Cybersecurity (n 1) 22–23.

12 Ax Sharma, 'Hive Claims Ransomware Attack on Tata Power, Begins Leaking Data' (*BleepingComputer*, 25 October 2022) <<https://www.bleepingcomputer.com/news/security/hive-claims-ransomware-attack-on-tata-power-begins-leaking-data/>> accessed 18 January 2024.

13 Adam Castleman et al., 'Vulnerable SDK Components Lead to Supply Chain Risks in IoT and OT Environments' (*Microsoft Security Blog*, 22 November 2022) <<https://www.microsoft.com/en-us/security/blog/2022/11/22/vulnerable-sdk-components-lead-to-supply-chain-risks-in-iot-and-ot-environments/>> accessed 18 January 2024.

14 Myles D Garvey, Jim Samuel and Andrey Kretinin, 'An Ontology of Supply Chain Cybersecurity' in Steven Carnovale and Sengun Yeniyurt (eds), *Cyber security and supply chain management: risks, challenges and solutions* (World Scientific 2021) 106.

15 The cybersecurity legislation of some Member States did already include supply chain security, see Sandra Schmitz-Berndt and Pier Giorgio Chiara, 'One Step Ahead: Mapping the Italian and German Cybersecurity Laws against the Proposal for a NIS2 Directive' (2022) 3 *International Cybersecurity Law Review* 163; Kaspar Rosager Ludvigsen, Shishir Nagaraja and Angela Daly, 'Preventing or Mitigating Adversarial Supply Chain Attacks: A Legal Analysis' Proceedings of the 2022 ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses (ACM 2022).

16 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 (NIS2) [2022] OJ L333/80.

problems for IoT devices used in critical sectors? I argue that, at first glance, the NIS2 supply chain cybersecurity rules can indeed support the current regulatory landscape, as the Directive introduces a set of rules that cover a currently unregulated area of cybersecurity through a suitable risk-based approach. However, the logic of the supply chain cybersecurity measures in the NIS2 Directive is flawed. The Directive does not clearly define integral elements of supply chain cybersecurity, such as the role of the focal company, the governing company within a supply chain. The chosen approach might, therefore, not achieve the aim of mitigating supply chain cybersecurity problems.

This article proceeds as follows. In Section 2, I draw on existing literature in the field of supply chain risk management to indicate how current research frameworks rely on risk management concepts such as cyber resilience, cybersecurity investments, and standardisation to define supply chain cybersecurity. In Section 3, I set out the NIS2 Directive's scope and supply chain cybersecurity provisions. I compare these provisions to the limited role of supply chain cybersecurity in other EU cybersecurity legislation. In Section 4, I analyse the relevance of the NIS2 supply chain cybersecurity approach for the cybersecurity of IoT devices, based on the research frameworks analysed in Section 3. In Section 5, I examine how, regardless of its benefits, the NIS2 Directive cannot offer an effective legal avenue for supply chain cybersecurity rules, as evident by its absence of clear definitions and diffused allocation of responsibilities. Section 6 concludes.

2 Supply chain cybersecurity

Modern products consist of hundreds of software and hardware components. Software components have the most significant share in product supply chains; a single software package can integrate numerous other packages (e.g., open-source software). The software supply chain therefore consists of thousands of software components.

IoT devices are primary examples of modern ICT products with diverse software and hardware supply chains. A smart watch combines a traditional physical watch with a software operating system. Both the physical watch and the operating system rely on their own separate components to function (i.e., the battery and software packages respectively).¹⁷ The production process of a smart watch, therefore, consists of various manufacturers, software developers and component suppliers. This network of different co-operating actors expands the cyberattack surface of the smart watch; each actor brings their own IT systems, processes and employees. For each of these domains, cybersecurity vulnerabilities can exist, and threat actors can exploit those vulnerabilities to infiltrate the network.¹⁸ As a result, the cybersecurity of 'supply chains' – the network of actors and processes involved in the creation of a product – is receiving increasing attention.

17 'Apple Watch Teardown' (*iFixit*, 23 April 2015) <<https://www.ifixit.com/Teardown/Apple+Watch+Teardown/40655>> accessed 18 January 2024.

18 Hugh Boyes, 'Cybersecurity and Cyber-Resilient Supply Chains' (2015) *Technology Innovation Management Review* 7.

In this Section, I highlight how researchers in risk management studies are developing theories to operationalise supply chain cybersecurity. First, I examine the actors involved in modern supply chains. Second, I analyse the field of supply chain cybersecurity to find its most important characteristics, which I mainly derive from literature in the emerging field of cyber supply chain risk management.

2.1 The multi-tiered supply chain

The supply chain of an IoT device consists of ‘the actors, processes and assets that participate in the realisation (e.g., development, design, maintenance, patch management) of any IoT device.’¹⁹ Within this network of various actors, the focal company has a prominent role. Focal companies ‘usually (1) rule or govern the supply chain, (2) provide the direct contact to the customer, and (3) design the product or service offered.’²⁰ Apple, for instance, is the focal company in the supply chains for Apple Watches. The focal company carries the primary responsibility for the functioning of the supply chain. Focal companies thus also often govern and implement cybersecurity measures for the supply chain.

A supply chain consists of multiple tiers of suppliers that co-operate with the focal company. First-tier suppliers work directly with the focal company and are familiar to them. First-tier suppliers produce direct components for the devices, such as network chips, cameras and batteries, or develop main software operating systems and applications. In certain cases, first-tier suppliers assemble components into a final product for the focal company.

First-tier suppliers integrate components from lower-tier suppliers (e.g., a software component). Lower-tier suppliers co-operate with the tiers above them (e.g., a second-tier supplier with a first-tier supplier) and have an indirect relation with the focal company. Focal companies often struggle with governing those lower-tier suppliers due to the number of suppliers within all tiers of the supply chain.²¹ The focal company might, for instance, struggle with assessing the risks of cybersecurity incidents at lower-tier suppliers (e.g., vulnerabilities in components).²² Multi-tier supply chain management, the governance of all tiers of the supply chain, is thus an important task of the focal company.

The supply chain also includes the importer, distributor and the seller. They are the entities that ensure the product reaches the consumer. Often, factories worldwide create IoT devices, which means importers must bring the product to the EU market. The distributor transports the product to stores in the Union, where sellers offer the product to the consumer.

19 European Union Agency for Cybersecurity (n 8) 9.

20 Stefan Seuring and Martin Müller, ‘From a Literature Review to a Conceptual Framework for Sustainable Supply Chain Management’ (2008) 16 *Journal of Cleaner Production* 1699, 1699.

21 Liyuan Wang-Mlynek and Kai Foerstl, ‘Barriers to Multi-Tier Supply Chain Risk Management’ (2020) 31 *The International Journal of Logistics Management* 465.

22 Jason K Deane et al., ‘Managing Supply Chain Risk and Disruption from IT Security Incidents’ (2009) 2 *Operations Management Research* 4.

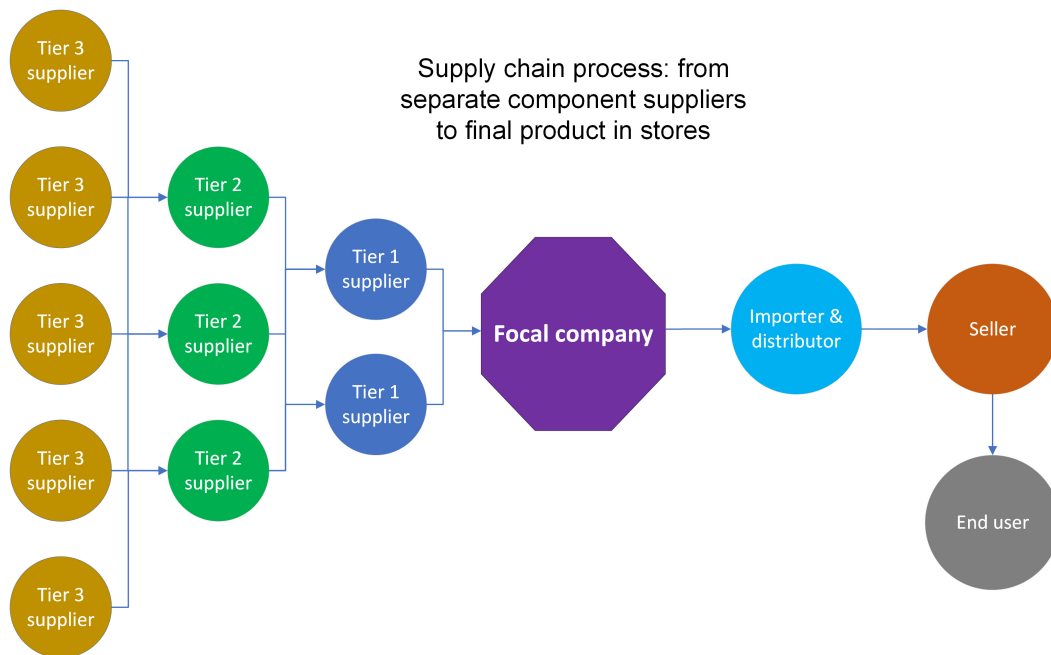


Figure 1: Multi-tier supply chain

Figure 1 illustrates a multi-tier software and hardware supply chain. Apple’s smart watch exemplifies this multi-tier supply chain well. Apple is the focal company that manages the supply chain and ensures that the development process runs smoothly. Foxconn, a Chinese company, manufactures the smart watches;²³ Foxconn is a prominent tier 1 supplier of Apple products.²⁴ Apple, through Foxconn, has multiple lower-tier suppliers (e.g., camera suppliers, battery suppliers). Together with the hardware supply chain, software suppliers ensure that the smart watch integrates an operating system with different functioning applications. After assembly, the watches are exported from China to, for example, the EU, where distributors bring the devices to sellers in stores. The end user, finally, is part of many ICT product supply chains, as they can return the device to the chain, or request maintenance.²⁵

23 Joe Rossignol, ‘Foxconn and Compal Will Reportedly Assemble “Apple Watch Series 6” Models Next Year’ (*MacRumors*) <<https://www.macrumors.com/2019/10/23/apple-watch-series-6-foxconn-compal/>> accessed 18 January 2024.

24 Jenny Chan, *Dying for an Iphone: Apple, Foxconn, and the Lives of China’s Workers* (Haymarket Books 2020).

25 This holistic view of the supply chain is often coined as the ‘end-to-end supply chain’. See <<https://supplychainmanagement.utk.edu/blog/end-to-end-supply-chain-planning/>> accessed 30 January 2024.

2.2 The developing field of supply chain cybersecurity

The multi-tiered supply chain highlights the various actors involved in a smart watch's production process. Supply chain cybersecurity measures aim to mitigate the diverse cybersecurity threats that each of these actors, with their own people, processes and technologies, can cause.²⁶

Research of supply chain cybersecurity remains limited to a few distinct fields, predominantly in risk management studies.²⁷ As a result of this recent emergence, Garvey et al. found that existing literature on supply chain cybersecurity does not define the concept clearly.²⁸ In turn, they offer their own definition of supply chain cybersecurity as 'the collection of strategies, policies, and processes that manage and mitigate against the possible loss of cyber assets and the possible subsequent disruption of any supply chain process that manifests as a result of the loss of a cyber asset.'²⁹

Under this definition, supply chain cybersecurity requires knowledge of the risks associated with the cyber assets that actors use in the supply chain (e.g., IoT devices). Such risks diverge between software and hardware components. The typical supply chain cybersecurity risk for hardware is hardware tampering, for example to create back doors, while for software, the risks mainly lie with software vulnerabilities in the numerous integrated software packages (e.g., as in the SolarWinds attack).³⁰ Supply chain cybersecurity is therefore a broad topic: many different actors across the supply chain must take cybersecurity measures and, as actors can vary significantly, supply chain cybersecurity covers a broad range of actor-tailored cybersecurity measures.³¹

Current theories on how to operationalise supply chain cybersecurity mainly stem from Cyber Supply Chain Risk Management (CSCRM) studies. This emerging field combines 'approaches, methods and practices from the fields of cybersecurity, enterprise risk management, and supply chain management.'³² CSCRM studies examine how organisations develop strategies and policies that prevent and mitigate cybersecurity threats to the supply chain.³³ Overall, three elements are highly prevalent in current CSCRM literature: 1) cyber resilience; 2) the required collaborative cybersecurity investments to achieve that resilience; and 3) the use of recognised

26 European Union Agency for Cybersecurity (n 5).

27 Arne Roar Nygård and Sokratis Katsikas, 'SoK: Combating Threats in the Digital Supply Chain', Proceedings of the 17th International Conference on Availability, Reliability and Security (ACM 2022).

28 Garvey, Samuel and Kretinin (n 14).

29 *ibid* 106.

30 Omitola and Wills (n 8).

31 See, e.g., the issue of sea piracy, which not all actors in the supply chain have to consider: Alexa K Sullivan, 'Piracy in the Horn of Africa and Its Effects on the Global Supply Chain' (2010) 3 *Journal of Transportation Security* 231.

32 Sandor Boyson, 'Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical IT Systems' (2014) 34 *Technovation* 342, 342.

33 *ibid*.

standards.³⁴ These three elements build upon each other: cyber resilience requires appropriate cybersecurity investments, while these investments are most efficient when the actors in the chain collaborate, which standardisation supports.

2.2.1 Cyber resilience

‘Cyber resilience’ refers to the capacity of the supply chain to recover after cyberattacks. Cyber resilience is therefore a component of cybersecurity. Without resilience, cyberattacks might interrupt the supply chain’s production process longer than necessary. Appropriate cyber resilience strategies ensure that the production processes can continue swiftly after an attack.

Boyes models the cyber resilience capacity of a supply chain along three perspectives: 1) the continuity of operations; 2) the control of access and system operations; 3) the quality and validity of information.³⁵ Cyber resilience therefore intertwines organisational and technical resilience measures. As Davis notes, cyber resilience ‘is a business issue and should be woven into business or enterprise risk management [and] it should be considered across all business operations.’³⁶ Cyber resilience is thus a combination of different business-specific requirements; a general approach for each supply chain does not exist. Therefore, each actor within the supply chain must examine what improvements they can make for their own organisation.

In supply chain risk management, cyber resilience is separate from cybersecurity.³⁷ Cyber resilience stems from the belief that insecurity is, as Bygrave notes, ‘a basic, inescapable condition of the digital world’.³⁸ In this context, cybersecurity and cyber resilience differ: cybersecurity strategies aim to prevent incidents, while cyber resilience strategies assume certain cybersecurity incidents are inescapable and, therefore, aim to ensure that services and processes can recover from security incidents. CSCRM theories specifically emphasise the need for cyber resilience to ensure supply chains can continue operations regardless of cyber threats.³⁹

However, modern cybersecurity practice does not clearly distinguish between cybersecurity and cyber resilience.⁴⁰ European cybersecurity law brings this lack of clarity to the fore, as it mainly promotes flexible security strategies (e.g., with ‘security-by-design’ policies).⁴¹ The transition from cybersecurity in supply chain risk *management* towards supply chain *regulation*, therefore, requires attention to both

34 Steven A Melnyk and others, ‘New Challenges in Supply Chain Management: Cybersecurity across the Supply Chain’ (2022) 60 *International Journal of Production Research* 162, 172–173. et al.

35 Boyes (n 18) 30.

36 Adrian Davis, ‘Building Cyber-Resilience into Supply Chains’ (2015) *Technology Innovation Management Review* 9, 24.

37 Fredrik Björck et al., ‘Cyber Resilience – Fundamentals for a Definition’ in Alvaro Rocha et al. (eds), *New Contributions in Information Systems and Technologies*, vol 353 (Springer International Publishing 2015).

38 Lee A Bygrave, ‘Cyber Resilience versus Cybersecurity as Legal Aspiration’, 14th International Conference on Cyber Conflict: Keep Moving! (CyCon) (2022) 29.

39 In line with the definition in Björck et al. (n 37) 312.

40 Bygrave (n 38).

41 *ibid.*

cybersecurity and cyber resilience. Supply chain cybersecurity in legislation thus usually integrates cyber resilience (as recovery measures) into a broad cybersecurity strategy that involves numerous other security measures (e.g., prevention, detection).

2.2.2 Collaborative cybersecurity investments

Creazza et al. refer to the relationship between cybersecurity investments and cyber resilience as ‘cyber supply chain balanced resilience’: a balanced approach between the cyber risks posed to the particular supply chain and the investments made to prevent those risks from impacting that chain.⁴² Cybersecurity investments balance the risk of cybersecurity breaches and its effects on the supply chain against the value of taking increased supply chain cybersecurity measures (e.g., stronger awareness campaigns or adopting new, more secure technologies).⁴³

With the balanced approach, managers of companies within the supply chain can invest in cybersecurity relative to the risks posed to their company. Generally, smaller suppliers might *want* to improve their overall cybersecurity, but simply lack the necessary knowledge or resources.⁴⁴ Cybersecurity investments therefore rely on the specific organisational capacities of each supply chain member. Larger organisations within the supply chain must thus also consider the risks posed to the network of actors when smaller organisations cannot sufficiently invest in cybersecurity. The focal company, for instance, might offer financial resources or cybersecurity awareness campaigns to smaller organisations. With these joint investments, the entire chain is more secure, instead of merely the actors that possess the financial or organisational means.⁴⁵

Finally, the supply chain profits from a balanced resilience investment approach as the benefits of the investments become more visible. If Supplier A and Supplier B make different cybersecurity investments, the benefits and pitfalls of both strategies are not visible to both suppliers.⁴⁶ Furthermore, suppliers cannot see the benefits of their investments for the overall security of the chain, thus reducing incentives to continue

42 Alessandro Creazza et al., ‘Who Cares? Supply Chain Managers’ Perceptions Regarding Cyber Supply Chain Risk Management in the Digital Transformation Era’ (2022) 27 *Supply Chain Management: An International Journal* 30, 32; Claudia Colicchia, Alessandro Creazza and David A Menachof, ‘Managing Cyber and Information Risks in Supply Chains: Insights from an Exploratory Analysis’ (2019) 24 *Supply Chain Management: An International Journal* 215, 234.

43 Tadeusz Sawik, ‘Balancing Cybersecurity in a Supply Chain under Direct and Indirect Cyber Risks’ (2022) 60 *International Journal of Production Research* 766.

44 Melnyk et al. (n 34) 173–174; Jillian K Kwong and Keri Pearlson, ‘Supply Chain Cybersecurity and Small and Medium-Sized Enterprises (SMEs): Exploring Shortcomings in Third Party Risk Management of SMEs’ (Proceedings of the 57th Hawaii International Conference on System Sciences, 2024) <https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/957a908a-cf71-47e7-84ac-ee3a2d8c088c/content> 3 January 2024; Davis (n 36).

45 Yanhui Li and Lu Xu, ‘Cybersecurity Investments in a Two-Echelon Supply Chain with Third-Party Risk Propagation’ (2021) 59 *International Journal of Production Research* 1216.

46 *ibid.*

investing.⁴⁷ A balanced and collaborative approach to cybersecurity investments is therefore crucial in improving the cybersecurity of the supply chain.

2.2.3 Standardisation

‘Standardisation’ refers to a set of guidelines that offer recommendations or requirements for specific processes, systems, services or products. Standards can support the improvement of the overall security level of the supply chain, by prescribing a framework for harmonisation of security throughout the chain.⁴⁸ The focal company can, for instance, mandate suppliers to adhere to certain security standards. Standard-setting bodies (e.g., the ISO) or the focal company can subsequently decide to audit the security of the supply chain according to the requirements of the standards.

However, standardisation comes with some uncertainties. First, many standards remain in development, especially in the field of supply chain cybersecurity.⁴⁹ Current standards often focus on individual risks, instead of on the interdependencies between organisations.⁵⁰ Before harmonised frameworks are possible, most organisations must wait for the standards to materialise. Second, standards can differ significantly per sector or even per organisation, which might impede efforts for cross-sector issues such as supply chain cybersecurity, which affects a diverse set of sectors.⁵¹ Finally, standards can sometimes give the impression of strong security *on paper*, while not necessarily improving security *in practice*.⁵² Proper standardisation is more than just checking certain boxes; instead, it requires the adoption of tangible organisational and technical change. Strong supply chain cybersecurity standardisation thus requires development of cross-sector standards that go beyond just ensuring strong security on paper; legislation, such as the NIS2 Directive, can stimulate such development.

In sum, supply chain cybersecurity is a rather novel field of study; at a wide, conceptual level, it requires that a broad set of actors within the supply chain adopt a diverse set of cybersecurity measures.

CSCRM researchers offer more precise guidance on how to implement these conceptual conditions. I examined three prevalent elements of this implementation. First, the supply chain must focus on improving its cyber resilience, as part of a broader cybersecurity strategy. Second, the chain must establish this strategy through

47 Yuhong Li et al., ‘Ripple Effect in the Supply Chain Network: Forward and Backward Disruption Propagation, Network Health and Firm Vulnerability’ (2021) 291 *European Journal of Operational Research* 1117.

48 Melnyk et al. (n 34) 173; Davis (n 36).

49 Abhijeet Ghadge et al., ‘Managing Cyber Risk in Supply Chains: A Review and Research Agenda’ (2019) 25 *Supply Chain Management: An International Journal* 223; Nygård and Katsikas (n 27).

50 Stefan Schauer, Nineta Polemi and Haralambos Mouratidis, ‘MITIGATE: A Dynamic Supply Chain Cyber Risk Assessment Methodology’ (2019) 12 *Journal of Transportation Security* 1.

51 Tania Wallis, Chris Johnson and Mohamed Khamis, ‘Interorganizational Cooperation in Supply Chain Cybersecurity: A Cross-Industry Study of the Effectiveness of the UK Implementation of the NIS Directive’ (2021) 48 *Information & Security: An International Journal* 36, 53–54.

52 Kwong and Pearson (n 44) 6660.

appropriate collaborative cybersecurity investments. Third, the use of harmonised standards should support baseline levels of security throughout the chain.

3 The NIS2 supply chain cybersecurity approach

The Network and Information Security Directive (NIS1) of 2016 was the EU's first fully cybersecurity-focused legislation.⁵³ The aim of NIS1 was to enhance cybersecurity across the EU, specifically by ensuring a high level of protection for network and information systems (e.g., IoT devices, communication networks).⁵⁴ To achieve this aim, NIS1 had three main tenets: 1) cross-border co-operation between Member States; 2) national cybersecurity strategies; and 3) national supervision of network and information systems used in critical sectors.

The scope of NIS1 covered several critical sectors (e.g., energy providers, hospitals). NIS1 aimed to improve the overall cybersecurity of those sectors, as disruptions in their services could prove especially critical.⁵⁵ Therefore, NIS1 obligated Member States to adopt national strategies and measures to improve the security of network and information systems. NIS1 divided entities in two categories: operators of essential services (e.g., electricity providers and hospitals);⁵⁶ and digital service providers (online marketplaces, search engines and cloud computing services).⁵⁷

Overall, NIS1 succeeded in making Member States introduce cybersecurity legislation that applied broadly across sectors, which brought more attention to the need for strong cybersecurity in those fields.⁵⁸ However, the Commission found that the NIS1 Directive could not fully cope with evolving cybersecurity threats and risks, due to the Directive's scope and enforcement mechanisms. These difficulties led to the Commission's NIS2 proposal.⁵⁹ NIS1 will be repealed after the transposition deadline of NIS2 in October 2024.⁶⁰

3.1 The scope of NIS2

NIS2 builds on some elements of NIS1. NIS2 still applies to the cybersecurity of a network and information system used by entities in several critical sectors. The definition of network and information systems does not differ from NIS1. IoT devices

53 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L194/1 (NIS1).

54 Recitals 1–3 NIS1 and Art 4(1) NIS1.

55 Recitals 1–3 NIS1.

56 Art 4(4) and Annex II NIS1.

57 Art 4(5), (6) and Annex III NIS1.

58 Wallis, Johnson and Khamis (n 51) 51.

59 Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 COM (2020) 823 final (NIS2).

60 Art 44 NIS2.

and other network and information systems (e.g., laptops) thus remain in scope of NIS2.

The two Directives have the same aim: to protect society from cybersecurity issues in the most critical sectors (e.g., energy, water supply).⁶¹ NIS2 applies to specific ‘essential’ and ‘important entities’, which build on the ‘operators of essential services’ and ‘digital service providers’ of NIS1 respectively.⁶²

NIS2 broadens the scope of entities from NIS1. Essential entities now include, inter alia, public administration entities.⁶³ The new category of important entities includes the manufacturing industry, a prominent user of ‘Industrial’ IoT devices (e.g., network-connected machinery).⁶⁴ The Industrial IoT devices exemplify the scope of NIS2: the devices are *network and information systems* that manufacturers, an *important entity*, use to provide their services.⁶⁵ Figure 2 illustrates this scope in more detail.

The Commission decided to exclude most small and micro-sized enterprises from the scope of NIS2.⁶⁶ This is for two reasons. First, the enforcement capabilities of Member States created a major issue in NIS1: Member States were not able to enforce the NIS1 obligations in a coherent manner as their identification of essential entities differed significantly (e.g., the minimum number of customers for water supply operators varied from 10,000 in one Member State to 500,000 in another).⁶⁷ If the Commission included small and micro-sized enterprises in the scope of NIS2, Member States would have to identify all relevant enterprises within the sectors of NIS2. This would create a significant administrative burden for the Member States, which would stand in the way of effective enforcement, according to the Commission.⁶⁸ Second, the Commission does not want to burden small and micro-sized enterprises with the significant security investments that compliance with the Directive could require.⁶⁹ I address the significance of this exclusion for supply chain cybersecurity in more detail in Section 5.1.

3.2 Supply chain cybersecurity provisions

NIS2 contains several obligations for the cybersecurity of supply chains. Two main actors are involved in these obligations: the Member States and the essential and important entities (henceforth ‘IoT-using entities’). The obligations do not explicitly

61 Art 1(1) and Recital 1 NIS2.

62 Art 2 NIS2.

63 Annex I(10) NIS2.

64 Annex II(5) NIS2.

65 See, e.g., the wording of Art 21 NIS2 and Section 3.2 below.

66 Art 2(1) NIS2; Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises [2003] OJ L124/36.

67 Commission, ‘Impact Assessment Report Accompanying the Document Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity across the Union, Repealing Directive (EU) 2016/1148’ SWD (2020) 345 final 23.

68 *ibid* 74.

69 *ibid* 73.

General scope of NIS2 supply chain cybersecurity measures for a single IoT device (e.g., Apple Watch) used by an entity (e.g., hospital)

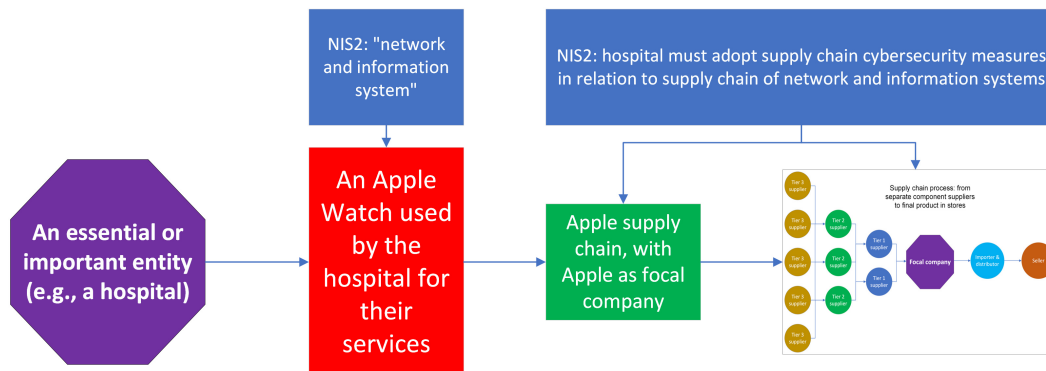


Figure 2: NIS2: general scope for supply chain cybersecurity provisions

address focal companies or suppliers.⁷⁰ NIS2 came in effect at the same time as the Digital Operational Resilience Act (DORA), which introduced similar rules – including supply chain cybersecurity rules – for financial institutions.⁷¹

Member States have a prominent role in guiding supply chain cybersecurity. First, they must adopt national policies which address supply chain cybersecurity (Article 7). Second, Member States must ensure that IoT-using entities adopt a cybersecurity risk management strategy, which includes supply chain cybersecurity measures (Article 21). Third, as part of a wider Coordination Group, together with the European Union Agency for Cybersecurity (ENISA) and the Commission, Member States must conduct risk assessments of the supply chains of particularly critical products used by IoT-using entities (Article 22).

Article 7(2)(a) requires Member States to adopt national policies that address the cybersecurity of supply chains. Since NIS1, all Member States have adopted such

⁷⁰ The focal company is addressed indirectly if it also manufactures its products. However, this condition does not apply to all focal companies, which means that only specific focal companies are indirectly addressed (as manufacturing IoT-using entities) by the provisions. The notion of a focal company, separately, does not exist in NIS2. See further Section 5.2.

⁷¹ Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 [2022] OJ L333/1. The DORA is a *lex specialis* for the banking sector, while NIS2 is a *lex generalis*. This article therefore focuses on NIS2.

national cybersecurity strategies.⁷² However, many of these strategies do not yet consider supply chain cybersecurity.⁷³ Pursuant to Article 7(2)(a), Member States must now state in their strategies how they will enhance supply chain cybersecurity for devices employed by essential and important entities. The exact policies might thus differ per Member State.

Article 21 prescribes a cybersecurity risk management approach for IoT-using entities. The entities must take appropriate and proportionate technical and organisational measures to manage supply chain risks. IoT-using entities must take the supply chain cybersecurity measures as part of an ‘all-hazard approach’, which requires attention to both technological (e.g., unauthorised access) and physical (e.g., theft and fire) environments.⁷⁴ Pursuant to Article 21, IoT-using entities must, as part of a broader supply chain cybersecurity strategy, assess the vulnerabilities of each of their *direct* suppliers or service providers.⁷⁵ The Directive does not explicitly identify which suppliers are understood as the direct suppliers of an IoT-using entity.

The IoT-using entities must conduct the supply chain risk assessment on the basis of the ‘overall quality of products and cybersecurity practices of their suppliers and service providers’.⁷⁶ Therefore, the entities cannot rely on generic risk assessments for the supply chains of the devices that they use; they must continuously adapt to the characteristics and risks of the particular supply chain. The essential and important entities (e.g., a hospital that uses medical IoT devices) must thus collaborate intensively with IoT-producing focal companies (e.g., a multinational such as Philips) and other direct suppliers. In Section 5.2, I analyse whether Article 21’s allocation of responsibilities is effective.

To support IoT-using entities in taking appropriate measures, Article 21 requires the entities to take into account European or internationally accepted standards relevant to the security of network and information systems (e.g., ISO standards). As illustrated earlier, such standards could theoretically contribute to harmonised supply chain cybersecurity measures throughout the IoT-producing chain, as each actor takes similar cybersecurity measures. The standards can thus support the collaboration Article 21(2)(d) requires.

Finally, Article 22(1) includes the option for co-ordinated risk assessments of supply chains. The Cooperation Group, which is composed of representatives of ENISA, the Commission and Member States,⁷⁷ can carry out assessments of critical ICT products

⁷² See for an overview of national security strategies: European Union Agency for Cybersecurity, ‘National Cyber Security Strategies – Interactive Map’ <<https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map>> accessed 30 January 2024.

⁷³ Germany has a substantial cybersecurity strategy, which also includes some references to supply chain cybersecurity; see Cyber Security Strategy for Germany 2021. Based on a quick survey, the term ‘supply chain’ (or ‘chain’) is not found in many other national strategies yet.

⁷⁴ Recital 79 NIS2.

⁷⁵ The European co-legislators added the condition for a direct relation; it did not exist in the initial Commission proposal.

⁷⁶ Art 21(3) NIS2.

⁷⁷ Art 14(3) NIS2.

and services for supply chains, based on technical and non-technical risk factors.⁷⁸ The Group can rely on several criteria in its decision to perform a risk assessment, including the importance of the ICT product for essential and important entities, the critical functions of the product, and the resilience of the overall supply chain against disruptive events.⁷⁹

The Directive requires supply chain cybersecurity measures from IoT-using entities with methods that strongly resemble cyber supply chain risk management. Figure 3 illustrates this framework. I will address the benefits of this approach for IoT cybersecurity in Section 4.

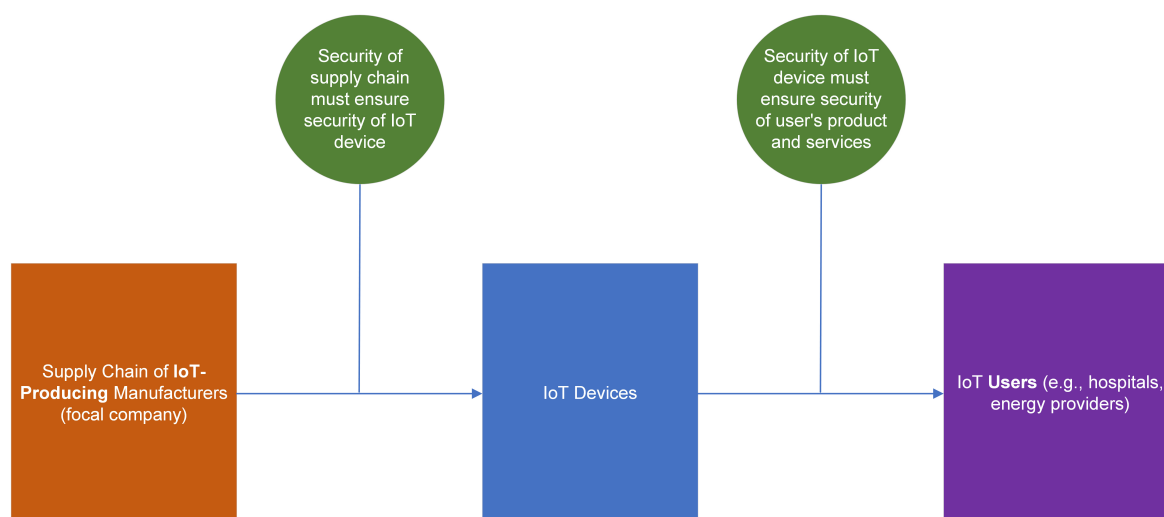


Figure 3: The supply chain cybersecurity process in the NIS2 Directive

3.3 The novelty of supply chain cybersecurity regulation

Supply chain cybersecurity rules did not exist in legislation prior to NIS2 and the Digital Operational Resilience Act. In this Section, I briefly highlight how these supply chain rules differ from security rules in existing (the General Data Protection

⁷⁸ Art 22(1) NIS2.

⁷⁹ Recital 91 NIS2.

Regulation) and forthcoming legislation (the Cyber Resilience Act).⁸⁰ I identify how the security provisions in this legislation differ from supply chain cybersecurity provisions, based on the two preconditions of supply chain cybersecurity from Section 2.2: rules must cover: 1) a variety of actors within the supply chain; and 2) a diverse set of cybersecurity measures, to ensure that actors take measures tailored to their organisation.

3.3.1 General Data Protection Regulation

The General Data Protection Regulation (GDPR) contains rules for the processing of personal data. In that context, the GDPR prescribes several cybersecurity requirements.

From a supply chain perspective, the main rule that emerges in the GDPR is the security of processing between the *controller* and the *processor*.⁸¹ The controller determines the means and purposes of personal data processing (e.g., Apple for their digital watches), while the processor is an actor employed *by the controller* for data processing (e.g., a cloud service).⁸² The controller and processor must securely process personal data, for example through the use of encryption measures.⁸³

The GDPR also includes an option for further ‘sub-processors’ hired by the initial processor, which means it allows for a layered chain of multiple data-processing actors.⁸⁴ In the supply chain context, this chain resembles the relationship between focal companies – the ‘controllers’ of the supply chain – and their multi-tiered suppliers. Therefore, the GDPR acknowledges the importance of cybersecurity rules that apply to different partners in a data processing activity.

At the same time, the GDPR has a limited approach, as it only applies to the actors that *process personal data*. These actors have suppliers (e.g., hardware component suppliers) that do not process personal data. The GDPR does not apply to those actors, even though they play a key role for the security of the personal data.⁸⁵

3.3.2 Cyber Resilience Act

The European Commission proposed the Cyber Resilience Act (CRA) in September 2022,⁸⁶ with the aim of introducing a comprehensive cybersecurity framework for ‘products with digital elements’, i.e., any software or hardware product.⁸⁷ The most

80 For a broader overview of the IoT cybersecurity regulatory landscape, see Pier Giorgio Chiara, ‘The IoT and the New EU Cybersecurity Regulatory Landscape’ (2022) *International Review of Law, Computers & Technology* 1.

81 Art 32 GDPR.

82 Art 4(7), (8) GDPR.

83 Art 32 GDPR.

84 Art 28(4) GDPR.

85 PTJ Wolters, ‘The Security of Personal Data under the GDPR: A Harmonized Duty or a Shared Responsibility?’ (2017) 7 *International Data Privacy Law* 165.

86 Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 COM (2022) 454 final (CRA).

87 Art 3(1) CRA.

recent version of the CRA is the compromise text of the Council and Parliament from December 2023.⁸⁸

The CRA is not the first product regulation to bring security requirements for the IoT. The Radio Equipment Directive (RED) applies to manufacturers, importers, and distributors of radio equipment that is brought to the EU market.⁸⁹ In a Delegated Regulation, the Commission determined that IoT devices are a specific category of radio equipment that must comply with certain requirements of the Directive.⁹⁰ The Directive requires IoT devices to contain security measures that prevent the device from harming its network resources or from violating the privacy and data protection of the end user.⁹¹ The CRA builds on the RED's security requirements and extends them to several different categories.⁹²

The CRA applies when a product is brought to the EU market;⁹³ therefore, manufacturers of products with digital elements are primarily responsible under the Act. The Act defines 'manufacturers' as natural or legal persons who *manufacture* or *develop* software or hardware products.⁹⁴ These developers or manufacturers must also market the product under their name or trademark. This 'marketing condition' means that, in supply chain terms, the CRA primarily applies to the focal company, not to all software developers and manufacturers within the supply chain. Importers, distributors and other natural persons have the same obligations as manufacturers when they act as a manufacturer (e.g., by bringing the product to the European market).

Products must comply with a broad set of cybersecurity requirements.⁹⁵ Security-by-design is a main component of those requirements; the Act requires that all products 'shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity'.⁹⁶ This security-by-design requirement implicitly covers supply chains, as design, development and production are all part of the supply chain process. However, the more extensive list of cybersecurity requirements in Annex I of the Act lacks an explicit reference to supply chain cybersecurity.

88 Council of the European Union, 'Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 – Letter sent to the European Parliament' [2023] 17000/23. ('CRA' in the footnotes refers to this compromise text.)

89 Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC [2014] OJ L153/26 (RED).

90 Commission Delegated Regulation (EU) 2022/30 of 29.10.2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive [2022] OJ L7/6.

91 Art 3(3) RED.

92 Recital 15 CRA.

93 Art 1 CRA.

94 Art 3(18) CRA.

95 Art 5(1) and Annex I CRA.

96 Art 1(1) Annex I CRA.

The requirements therefore only serve supply chain cybersecurity by independently supporting the overall cybersecurity of software and hardware.⁹⁷

Article 10 lists several separate obligations for manufacturers. One obligation does seem to refer to supply chain cybersecurity, as manufacturers must ‘exercise due diligence when integrating components sourced from third parties in [their products]’.⁹⁸ In addition, manufacturers must ensure that the components do not compromise the security of their end product.⁹⁹ This obligation requires a certain level of attention to the manufacturer’s supply chain. However, acting with ‘due diligence’ is a rather open-ended obligation. Nonetheless, the Act requires a certain level of attention to secure design, development and integration of components.

3.3.3 Current legislation in comparison to NIS2

The NIS2 Directive, when compared to similar legislation, requires more explicit and comprehensive supply chain cybersecurity measures from IoT-using entities. Similar pieces of legislation mainly lack the preconditions of supply chain cybersecurity: their scopes are limited to certain actors within the supply chain and those actors are responsible for certain specific cybersecurity measures. Table 1 summarises these problems for the GDPR and the CRA.¹⁰⁰

Table 1: The lack of supply chain cybersecurity provisions in current EU cybersecurity legislation

Scope	GDPR	CRA (compromise text)
Supply chain actors in scope	Processors of personal data (e.g., software developers, cloud providers).	Manufacturers and developers, importers, distributors, other persons acting as manufacturer, when they market the product under their name.
Cybersecurity measures in scope	Only cybersecurity measures required for secure processing of personal data.	Various cybersecurity measures, including security-by-design and secure integration of components. Intended as independent cybersecurity components that support overall supply chain cybersecurity.

⁹⁷ Recital 8 CRA.

⁹⁸ Art 10(4) CRA.

⁹⁹ *ibid.*

¹⁰⁰ See also about national legal approaches to supply chain cybersecurity: Ludvigsen, Nagaraja and Daly (n 15).

Scope	GDPR	CRA (compromise text)
Tangible supply chain cybersecurity measures	No, scope of actors and measures restricted to personal data processing.	Scope of actors restricted mainly to focal companies. Security-by-design and secure integration of components indicate growing concern for supply chain cybersecurity at EU level.

NIS2 does regulate supply chain cybersecurity: it covers all *direct* suppliers and service providers of entities, without discerning between the activities of the suppliers. It also requires an all-hazard approach: supply chain cybersecurity is an element of broader cybersecurity risk management.

4 NIS2 Cyber Supply Chain Risk Management

NIS2 approaches supply chain cybersecurity through a risk management lens; some elements of this legal approach therefore coincide with the frameworks developed in CSCRM studies. NIS2, too, integrates efforts to improve cyber resilience with attention to cyber investments and standardisation. I briefly review below the integration of these three elements to place the NIS2 provisions in a supply chain management context.

4.1 Addressing cyber resilience within cybersecurity

NIS2 requires IoT-using entities to take an all-hazard approach to, inter alia, preventing cyberattacks from impacting their services,¹⁰¹ employing both technological and physical protection of network and information systems to achieve this.¹⁰²

It also requires IoT-using entities to address cyber resilience within their cybersecurity risk management. The entities must aim to ensure that recipients of their services (e.g., patients in a hospital) do not encounter the effects of a cyberattack.¹⁰³ This mitigation of effects is inherent to a cyber resilient organisation: if an attack happens, the organisation must swiftly recover and prevent further problems. In the specific context of supply chain cybersecurity, NIS2 further confirms this aim, stating that IoT-using entities should specifically assess the resilience of products and services of their

¹⁰¹ Art 21(1) NIS2.

¹⁰² Recital 79 NIS2: ‘The cybersecurity risk-management measures should therefore also address the physical and environmental security of network and information systems by including measures to protect such systems from system failures, human error, malicious acts or natural phenomena.’

¹⁰³ Art 21(1) NIS2: ‘entities take [...] measures [...] to prevent or minimise the impact of incidents on recipients of their services’.

suppliers.¹⁰⁴ Resilience is also a key element for the risk assessment of critical products by the Coordination Group.¹⁰⁵ Cyber resilience, therefore, has a prominent role in the flexible NIS2 cybersecurity risk management approach.

4.2 Collaborative cybersecurity investments

NIS2 aims to incentivise the IoT-using entities to make cybersecurity investments, as it suggests the integration of cybersecurity risk management in the contractual arrangements between the entities and the suppliers of their devices.¹⁰⁶ To comply with these arrangements, IoT-producing actors may need adequate supply chain cybersecurity to continue their product sales.

The actual efficacy of NIS2 on the cybersecurity investments by IoT-producing organisations strongly depends on several conditions. First, as Woods and Ceross highlight, the question remains whether organisations invest to improve their security practices or merely to prevent legal risks associated with non-compliance.¹⁰⁷ Further, the effects of any regulation-induced cybersecurity investment rely on the specific capabilities and security practices of each organisation and their existing resource allocations.¹⁰⁸

To support proper resource allocation, NIS2 places responsibility for cybersecurity governance with the management bodies of IoT-using entities.¹⁰⁹ Management bodies must, for instance, approve the implementation of the cybersecurity risk framework of Article 21. Article 20(1) also requires Member States to implement provisions that can hold the management bodies liable for infringements of Article 21. In addition, management bodies must follow cybersecurity training, so that they are able to identify and assess cybersecurity risks in their organisation.¹¹⁰ Given these responsibilities, management bodies are directly involved in cybersecurity risk management and might therefore more quickly acknowledge the necessity of proper cybersecurity investments.¹¹¹

104 Recital 85 NIS2.

105 Recital 91 NIS2.

106 Recital 85 NIS2: ‘Essential and important entities should in particular be encouraged to incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers.’ This contract management could even cover other suppliers than the direct supplier, as Recital 85 further states: ‘Those entities could consider risks stemming from other levels of suppliers and service providers.’

107 Daniel W Woods and Aaron Ceross, ‘Blessed Are The Lawyers, For They Shall Inherit Cybersecurity’ Proceedings of the 2021 New Security Paradigms Workshop (Association for Computing Machinery 2022).

108 Lawrence A Gordon et al., ‘Increasing Cybersecurity Investments in Private Sector Firms’ (2015) *Journal of Cybersecurity* 3.

109 Art 20(1) NIS2.

110 Art 20(2) NIS2.

111 Niels Vandezande, ‘Cybersecurity in the EU: How the NIS2-Directive Stacks up against Its Predecessor’ (2024) 52 *Computer Law & Security Review* 105890, 7–8.

4.3 Standardisation

NIS2 supports the integration of security standards in supply chain management in several ways.

First, Article 21 specifically notes that IoT-using entities must take European and international standards into account as part of their cybersecurity risk management. The supply chain cybersecurity measures should thus, where feasible, stem from European or international security standards.¹¹²

Second, NIS2 requires the Commission, ENISA and Member States to promote the use of standards.¹¹³ Moreover, this group must take an active role in maintaining relations with standard-setting bodies and in fostering opportunities for future co-operation.¹¹⁴ Standards are therefore key components of NIS2's cybersecurity framework.

5 Supply chain cybersecurity beyond NIS2: perfecting the approach

The introduction of supply chain cybersecurity regulation in NIS2 offers, at first glance, a proper response to supply chain cybersecurity threats. At the same time, supply chain cybersecurity only has a limited role in NIS2, as a component of a broader risk management approach.

In this Section, I highlight two emerging problems from the limited role of supply chain cybersecurity in NIS: first, an overall lack of clear definitions about supply chains and supply chain cybersecurity; second, the focus of NIS2 on the IoT-using entity, instead of the focal company.

As a result of both problems, NIS2 is most beneficial for supply chain cybersecurity if the European legislators utilise it as groundwork for further, concentrated supply chain cybersecurity regulation.

5.1 What is supply chain cybersecurity?

Recent literature reviews indicate an overall lack of clear definitions within the supply chain cybersecurity field.¹¹⁵ NIS2 suffers from similar problems: it lacks distinct definitions for the 'supply chain' and, as a result, for 'supply chain cybersecurity'. This is surprising, given the comprehensive attention paid to 'ICT third-party risks' in the Digital Operational Resilience Act (DORA).¹¹⁶ The question, therefore, is if NIS2,

112 Art 21(1) NIS2: 'Taking into account the state-of-the-art and, where applicable, relevant European and international standards, the [security] measures shall ensure a level of security [...] appropriate to the risks posed.'

113 Art 25(1) and Recital 80 NIS2.

114 Art 25 and Recital 59.

115 Garvey, Samuel and Kretinin (n 14); Melnyk et al. (n 34); Colicchia, Creazza and Menachof (n 42).

116 See Ch V DORA.

with its much broader scope than the DORA, can still offer effective supply chain cybersecurity measures.

The lack of clear supply chain-related definitions leads to several questions about the *intent* of NIS2. For instance, it explicitly excludes small and micro-sized enterprises from its scope. The Commission did not want to burden these enterprises with extensive cybersecurity investments.¹¹⁷ However, virtually all companies in the EU are small enterprises.¹¹⁸ Small and micro-sized enterprises are, therefore, part of nearly all supply chains, as they offer niche services or products (e.g., a camera component supplier).¹¹⁹ It is therefore hardly imaginable that these enterprises would be left out of the scope of NIS2's prescribed supply chain cybersecurity measures. A clear definition of the supply chain would contribute to answering questions about the type of actors, in particular the 'direct suppliers', that IoT-using entities must adopt measures for.

Additionally, NIS2 does not indicate the *type* of security measures that 'supply chain security' requires. For instance, it states that the all-hazard risk management approach must include 'supply chain security, *including* security-related aspects concerning the relationships between each entity and its direct suppliers or service providers'.¹²⁰ It thus primarily requires 'supply chain security', which includes measures for 'security-related aspects' concerning relationships between entities and suppliers. However, the use of 'including' also leaves room for other types of measures. Therefore, supply chain cybersecurity under NIS2 can consist of an extensive array of cybersecurity measures (e.g., preventing hardware tampering, addressing software vulnerabilities).

Transport security illustrates the issues with such an extensive array of possible measures. International shipping companies can, to a certain extent, prevent piracy by reducing the information that is digitally available about their ships and crew, a type of online privacy management.¹²¹ Under the abstract terms of NIS2, entities might interpret that such cargo privacy management measures are required. Such flexible interpretations have two sides: the entities might opt to take considerable security measures; however, the flexible terms of NIS2 leave room for minimally compliant measures, especially as supply chain cybersecurity is still a developing field without clear guidance from, for instance, supervisory authorities.¹²²

Furthermore, NIS2 lacks a definition of the *extent* of the supply chain cybersecurity process. Supply chain cybersecurity can begin and end at different points during the production process, depending on the chosen approach. The Council of the

117 Commission (n 67) 73.

118 'Small and Medium-Sized Enterprises: An Overview' <<https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20200514-1>> accessed 30 January 2024.

119 Melnyk et al. (n 34) 171; Kwong and Pearlson (n 44).

120 Art 21(2)(d) NIS.

121 Sullivan (n 31) 241.

122 Consider here, for instance, the overall lack of compliance with the GDPR, which stemmed from a longer line of existing data protection law and benefited, therefore, from guidance from supervisory authorities (the old Article 29 Working Party, now the European Data Protection Board). Supply chain cybersecurity does not yet enjoy such a firm status. See on the GDPR, Claudia Quelle, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-Based Approach' (2018) 9 *European Journal of Risk Regulation* 502.

EU, for instance, notes that supply chain cybersecurity ‘begins with the sourcing of raw material and extends through the manufacturing, processing, handling and delivery of ICT products and services, including provision of support during ICT products and services’ life cycle’.¹²³ Under this definition, IoT-using entities could require continuous security updates as part of supply chain cybersecurity, as such updates are part of the ‘provision of support’ during the lifecycle of the IoT device.¹²⁴ Such continuous support ensures that vulnerabilities in the IoT device’s software are quickly patched, thus significantly reducing the possibility of cyberattacks. However, NIS2 does not indicate whether such support is part of its envisioned supply chain cybersecurity measures. Again, the lack of a distinct definition leaves entities with considerable interpretative leeway.

Supply chain cybersecurity in NIS2 is one element of broader cybersecurity risk management. As a result of this auxiliary role, NIS2 does not (and cannot) sufficiently define the integral components of supply chain cybersecurity. Supply chain cybersecurity remains a complex, multidisciplinary field in development; the limited regard for its intricacies in NIS2, therefore, might decrease the efficacy of the chosen measures.

5.2 The right responsibility in the wrong hands

The focal company generally governs the supply chain. The company is primarily responsible for the overall level of cybersecurity of the supply chain, for instance by requiring that new suppliers adhere to a set of security standards or best practices.¹²⁵ The focal company can properly take these measures as it stands in direct relation to first-tier suppliers. As described earlier, this collaboration is essential for proper supply chain cybersecurity.

Article 21 NIS2 does not build on these capabilities of the focal company. The provision requires IoT-using entities to take security measures, not the focal companies (i.e., IoT manufacturers) themselves. Figure 4 illustrates this hierarchy of responsibilities under Article 21.

The allocation of responsibilities in Article 21 lacks regard for the diversity of supply chain actors. Focal companies are as diverse as the supply chains they manage. Frostenson and Prenkert highlight how focal companies often operate in complex networks of multiple legal entities and ownership models.¹²⁶ The IoT-using entities under NIS2 are equally diverse, ranging from energy providers to the health sector. The responsibilities under Article 21, therefore, become increasingly complex. The IoT-using entities must take appropriate measures, then communicate them with the focal company or network of companies of each IoT device they use. Although NIS2 only

123 Council of the European Union, ‘Council Conclusions on ICT Supply Chain Security’ (2022) 13664/22 4.

124 European Union Agency for Cybersecurity (n 8) 17.

125 Melnyk et al. (n 34) 173.

126 Magnus Frostenson and Frans Prenkert, ‘Sustainable Supply Chain Management When Focal Firms Are Complex: A Network Perspective’ (2015) 107 *Journal of Cleaner Production* 85.

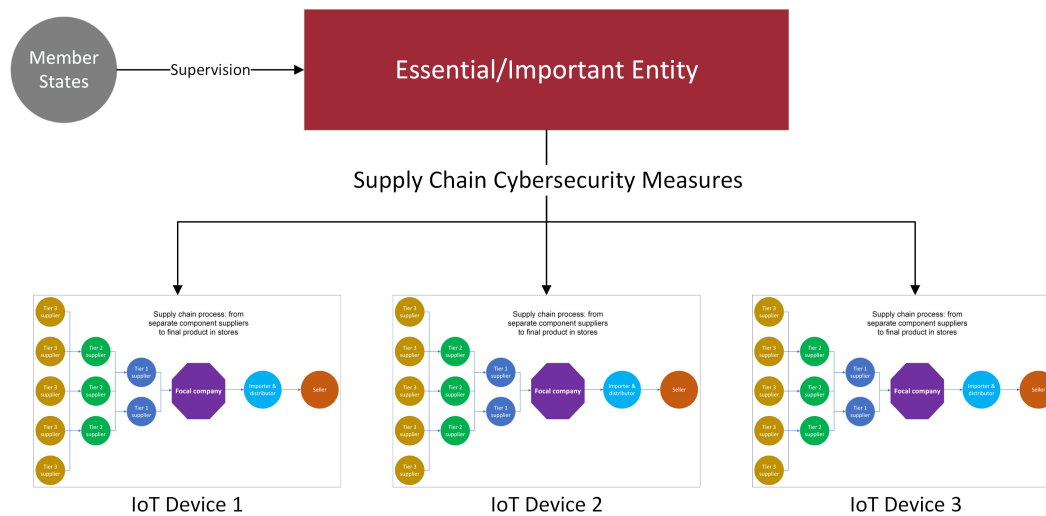


Figure 4: NIS2: allocation of responsibilities

requires the IoT-using entity to take measures in relation to its direct suppliers, these diverse direct suppliers (e.g., the focal company) must inevitably collaborate with their own suppliers for effective cybersecurity throughout the chain. This complex process does not seem practically feasible to ensure effective supply chain cybersecurity measures.

The allocation of responsibilities in NIS2 resembles the controller–processor relationship in the GDPR, as illustrated in Section 3.3. The approach in the GDPR is to keep the responsibilities with the controller as they supervise and direct the personal data processing.¹²⁷ However, privacy scholars often posit that practice does not clearly distinguish between controller and processor.¹²⁸ For instance, in cloud processing, the power of the cloud processor (e.g., Google) is often much larger than the controller that employs the cloud service (e.g., a small school).¹²⁹ The question, in that case, is whether the controller (i.e., the IoT-using entity under NIS2) should implement the data protection measures, or the cloud service as the processor (i.e., the focal company). Data protection law must protect the data subject, i.e., the individual whose data is processed. From this perspective, it is logical to ensure that the most capable entity implements the data protection measures, whether that is the controller or the

¹²⁷ EDPB, ‘Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR’ 11.

¹²⁸ Peter Blume, ‘An Alternative Model for Data Protection Law: Changing the Roles of Controller and Processor’ (2015) 5 *International Data Privacy Law* 292; Wolters (n 85).

¹²⁹ *ibid* 296.

processor. Google, as the processor that provides a cloud service, is presumably more capable of implementing those measures.

The law, too, should place the responsibilities of supply chain cybersecurity where they are most effective for the cybersecurity of ICT products. An alternative approach to supply chain cybersecurity, outside of NIS2, is required for this shift towards effective supply chain cybersecurity responsibilities. A stronger position for supply chain cybersecurity in product safety law, which focuses on the manufacturer instead of the user, could, in this context, offer a more effective legal framework. NIS2 thus offers a solid introduction to supply chain cybersecurity regulation, but its rules are best served as groundwork for further legislation.

6 Conclusion

NIS2 came into effect in January 2023. It introduces a set of rules aimed at the previously unregulated area of supply chain cybersecurity, which offers a response to the growing number of cyberattacks aimed at the most vulnerable partner in a co-operating network of actors. Supply chain cybersecurity is therefore closely connected to the increasing use of IoT devices, which allow data exchange between many different systems and sensors. In this article, I have sought to answer the following question: to what extent can the NIS2 supply chain cybersecurity rules help mitigate the emergence of supply chain cybersecurity problems in IoT devices used in critical sectors?

Supply chain cybersecurity is a rather novel field, with a distinct lack of definitions. A general concept of supply chain cybersecurity often requires the diverse set of actors in the supply chain, regardless of their operations, to take cybersecurity measures tailored to their organisation to protect the overall security of the supply chain.

Novel studies in the field of CSCRM offer prominent components of supply chain cybersecurity. First, organisations must focus on cyber *resilience*, i.e., the capacity of an organisation to recover after a cyberattack, as a component of cybersecurity. Second, organisations can build cyber resilience in close collaboration with partners throughout the chain, to ensure appropriate cybersecurity *investments*. Third, cybersecurity *standards* can strongly support a harmonised, collaborative approach.

NIS2 addresses ‘essential’ and ‘important’ entities, which offer critical services (e.g., hospitals, energy providers). Under NIS2, these entities must take a cybersecurity risk management approach to ensure that the network and information systems they use (e.g., IoT devices) are secure. Under this approach, they must, inter alia, focus on supply chain cybersecurity. This requirement is new in European cybersecurity law. The GDPR and the upcoming CRA, for instance, do cover respective actors in the chain and some specific cybersecurity measures, but their scope is too narrow for proper supply chain cybersecurity.

NIS2 approaches supply chain cybersecurity through an apt risk management framework. The three components of recent CSCRM studies – cyber resilience,

cybersecurity investments and standardisation – form important pillars within NIS2. The supply chain cybersecurity rules in NIS2 are thus grounded on a proper risk management approach.

However, supply chain cybersecurity has only a lateral role within this risk management approach. NIS2 simply requires ‘supply chain security’ measures, which lacks awareness of the multi-faceted nature of supply chains and supply chain cybersecurity measures. In addition, it places the responsibility for supply chain cybersecurity measures on the *end user* of the IoT device (e.g., the hospital). Legislation should instead require the focal company (i.e., the IoT vendor) to maintain a secure supply chain, for instance in product-focused legislation. Future legislation should thus build on the solid groundwork of NIS2, but offer more clearly defined, concentrated supply chain cybersecurity measures aimed at the focal company.

References

- '2021 Apple Supplier List' (2020) <<https://www.apple.com/supplier-responsibility/pdf/Apple-Supplier-List.pdf>>
- 'Apple Watch Teardown' (*iFixit*, 23 April 2015) <<https://www.ifixit.com/Teardown/Apple+Watch+Teardown/40655>> accessed 18 January 2024
- Björck F and others, 'Cyber Resilience – Fundamentals for a Definition' in Alvaro Rocha and others (eds), *New Contributions in Information Systems and Technologies*, vol 353 (Springer International Publishing 2015)
- Blume P, 'An Alternative Model for Data Protection Law: Changing the Roles of Controller and Processor' (2015) 5 *International Data Privacy Law* 292
- Boyes H, 'Cybersecurity and Cyber-Resilient Supply Chains' [2015] *Technology Innovation Management Review* 7
- Boyson S, 'Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical IT Systems' (2014) 34 *Technovation* 342
- Boyson S, Corsi TM and Paraskevas J-P, 'Defending Digital Supply Chains: Evidence from a Decade-Long Research Program' (2022) 118 *Technovation* 102380
- Bygrave LA, 'Cyber Resilience versus Cybersecurity as Legal Aspiration', 2022 14th *International Conference on Cyber Conflict: Keep Moving! (CyCon)* (2022)
- Castleman A and others, 'Vulnerable SDK Components Lead to Supply Chain Risks in IoT and OT Environments' (*Microsoft Security Blog*, 22 November 2022) <<https://www.microsoft.com/en-us/security/blog/2022/11/22/vulnerable-sdk-components-lead-to-supply-chain-risks-in-iot-and-ot-environments/>> accessed 18 January 2024
- Chan J, *Dying for an Iphone: Apple, Foxconn, and the Lives of China's Workers* (Haymarket Books 2020)
- Cheruvu S and others, *Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment* (Apress 2020)
- Chiara PG, 'The IoT and the New EU Cybersecurity Regulatory Landscape' [2022] *International Review of Law, Computers & Technology* 1
- Colicchia C, Creazza A and Menachof DA, 'Managing Cyber and Information Risks in Supply Chains: Insights from an Exploratory Analysis' (2019) 24 *Supply Chain Management: An International Journal* 215
- Commission, 'Impact Assessment Report Accompanying the Document Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity across the Union, Repealing Directive (EU) 2016/1148' SWD (2020) 345 final

Council of the European Union, 'Council Conclusions on ICT Supply Chain Security' (2022) 13664/22

Creazza A and others, 'Who Cares? Supply Chain Managers' Perceptions Regarding Cyber Supply Chain Risk Management in the Digital Transformation Era' (2022) 27 Supply Chain Management: An International Journal 30

Davis A, 'Building Cyber-Resilience into Supply Chains' [2015] Technology Innovation Management Review 9

Deane JK and others, 'Managing Supply Chain Risk and Disruption from IT Security Incidents' (2009) 2 Operations Management Research 4

EDPB, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR'

European Union Agency for Cybersecurity, *Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures* (European Network and Information Security Agency 2017)

——, *Guidelines for Securing the Internet of Things – Secure Supply Chain for IoT* (European Network and Information Security Agency 2020)

——, *ENISA Threat Landscape for Supply Chain Attacks* (A Malatras and others eds, European Network and Information Security Agency 2021)

Frostenson M and Prenkert F, 'Sustainable Supply Chain Management When Focal Firms Are Complex: A Network Perspective' (2015) 107 Journal of Cleaner Production 85

Garvey MD, Samuel J and Kretinin A, 'An Ontology of Supply Chain Cybersecurity' in Steven Carnovale and Sengun Yeniyurt (eds), *Cyber security and supply chain management: risks, challenges and solutions* (World Scientific 2021)

Ghadge A and others, 'Managing Cyber Risk in Supply Chains: A Review and Research Agenda' (2019) 25 Supply Chain Management: An International Journal 223

Gordon LA and others, 'Increasing Cybersecurity Investments in Private Sector Firms' [2015] Journal of Cybersecurity 3

Kwong JK and Pearlson K, 'Supply Chain Cybersecurity and Small and Medium-Sized Enterprises (SMEs): Exploring Shortcomings in Third Party Risk Management of SMEs' Proceedings of the 57th Hawaii International Conference on System Sciences 6656

Li Y and others, 'Ripple Effect in the Supply Chain Network: Forward and Backward Disruption Propagation, Network Health and Firm Vulnerability' (2021) 291 European Journal of Operational Research 1117

Li Y and Xu L, 'Cybersecurity Investments in a Two-Echelon Supply Chain with Third-Party Risk Propagation' (2021) 59 International Journal of Production Research 1216

Ludvigsen KR, Nagaraja S and Daly A, 'Preventing or Mitigating Adversarial Supply Chain Attacks: A Legal Analysis', *Proceedings of the 2022 ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses* (ACM 2022)

Melnyk SA and others, 'New Challenges in Supply Chain Management: Cybersecurity across the Supply Chain' (2022) 60 *International Journal of Production Research* 162

Mentzer JT and others, 'Defining Supply Chain Management' (2001) 22 *Journal of Business Logistics* 1

Nygård AR and Katsikas S, 'SoK: Combating Threats in the Digital Supply Chain', *Proceedings of the 17th International Conference on Availability, Reliability and Security* (ACM 2022)

Oladimeji S and Kerner SM, 'SolarWinds Hack Explained: Everything You Need to Know' (*TechTarget*, 29 June 2022) <<https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know>> accessed 17 January 2024

Omitola T and Wills G, 'Towards Mapping the Security Challenges of the Internet of Things (IoT) Supply Chain' (2018) 126 *Procedia Computer Science* 441

Quelle C, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-Based Approach' (2018) 9 *European Journal of Risk Regulation* 502

Rossignol J, 'Foxconn and Compal Will Reportedly Assemble "Apple Watch Series 6" Models Next Year' (*MacRumors*) <<https://www.macrumors.com/2019/10/23/apple-watch-series-6-foxconn-compal/>> accessed 18 January 2024

Sawik T, 'Balancing Cybersecurity in a Supply Chain under Direct and Indirect Cyber Risks' (2022) 60 *International Journal of Production Research* 766

Schauer S, Polemi N and Mouratidis H, 'MITIGATE: A Dynamic Supply Chain Cyber Risk Assessment Methodology' (2019) 12 *Journal of Transportation Security* 1

Schmitz-Berndt S and Chiara PG, 'One Step Ahead: Mapping the Italian and German Cybersecurity Laws against the Proposal for a NIS2 Directive' (2022) 3 *International Cybersecurity Law Review* 163

Serror M and others, 'Challenges and Opportunities in Securing the Industrial Internet of Things' (2021) 17 *IEEE Transactions on Industrial Informatics* 2985

Seuring S and Müller M, 'From a Literature Review to a Conceptual Framework for Sustainable Supply Chain Management' (2008) 16 *Journal of Cleaner Production* 1699

Sharma A, 'Hive Claims Ransomware Attack on Tata Power, Begins Leaking Data' (*BleepingComputer*, 25 October 2022) <<https://www.bleepingcomputer.com/news/security/hive-claims-ransomware-attack-on-tata-power-begins-leaking-data/>> accessed 18 January 2024

Sullivan AK, 'Piracy in the Horn of Africa and Its Effects on the Global Supply Chain' (2010) 3 Journal of Transportation Security 231

Vandezande N, 'Cybersecurity in the EU: How the NIS2-Directive Stacks up against Its Predecessor' (2024) 52 Computer Law & Security Review 105890

Wallis T, Johnson C and Khamis M, 'Interorganizational Cooperation in Supply Chain Cybersecurity: A Cross-Industry Study of the Effectiveness of the UK Implementation of the NIS Directive' (2021) 48 Information & Security: An International Journal 36

Wang-Mlynek L and Foerstl K, 'Barriers to Multi-Tier Supply Chain Risk Management' (2020) 31 The International Journal of Logistics Management 465

Wolters PTJ, 'The Security of Personal Data under the GDPR: A Harmonized Duty or a Shared Responsibility?' (2017) 7 International Data Privacy Law 165

Woods DW and Ceross A, 'Blessed Are The Lawyers, For They Shall Inherit Cybersecurity', *Proceedings of the 2021 New Security Paradigms Workshop* (Association for Computing Machinery 2022)

3.

Measuring Up to (Reasonable) Consumer Expectations: Providing an Empirical Basis for Holding IoT Manufacturers Legally Responsible

This article was published in the Proceedings of the 32nd USENIX Conference on Security Symposium on 9 August 2023. The text was last revised on 1 March 2023, with some minor textual corrections for inclusion in this dissertation.

Lorenz Kustosch, Carlos Gañán, Mattis van 't Schip, Michel van Eeten and Simon Parkin, 'Measuring Up to (Reasonable) Consumer Expectations: Providing an Empirical Basis for Holding IoT Manufacturers Legally Responsible' Proceedings of the 32nd USENIX Security Symposium (2023).

Abstract

With continued cases of security and privacy incidents with consumer Internet-of-Things (IoT) devices comes the need to identify which actors are in the best place to respond. Previous literature studied expectations of consumers regarding how security and privacy should be implemented and who should take on preventive efforts. But how do such normative consumer expectations differ from what is actually realistic, or reasonable to expect how security and privacy-related events will be handled? Using a vignette survey with 862 participants, we studied consumer expectations on how IoT manufacturers and users would and should respond when confronted with a potentially infected or privacy-invading IoT device. We find that expectations differ considerably between what is realistic and what is appropriate. Furthermore, security and privacy lead to different expectations around users' and manufacturers' actions, with a general diffusion of expectations on how to handle privacy-related events. We offer recommendations to IoT manufacturers and regulators on how to support users in addressing security and privacy issues.

1 Introduction

There are a growing number of consumer Internet-of-Things (IoT) devices in daily use in homes, such as smart speakers, smart lighting, and other home appliances now being offered with network connectivity. Flaws have been exposed in consumer IoT devices after release and purchase, such as security vulnerabilities and misconfigurations [72] and undisclosed data collection flows [28, 76]. How published flaws are addressed by their manufacturers is inconsistent – ranging from no response to security updates to, in rare cases, product recalls (as for smart cars [39]).

Home users have varying ideas on who they want to take responsibility for securing the devices before they enter the consumer market [40]. In parallel, government-level policymakers in various countries have set standards for consumer IoT security and privacy [30, 35], in an effort to reduce the problems that devices come with ‘out of the box’.

Existing efforts in academia and policy focus on boosting the baseline of security and privacy for consumer IoT devices. Still, problems do arise, and home users attempt to mitigate them in their own way when this happens [59, 16, 73]. It is uncertain whether entities in the consumer ecosystem other than users are providing adequate paths toward resolving these problems, where this includes the responsibility of the IoT manufacturer to fix issues or even refund a purchase. What is also not well understood is what support home users have come to expect of others when they learn that something has gone wrong with the security or privacy of their device. This raises questions around whether they have the same expectations for IoT devices as for the more familiar categories of smartphones or personal computers.

It is critical to understand the presumptions users make as to who they can turn to, as it should be that they can go to the right person for the right help, and do so easily and with some confidence that it is a predictable process. Would they assume first to have to go to the point of purchase [65], ask a (supposedly) ‘tech-savvy’ friend [66], or stop using the device altogether [16]? At present, issuing a software update is the easiest path for manufacturers, but even this patching is patchy, and does not always remediate inherent defects [72].

We conducted an online survey with 862 participants to study their expectations about the handling of IoT security and privacy events for products that they might own. We did so by presenting systematically varied vignettes. We answer a series of research questions: **(RQ1)** What do consumers expect how manufacturers *will* respond to emerging privacy and security risks with IoT devices?; **(RQ2)** What do consumers expect how manufacturers *should* respond to emerging privacy and security risks with IoT devices?; **(RQ3)** Do expectations differ across product types and threat events?; and **(RQ4)** How do participants evaluate the user’s responsibility to handle emerging privacy and security risks with IoT devices?

In the legal domain, *reasonable expectations* are critical to determining when a product or service can be considered defective [91] and thus trigger liability and product conformity regulation. While there is prior research into consumer expectations around

Internet of Things (IoT) and smart devices [79, 82, 55], it is centred around normative expectations – that is, the preferences of consumers for how things should *ideally* be and which actors should *ideally* be responsible [40]. This does not capture what can reasonably be expected once something goes wrong with devices already in the market [40, 41, 45]. We examine reasonable expectations by what is reasonable to expect (likelihood expectations), relative to what is hoped for (normative expectations), where the latter have been explored regularly in existing literature. Our main contributions are:

- We provide empirical insights on an important but understudied topic: What are consumers’ expectations when something ‘goes wrong’ with the security and privacy of IoT devices?
- We extend ongoing user research on IoT security and privacy by framing users’ needs in terms of what they realistically *expect* from device manufacturers relative to what they *hope* for. We find consumer expectations diverge between these two types of expectations, between privacy and security risks, and across device types.
- Our results provide a new angle for consumer protection policymakers and IoT device manufacturers when considering users’ expectations, and we frame recommendations for addressing user needs to meet their expectations.

2 Background and Related Work

Here we frame existing research on home users’ experiences with IoT security and privacy against legal processes involving reasonable expectations. These are then considered alongside the expectations then placed upon other actors in the market, such as manufacturers and retailers.

2.1 Expectations of IoT security and privacy

There has been considerable research on consumer expectations for IoT security and privacy. This can include the features users expect for security [94, 82] and privacy [11, 49], but also the security concerns they would want a solution for [23, 93, 41]. Existing work conceptualizes expectations as *normative expectations* [36, 43] – that is, what users’ preferences are for how things *should* be to minimise the potential for security and privacy problems to reach those users.

Normative user expectations have been captured as indicators of many preferences relating to consumer IoT devices: purchasing decisions relative to data access preferences [33], intentions to use devices relative to utility and data sensitivity [82], and approachability of security and privacy protection solutions [45]. Normative preferences are embodied most clearly in research on the *contextual integrity* [12] of data, regarding individuals’ privacy preferences around the appropriateness of data flows involving IoT devices [3, 1, 55, 7, 79].

Alongside normative expectations, realistic expectations have been examined, albeit in limited scope. Zhang et al. [95] studied users' likelihood expectations of internet-connected security cameras with facial recognition capabilities and found that scenarios involving facial recognition prompted higher discomfort and more surprise. Furthermore, Gabriele et al. [38] prompted fitness tracker users about how feasible and likely a range of different threat scenarios were, finding that participants indicated a general optimism bias by underestimating likelihood of negative outcomes.

Here we move beyond risk perceptions and focus on what users regard as being reasonable to expect from different actors to resolve security and privacy issues with IoT devices. To the best of our knowledge, Haney et al. [40] provide the only account so far that relates to expectations about responsibilities for ensuring the highest security and privacy of IoT devices. Participants framed 'ideal' situations wherein IoT manufacturers would be duty-bound to uphold the security and privacy of their smart home devices; at the same time, participants were unsure if manufacturers were in reality willing or able to do so. It is this distance between what *should* be done as a preferred ideal, and what *can be expected* as reasonable, that we study here.

2.2 Reasonable expectations in law

Expectations of consumers of a given product play a role in the domain of product liability and conformity laws. A concept originating in the United States, consumer expectations can be taken into account in product liability cases, when a 'consumer expectations test' is an option for the plaintiff to prove that the design of a product is defective [29]. This is the case if the product *"failed to perform as safely as an ordinary consumer would expect when used in an intended or reasonably foreseeable manner."* In product liability cases, the plaintiff must thus prove that the expectations of a reasonable consumer were breached by the manufacturer.

The 'reasonable expectations' of consumers are relevant in other legal frameworks. For instance, the European Product Liability Directive [86] requires manufacturers of products – including IoT devices – to ensure that products conform to specific requirements. A product is defective, or regarded as not conforming to requirements, *"when it does not provide the safety which a person is entitled to expect, taking all circumstances into account."*, as is also applied in EU courts (e.g., [9]).

Regardless of jurisdiction, the decision-making of courts is complex and context-dependent. Different factors can be taken into account to determine if a product conforms with requirements, such as product marketing and presentation, the baseline of comparable products on the market, or pertinent regulations and standards (e.g., [86, 87, 35]). Among these considerations, we find expectations of 'ordinary' or 'reasonable' consumers [51].

How consumer expectations and 'reasonableness' are conceptualized and determined lies ultimately with the court. However, case law commonly shows how expectations of 'ordinary' or 'average' consumers are considered in the verdict (e.g., [6, 90]), and regulations highlight the importance of the expectations of a 'public at large' [86].

To the best of our knowledge, courts have not drawn on survey evidence to inform their assessments of consumer expectations in the domain of security and privacy. That being said, we hope to provide empirical support for those assessments with our study. Our work connects to these legal notions via quantitative data on a large sample, to capture what consumers expect as opposed to what they consider desirable.

2.3 The role of other stakeholders

Governments and regulatory bodies are at work to establish a basic level of privacy and security for IoT devices, such as consumer data protection laws like the GDPR [88] or CCPA [21], or regulations aiming at securing connected devices specifically such as the EU radio equipment directive [87]. There are several industry and government organizations publishing guidelines and voluntary standards to help manufacturers implement improved security and privacy into their products, e.g., from NIST and ENISA [35, 34, 30].

Looking at market actors, there are a few instances of product recalls, in case of serious security and privacy risks. These include smartwatch encryption for younger users [60], network-vulnerable smart security cameras [44], and vulnerable automobile software [39]. The most common response is the release of a software patch [62, 4]. Retailers serve a role as a contact point when a purchased device has problems or must be replaced [65], and this role is being recognised in some EU countries, e.g., the Netherlands [56]. Other emerging initiatives involve IoT product ‘labels’ [53, 32, 31] to guide consumers to purchase more secure IoT devices with more transparent details of the security and privacy features; consumer guides complement this, e.g., Mozilla’s ‘*Privacy Not Included’ [54]. We revisit how the manufacturer response informs the role of other stakeholders (such as retailers and governments) in section 5 based on our survey results.

Outside of policy and market mechanisms, Internet Service Providers (ISP) are also well-positioned to detect, inform, or quarantine infected users [22, 16]. Otherwise, if a user has problems with a device, they may reach out to someone they regard as ‘informal’ technical support [66], or seek information on news or specialist websites [70] or on forums [42].

3 Method

To address our research questions defined in section 1, we deployed a vignette-driven online survey with 862 participants from the Prolific [68] crowdsourcing platform during August 2022. Participants were each presented with seven fictional text-based scenarios (*vignettes*) about a user experiencing a privacy or security risk with their IoT device, accompanied with varying ways in which the manufacturer and user respond to the situation.

As we were interested to measure expectations about concrete actions from manufacturers and users and how this would be influenced by IoT devices and security and privacy events, we systematically varied all these factors as variables in the vignettes to measure their relative impact on participants' expectations.

Vignettes have been widely used in privacy and security user research [55, 3, 10, 7, 50, 13, 15] and allow to study participants' judgments on multidimensional phenomena, while reducing social desirability biases of direct survey questions [85, 46]. Vignettes have been demonstrated elsewhere to be useful in exploring scenarios with *unresolved issues* in security and privacy [15], here being the uncertainty around who is best-placed to address a perceived security or privacy shortcoming with a consumer IoT device.

Each vignette described a situation with the same overall structure: 1) A user has an IoT device which gathers specific data and is used in a certain context and for certain purposes; 2) The user learns that the device has a software vulnerability (*security*) or is used for previously-undisclosed data practices (*privacy*); 3) The device manufacturer has responded in a particular way; 4) the user follows a certain course of action in response to the event. Each of these four phases constituted a factor in the vignette that could take on several varying levels, which are summarized in Table 1. An example vignette about a security event is given as follows, involving a protagonist (Alex); numbers in brackets are inserted here (and do not appear in the survey itself), representing (1) Device, (2) Event, (3) Manufacturer response, and (4) User response:

Alex has several [1] **internet connected security cameras** at home, which are kept switched on continuously. The cameras continually collect video recordings of Alex's home and its surroundings to act as a deterrent against break-ins and allow Alex to check the video feeds remotely from a mobile app via an internet connection. Alex reads in a news post that a software vulnerability has been found in this device model and that similar vulnerabilities have been attacked. The [2] **vulnerability could allow other people to remotely install software on the device without Alex noticing**. The device could then be used to remotely attack other websites or devices connected to the internet, but Alex would still be able to use the device without noticing a problem. In response to this, the [3] **device manufacturer releases a statement** on their website and social media channels, which informs users about the vulnerability and the risks. Alex decides to try to [4] **return the devices** to the store where they were bought, hoping to receive a full refund or a replacement.

3.1 Measuring consumer expectations: the ideal and the learned

To measure participants' expectations about manufacturers' responsibilities and users' roles, we asked several 7-point Likert scale questions after each vignette, as follows:

- 1) **Likelihood expectation.** How likely a real manufacturer would respond this way;

Table 1: Overview of vignette factors and levels.

Factor	Levels security vignettes	Levels privacy vignettes
Device	1. Smart speaker 2. Smart watch 3. Smart washing machine 4. Smart security camera 5. Smartphone 6. Connected car	1. Smart speaker 2. Smart watch 3. Smart washing machine 4. Smart security camera 5. Smartphone 6. Connected car
Event	1. DDoS 2. Unauthorized data access 3. Ransomware	1. Data collection without consent 2. Third party data sharing 3. Forced data collection
Manufacturer response	1. Announce patch 2. Inform users via website and social media 3. No response 4. Recall	1. Announce update with more privacy settings 2. Inform users via updated privacy policy 3. No response -
User response	1. Attempt to return device 2. Attempt technical mitigation 3. Seek advice online 4. Turn device off 5. Keep using as before	1. Attempt to return device 2. Attempt technical mitigation 3. Seek advice online 4. Turn device off 5. Keep using as before

- 2) **Normative expectation.** How appropriate the manufacturer response was. This relates to prior examination of what consumers expect of other ecosystem actors [40];
- 3) **Appropriateness of user action.** How suitable the user's action was in light of the scenario and manufacturer response;
- 4) **Vignette realism.** How realistic participants deemed the vignette to be.

This approach allowed us to simultaneously measure the impact of the vignette factors on these response scales. We designed two separate sets of vignettes, one for security events and one for privacy events, allowing us to contrast the arguably more state-driven nature of security dilemmas (whether a device is secure or not) with the context-driven nature of privacy dilemmas (whether personal privacy preferences have been respected).

3.2 Survey procedure

Participants on the Prolific platform were directed to a Qualtrics [69] survey, hosted at our research institution. After reading and agreeing to the informed consent, participants were presented with a short summary of consumer IoT devices to ensure all participants had a working understanding of what was and was not regarded as an IoT device (which is important for the purpose of shared understanding between researcher and participant [46]). To capture prior experience with internet-connected devices, participants were then asked to select from a multiple choice list of devices they have used at least once during the last four weeks.

Participants were each assigned a set of vignettes generated from source factors as in Table 1, constructed to resemble a scenario as in the example vignette (subsection 3.1). Participants then answered questions about a differing set of these kinds of vignettes. Participants either received a full set of security vignettes, or of privacy vignettes. Vignette construction is detailed in subsection 3.3. After reading and answering questions about all assigned vignettes, participants were asked how confident they felt about their answers. Participants were then asked if the vignettes reminded them of any personal experiences with electronic devices, allowing them to provide personal stories [71] of security and privacy in an open text field. Participants then answered closing demographic questions, were debriefed and thanked for participation. It took 17.69 minutes on average to complete the survey (SD = 9.47 min), which also includes two attention checks; each vignette set included one Likert-scale question, which asked participants to answer with '*agree*'. After finishing all vignettes, participants were also asked to select a specific device from a short list of devices. The full survey instrument can be found online as accompanying material¹.

3.3 Vignette design

Participants were randomly assigned to either see security or privacy vignettes and were presented with seven vignettes in a random order to avoid sequencing

¹ <https://doi.org/10.4121/c.6440264.v1>

effects [75, 8]. We opted to present seven vignettes to strike a balance between more repeated measures per participant (increasing statistical power) [8] while not mentally overloading them with too many vignettes [48]. After each vignette the four Likert scale questions described in subsection 3.1 were asked.

If participants rated the manufacturer response as inappropriate, the user response as not suitable, or the vignette as unrealistic (selecting a value below the mid-value ‘*neither agree nor disagree*’), a free-text entry box was presented prompting to explain what motivated their answer. This encouraged participants to suggest other user or manufacturer responses that were not covered by the vignettes. These were typically seen to involve suggesting one of the response types presented in the survey, so for brevity these are not discussed further here.

Combining all possible combinations of the vignette levels depicted in Table 1 led to a total vignette population of 360 different combinations for security, and 270 different combinations for privacy. Adhering to methodological literature [8, 80], we reduced both vignette populations (*full factorial*) to a subset (*fractional factorial*), so that only a selected fraction of possible vignette factor combinations would be tested by participants. The resulting two subsets consisted of 91 different vignettes each and were then split up into 13 smaller subsets (*blocks*) with seven vignettes each, so that participants would be randomly allocated to one of the blocks. This kept the required number of participants manageable and limited the number of vignettes presented to participants to avoid mental fatigue [48].

We removed illogical combinations between factor levels to retain vignette credibility, e.g., the recursive example of a manufacturer updating the privacy policy to inform users about an updated privacy policy explaining additional data collection. We furthermore ensured that every participant would see each factor level at least once when reading the seven vignettes (e.g., not be predominantly presented with vignettes about smart cars, but see each device at least once) and that combinations of factor levels would occur equally often over the entire sample, e.g., to avoid that a recall of a smart speaker would occur more often than a recall of a smartphone.

We took great care in generating empirically grounded and realistic vignettes by deriving them from news reports, prior empirical literature, consultations with security and privacy as well as legal scholars, and a focus group. In the following paragraphs we explain our procedure and motivation for selecting the vignette factors and levels.

3.4 Choice of vignette factors

Choice of IoT devices. As factor levels, devices were selected which ranged from common ‘smart home’ devices such as smart speakers or IP cameras, to connected cars and smart washing machines. We also added smartphones as a prevalent and familiar device for comparison.

The goal was to compare a diverse variety of IoT devices with varying usage contexts, data collection capabilities, and risks, to determine their influence over security and privacy expectations.

Choice of security and privacy events. We examined whether different security- and privacy-related risks would influence expectations on how manufacturers and users should handle them. We primarily based event types on prior user studies, and news reports. For instance, we identified reports of DDoS malware [52], unauthorized access to IoT sensor data [74], and ransomware attacks targeting IoT devices [64]. Privacy-related events included reports of staff listening to device recordings for training of algorithms [28, 57], or device data being shared without the user's consent [76, 27].

Events followed one of three different outcomes: that continued use of a device is impaired or 'forces' consent to be given; personal data from the device could be accessed by unknown parties (attackers or secondary data recipients), or; the device or its functional data is leveraged without the user's knowledge or consent.

Choice of manufacturer responses. There is a focus in the literature on provision of software updates as a core response to security issues such as vulnerabilities [62, 4] and privacy issues such as providing more privacy controls [18]. We included these as possible manufacturer responses, but examination of news reports indicated a range of different responses beyond this. For instance, we noted product recalls in case of risks posed to children by smartwatches [60], smart security cameras being vulnerable to DDoS malware [44], or smart vehicle vulnerabilities [39]. There were also accounts of manufacturers not visibly responding directly to an event [61, 63, 24], reflecting that there is – as yet – little in the way of direct and consistent legal obligation for manufacturers to respond in a specific, predictable way.

Based on these reports and related research we conceptualized companies' responses to disruptive events along a continuum, of enacting no responsibility to considerable responsibility [20, 19, 67], specifically: No reaction, informing users, releasing a software update, and recalling a device.

Choice of user responses. We grounded user responses in privacy and security user studies. However, empirical research on how IoT owners respond to security and privacy events is scarce [16, 73], as existing work mostly focuses on preventative mitigation by users [40, 41, 81, 37, 2]. We included five different user responses: 1) Keep using the device, due to e.g., discounting of risks to data [93, 45, 47, 81] or security [40, 81], or resignation [77, 40, 47]; 2) Unplug the device, ceasing or pausing use [84, 74, 16]; 3) Opportunistically seek help from others [66, 25] or online [78, 42, 5, 74]; 4) Attempt technical remediation oneself through device configuration or isolation from the network [37, 41]; 5) Request a refund or a replacement device from the seller. Such a response is commonplace when users perceive a defect in purchased goods and is protected by legal frameworks. However, with suspected security and privacy flaws this may be subject to the seller's judgement and hence unpredictable.

3.4.1 Uncertainty and consumer expectations

We phrased the vignettes so that the protagonist, and in turn the survey participant, would have incomplete information about the situation involving a security or privacy risk. For instance, all software vulnerabilities were phrased in a way that the vulnerability *could* allow for an undesirable outcome, or that data collected and shared with third parties *could* be linked to other information about the user. This level of ambiguity was chosen since users of consumer IoT devices usually face such uncertainty [74, 16, 84].

3.4.2 Pilot study

Prototype vignettes were tested ‘offline’ in an iterative manner with volunteers without a technical background to check comprehensibility. This resulted in removal of illogical vignette combinations, language improvements, and efforts to give the protagonist a gender-neutral name (Alex).

A pilot study was conducted online with 32 participants from Prolific [68] to assess survey functioning, completion time, and vignette comprehension. It took participants 19.2 minutes on average to complete the survey, vignettes were rated as easy to understand, and open text responses did not indicate any major comprehension or technical issues. This resulted in slight adjustments to phrasing of some factor-level combinations within vignettes.

3.5 Ethics

The study was approved by the host institution’s human research ethics committee prior to survey deployment. To participate in the survey, individuals were informed that participation was voluntary, could be stopped at any time, and that no personally identifiable data would be collected. Participants had to agree to these points to be able to take the survey. We paid participants £3.00 for 20 minutes of their time, matching the minimum wage in the host institution’s country.

3.6 Participants

Participants were recruited via the crowdsourcing platform Prolific [68] during August 2022. We screened for fluency in English, prior participation in at least five other studies on the platform, and a minimal approval rating of 95%. We did not screen for IoT device ownership or usage, but we did assess their experience, as we were interested if people with less or no IoT experience had differing expectations. In an effort to sample participants from different countries, we opened the survey several times, at different times and for different regions.

Demographics are summarised in Table 2. 862 participants took part in the survey: 443 female (51%), 399 male (46%), and 20 non-binary or no answer (3%). Age was skewed towards a younger population, which is a typical characteristic of Prolific samples [83]. Participants indicated to be from 30 different countries, which we mapped to regions

Table 2: Distribution of age and region in the sample. The three most prevalent countries were USA (N = 179), Canada (N = 125), and Portugal (N = 86).

Age (in years)		Region of residence	
18-24	312	Europe (inc. UK)	464
25-34	303	North America	304
35-44	142	Africa (South Africa)	65
45-54	55	Cent. and S. America	26
55-64	42	Other	3
65	6		
Prefer not to say	2		
		Sample size:	862

for further analysis. The majority of participants lived in western countries (Europe and North America), while a smaller number lived in other regions such as Africa and Central and South America. Participants used on average 5.65 (SD = 2.30) internet-connected devices during the previous four weeks, indicating considerable experience with IT devices.

Due to random allocation to either the security or privacy vignette condition, participant characteristics (age, gender, region of residence, and device usage) were similarly distributed in both conditions.

23 participants got one of the two attention-check questions wrong; no participant failed both. We found no indication of suspicious response patterns from these 23 participants, and thus treated their responses as genuine and included them in analysis.

3.7 Vignette and response quality

Prior security-related studies have indicated the usefulness of realism checks for scenarios, for moderating the quality of response data [14]. We checked the responses to the prompt *'The situation described in the story is realistic.'*, on a 7-point Likert scale, where a 1 would indicate *'Strongly disagree'* and 7 *'Strongly agree'*. On average, vignettes were rated to be realistic, not warranting concerns about implausible vignettes: for security vignettes, mean realism rating = 5.48, SD = 1.16; for privacy vignettes, mean realism rating = 5.67, SD = 1.09.

Participants' confidence in their responses was checked with *'How confident do you feel about your answers to the previous stories?'*, on a 4-point Likert scale from 1 = *Very unconfident* to 4 = *Very confident*. Participants were highly confident about their responses (Mean = 3.51, SD = 0.54).

3.8 Data analysis

To answer our research questions, we first assessed average response patterns across vignette levels to identify general trends in the data. To quantify vignette factors' effect on expectation ratings, we ran multilevel regression models with maximum-likelihood estimation. Vignette factors were used as explanatory categorical variables predicting the response variables *Appropriateness of manufacturer response*, *likelihood of manufacturer response*, and *suitableness of user response*. Thus, six regression models were run, one for privacy and one for security for each response variable. In each model, we tested if demographic background (age, gender, region) and recent device usage had an effect.

Multilevel regression analysis allowed us to conduct tests of significance of factor levels, assess model fit, and control for any effects of participant characteristics such as recent device usage or region of residence. As suggested by methodological literature [8], random intercepts were included to account for individual differences between participants. As the response variables were on seven-point Likert scales, we treated them as continuous [58].

All regression models were built up with the following sequence: 1) A baseline with vignette levels as fixed explanatory variables and a random intercept term. For all tested regression models, likelihood ratio tests of the random intercept term were statistically significant, indicating that accounting for differences between participants explained significant variance in the data; 2) After the baseline model was defined, participant-level variables (age, gender, region, recent device usage) and possible interaction terms were added in a step-wise fashion to assess whether they significantly improved model fit. In Table 1 in the Appendix we include the final models, reporting participant-level or interaction effects in the next sections only if they were found to be present.

Open-text responses were reviewed for any additional insight into participants' motivations behind their survey answers. We include representative quotes alongside results in the next section. To study participants' personal experiences with security and privacy incidents, two researchers independently reviewed the text responses to the survey question (*'Did the previous stories remind you of any personal experiences you have had with electronic devices?'*). During this thematic analysis [17], initial codes of reoccurring themes in the data were generated, which were then regularly discussed between the researchers in an iterative coding process.

4 Results

4.1 Expectations of manufacturers

We first present how participants judged the manufacturer responses described in the vignettes, as an expression of expectations about how IoT manufacturers *would* and *should* respond to security and privacy events.

4.1.1 Likelihood judgements of manufacturer responses

Our first research question (RQ1) examines what consumers expect of how device manufacturers actually *will* respond to emerging privacy and security risks with IoT devices, as a construct closely relating to reasonable expectations. The left-hand side of Figure 1 shows how likely the manufacturer responses to a security event were rated on average across device types; Figure 2 does the same for privacy events.

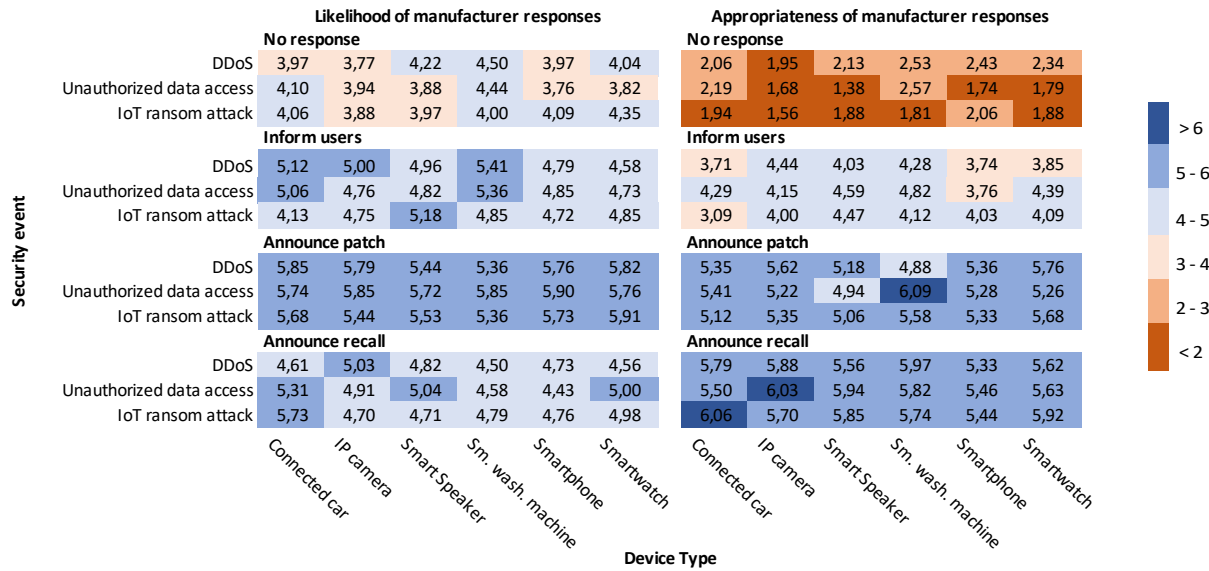


Figure 1: Ratings of likelihood and appropriateness of manufacturer responses to security events. Measured on a 7-point Likert scale with 1 = 'Extremely unlikely' to 7 = 'Extremely likely' for likelihood of manufacturer response and 1 = 'Strongly disagree' to 7 = 'Strongly agree' for appropriateness of manufacturer response.

For security vignettes, patching was seen as the most likely response overall (mean of block 'Announce patch' = 5.70), followed by informing users about the risks (mean of block 'Inform users' = 4.87), recalling devices (mean of block 'Announce recall' = 4.84), and lastly, not visibly/publicly responding at all (mean of block 'No response' = 4.05). Figure 1 illustrates this, as average ratings were generally higher for patching across security events and IoT devices. The unexpected nature of manufacturers not responding was reflected by participants' comments, e.g., "I believe most manufactures would speak about the matter and possibly would recall the devices or issue an update for the devices." (PID293). The regression analyses (Table 1, Model 3) supported this trend: for security, all manufacturer responses were judged as significantly more likely than no response.

Figure 2 shows that for privacy vignettes, participants rated it most likely that a manufacturer would update the privacy policy and inform users (mean of block 'Inform users via privacy policy' = 5.28), while no response was seen as least likely (mean of block 'No response' = 4.74). In contrast to security vignettes however, this response omission was seen as relatively more likely. The regression analysis (Table 1, Model 4 in the

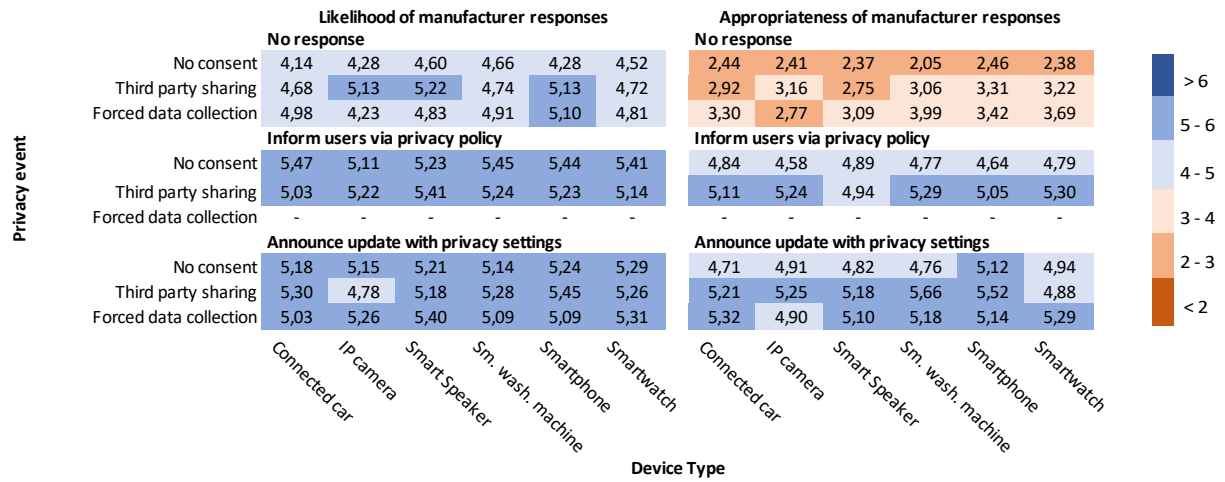


Figure 2: Ratings of likelihood and appropriateness of manufacturer responses to privacy events. Measured on a 7-point Likert scale with 1 = 'Extremely unlikely' to 7 = 'Extremely likely' for likelihood of manufacturer response and 1 = 'Strongly disagree' to 7 = 'Strongly agree' for appropriateness of manufacturer response. Empty cells correspond to less plausible vignette level combinations, which were removed from the design.

Appendix) shows that the likelihoods of the two explicit manufacturer responses were comparable, indicated by similar coefficient estimates.

4.1.2 Normative judgments of manufacturer responses

Our second research question (RQ2) examines what consumers expect of how IoT manufacturers *should* respond to emerging privacy and security risks with IoT devices to contrast such normative preferences with perceptions of the status quo. This is then closer to the aims of prior research [40]. The right-hand side of both Figure 1 and Figure 2 present how *appropriate* the manufacturer responses were, rated on average across both device types and security or privacy events respectively; *Model 1* and *2* in Table 1 in the Appendix show the regression models predicting appropriateness ratings of manufacturer responses.

For security vignettes, participants rated a product recall as the most appropriate manufacturer response across IoT devices and security events (mean of block 'Announce recall' = 5.76), followed by a patch (mean of block 'Announce patch' = 5.34). The manufacturer omitting a response to a security risk was rated as highly inappropriate on average (mean of block 'No response' = 2.05) across devices and security events, which was significantly lower than all other responses, as indicated by the regression coefficients in Table 1 (*Model 1*) in the Appendix. Among those participants who provided low ratings, indicative reasoning included, "They are completely ignoring an issue that could put people in danger, if malicious people were to find out their location, for example." (PID283).

Both recall and patching received comparable ratings across device classes and security threats, demonstrating that participants valued both responses regardless of context. Several participants also stressed the importance of the timing of patches, e.g., "*An expected date of update would be appropriate, as well as some sense of urgency*" (PID169).

For privacy events (Figure 2), releasing a software update with more privacy controls was most preferred across devices and privacy events (mean of block '*Announce update with privacy settings*' = 5.09). The regression model predicting the appropriateness ratings for privacy (Table 1, *Model 2* in the Appendix) supported this, as both of the explicit manufacturer responses were rated significantly more appropriate than no response.

4.1.3 Dependency on device type and risk event

In **RQ3**, we asked if participant expectations would vary across different device types and security and privacy risks. Looking at Figure 1 and Figure 2, this involved distinguishing between cells across rows and columns. For expectations of how manufacturers would actually respond, we did not find substantial effects of the type of security event on participants' estimations. For privacy events however, we observed that it was rated least likely that a manufacturer would not respond after it became public that data was shared without consent (*no consent*), while it was seen as comparably more likely that a manufacturer would show no response after it became public that data is shared with third parties (see Figure 2).

For device types, recalls were judged most likely as a response for vulnerable connected cars, presumably since recalls of cars occur more often than for the other devices. It was rated least likely that a manufacturer would not respond to arising security vulnerabilities of security cameras and smartphones. Regression *Model 3* in Table 1 in the Appendix indicates that a product recall and a patch for a vulnerable smart washing machine were seen as significantly less likely than for a smart security camera. This could be driven by smart washing machines being seen as less critical or complex, with participants judging both recalls and patches as excessive and thus unlikely, e.g., "*It's extremely rare that companies would make such expensive moves. These are absolutely the right things to do, but [...] it's much more convenient to warn costumers, issue patches, or even ignore the problems.*" (PID140).

Normative expectations were also slightly influenced by IoT device type and the nature of arising security and privacy risks. No manufacturer response was rated as especially problematic for security cameras and smart speakers (e.g., "*[Alex] should completely shut it [Smart speaker] down and wait until it is clear that the software patch is ready*" (PID70)), and relatively less problematic for smart washing machines (e.g., "*Someone knowing my washing schedule really wouldn't concern me. I'd probably just keep using it.*" (PID604)). Informing users of connected cars and smartphones was rated as less appropriate than for the other devices. We assume this was due to cars and smartphones usually being needed on a daily basis, and only informing users was seen as not sufficient, e.g., "*This solution [inform owners] does not seem proactive enough*" (PID608).

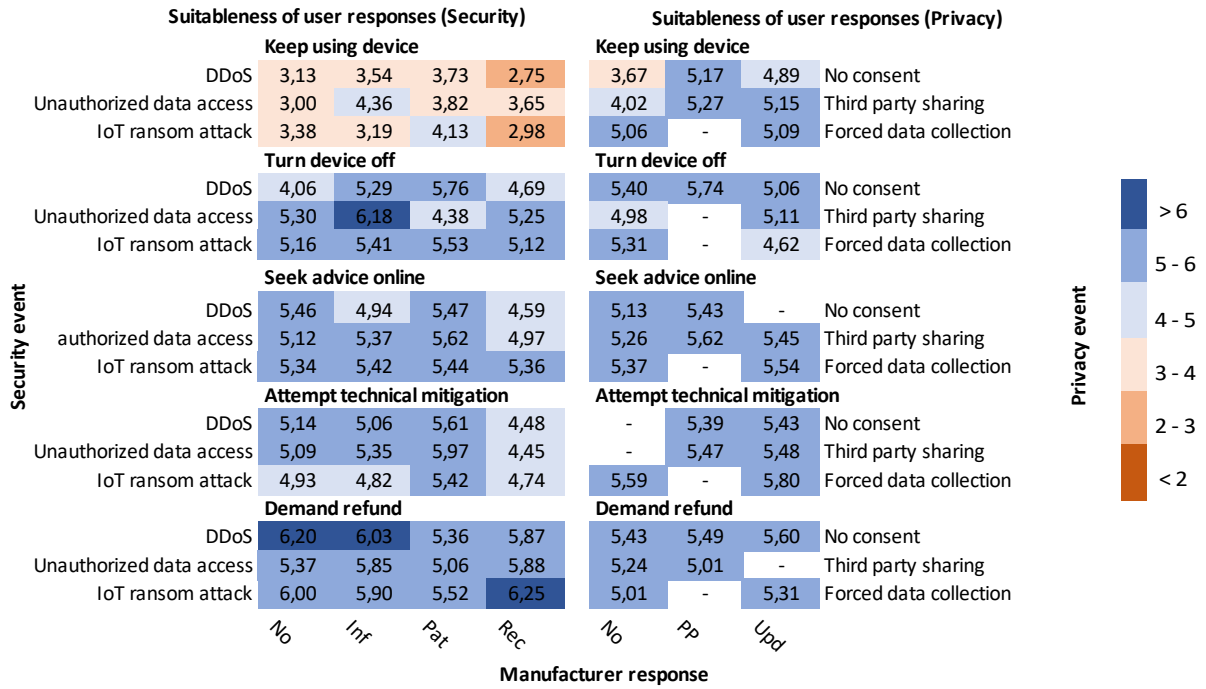


Figure 3: Ratings of user response suitability across security and privacy events and previous manufacturer responses. Measured on a 7-point Likert scale with 1 = 'Strongly disagree' and 7 = 'Strongly agree'. Empty cells correspond to less plausible combinations, which were removed from the design or combinations that were removed during the generation of the fractional factorial design, as not all three-way combinations of vignettes could be included. Key: No = 'No response'; Inf = 'Informed users'; Pat = 'Announced patch'; Rec = 'Announced recall'; PP = 'Informed via privacy policy'; Upd = 'Announced privacy settings'.

Privacy risks also influenced the judgement of manufacturer responses. Scenarios where the user finds out that data has been collected from the device without consent ('No consent', Figure 2) negatively impacted how appropriate manufacturer responses were rated, especially for 'No response', as also shown in the regression model in the Appendix (Table 1, Model 2, sign. diff. between no consent and third-party sharing).

4.2 The user's role

In this section we answer **RQ4** and report on how participants evaluated the behaviors exhibited by the user in the vignettes. These results do not only inform how participants judged the user's responses specifically, but also how these judgements translate to their expectations about the suitability of the user's options in reaching a satisfactory response to particular events. Figure 3 depicts how user behaviors presented in the vignettes were rated across previous manufacturer responses and security and privacy events and Model 5 and 6 in Table 1 in the Appendix present the results of the regression models predicting the suitability of the user responses with vignette factors.

4.2.1 Handling security risks

On average, participants in the security vignette condition rated returning the product for a replacement or refund as the most suitable user action (mean of block '*Demand refund*' = 5.79), and continued usage as the least suitable (mean of block '*Keep using device*' = 3.46). When asked for alternatives for the user after giving a low response, explanations included, e.g., "*Simply turning off the device and ceasing to use it is a waste of money. Instead, Alex should return the smart speaker.*" (PID659). All user responses were rated significantly higher than *Keep using*, as indicated by the regression coefficients in Table 1 (*Model 5*) in the Appendix. Attempts by the protagonist to find a technical solution themselves were rated as less suitable (mean of block '*Attempt technical mitigation*' = 5.01) than simply turning the device off (mean of block '*Turn device off*' = 5.18). This apparent scepticism towards the user attempting a technical strategy was also reflected in text responses, e.g., "*Doing the configuration on his own requires specific knowledge and from this story I get the feeling that he doesn't have it himself. He should contact specialists and take time to decide what's best.*" (PID655).

Returning the device for a refund was seen as especially suitable in case of DDoS vulnerabilities (Figure 3), while keeping a device in this case was rated very low. This effect was also reflected in a significant regression coefficient of IoT ransomware in comparison to the reference DDoS (Table 1, *Model 5* in the Appendix). It was rated highly suitable for the user to return the device when the manufacturer announced a recall. However, all other user responses, especially *attempt technical mitigation* and *keep using*, were rated lower if the manufacturer previously announced a recall. If a vulnerability allowed unauthorized access to sensor data and the manufacturer informed users about this, participants deemed it especially appropriate for the user to stop using the device (mean = 6.18).

4.2.2 Handling privacy risks

User responses to privacy events were rated similarly on average, with a user attempting a technical solution as the most suitable (mean of block '*Attempt technical mitigation*' = 5.53), and the user continuing to use the device as the least suitable (mean of block '*Keep using device*' = 4.74). In comparison to security risks, continued use was rated much higher (mean of '*Keep using device*' for security = 3.46), indicating that keeping the device on after a suspected privacy-violating event was seen as a comparably more acceptable option than after an emerging security risk.

There were lower regression coefficient estimates for the user responses to privacy events (*Model 6*) than for security events (*Model 5*) (see Table 1): in the case of privacy issues with IoT devices, participants were much less decided on a proper user response, to the extent that turning the device off was rated as the second most suitable response. This lack of a clear preference was also illustrated by a comparably low model fit (*Model 6*: $R^2_{\text{privacy}} = 0.172$ vs. *Model 5*: $R^2_{\text{security}} = 0.306$). Participants' comments hinted here at privacy resignation and feelings of helplessness, e.g., "[The] decision isn't ideal but what alternatives are there? Alex could use an older-model 'dumb' phone or look into a more security conscious manufacturer for a new device." (PID511).

The nature of the privacy event only slightly influenced responses: the user keeping the device was rated especially low if data had already been harvested without consent and the manufacturer did not respond (mean = 3.67). However, if the manufacturer informed users about the same privacy violation via an updated privacy policy, continued use was seen as much more suitable (mean = 5.17). This finding corresponds with the low appropriateness ratings participants gave all manufacturer responses to this privacy event (*No consent*). In fact, participants viewed it as the best option for the user to demand a refund or turn the device off in this case.

4.3 Personal experiences

To relate participants' expectations elicited by the vignettes with their personal experiences, we analyzed the text responses to the optional question '*Did the previous stories remind you of any personal experiences you have had with electronic devices?*'. In total, 310 participants provided answers with a wide range of topics. Of 310 participants, 58 provided accounts of how they experienced privacy or security incidents with their devices and how they or the manufacturer responded. The most commonly mentioned response was to stop using the device in some way ($n = 17$), like PID540, who noted: *"I stopped using a certain smart watch after it was unclear what data was collected from the manufacturer and third parties."* Other variations of this included interrupting usage until the situation was perceived to improve: *"I stopped using my [smart speaker] after [news about data collection] came out about it, until [the manufacturer] gave me better control over my data."* (PID382). This illustrates how users relied on manufacturers to respond and their willingness to pause device use until they received explicit reassurance. However, replacing devices in case of no manufacturer response was also seen as an option, e.g., *"When there were issues with cameras, I simply shut mine down and removed them for a time then switched over to something else that was more secure."* (PID673).

Other participants ($n = 14$) described changing device or privacy settings, for example: *"[I] have had manufacturers of devices I've used update their privacy policy, also their data collection practices. I've modified my privacy settings according to the updated policies."* (PID64). A few participants ($n = 6$) mentioned technical approaches such as limiting network capabilities, home network separation, or factory resetting. There were also rare stories of successfully having a device refunded or a device recalled: *"I had bought a [...] phone which had a security vulnerability [...] I had to return the phone [...] at the request of the manufacturer"* (PID70). There was also mention of directly contacting the manufacturer for support: *"[...] I saw many reviews stating that the speaker sells data collected from the speaker [...] I contacted the manufacturer who assisted [...] with instructions on how to turn on privacy settings"* (PID362). Generally, these reactions to security or privacy threats validated the chosen user responses in our vignette design and correspond to previous findings [16, 47, 73].

Apart from responses to problems with a device, several other themes emerged; (1) *Device linkage*; 24 respondents wrote about their concerns about apparent connections between information provided during device use and seemingly unrelated online activities. For example: *"Just seeing targeted ads that are clearly from one devices usage*

communicated to a different device in the household." (PID419). (2) *Data uncertainty*; 22 respondents described a general uncertainty about privacy policies and data flows (e.g., *"I have several smart devices [...]. There are times I don't believe there is enough transparency about how this data is used, stored, or sold. I have felt companies are dishonest about these issues before which makes me hesitant to continue to use smart products sometimes."* PID366). (3) *Dilemmas*; 20 respondents felt concerned and experienced dilemmas about whether security and privacy risks should be accepted, either in the form of resignation (e.g., *"[...] I am feeling helpless [about data collection], as there is nothing I can do about it, so I can either stop using the devices or use it and be 'tracked' down."* PID137) or as a convenience trade-off; *"[...] companies sharing the information has crossed my mind. But at the end of the day, there's not many ways around it, using the device is still more convenient than not using it."* (PID220). These themes reinforce the findings in Section 4.2.2, as they demonstrate a general uncertainty about data flows and how IoT users should manage privacy.

5 Discussion

Here we revisit our research questions and situate our findings within prior literature and ongoing discussions.

What manufacturers are likely to do. In **RQ1** we asked what consumers expect how manufacturers *would actually* respond to emerging IoT risks. As indicated by Figure 1, we found that participants in our study expected manufacturers to patch security vulnerabilities in IoT devices. This resonates with the current focus in policy circles. In contrast, no response at all was seen as unlikely, indicating that manufacturers are expected to visibly respond if a security event occurs. This supports recent standardization efforts recommending that IoT manufacturers notify and communicate with users in case of security incidents [35], and highlights the position of ISPs as being able to triangulate security problems to specific users (e.g., [16]).

The picture was less clear for emerging privacy issues with IoT devices (Figure 2), as different manufacturer responses were rated as comparably likely and no response was seen as somewhat less expected. A manufacturer not acting on problematic data flows was seen as highly inappropriate yet very conceivable. This hints at a lack of consumer trust despite GDPR regulations [88, 21] and a learned helplessness and resignation regarding control over the occurrence of privacy violations, and is in accordance with prior work [77, 40, 47].

These findings provide legal scholars and policymakers with novel empirical perspectives on the notion of consumer expectations in case of IoT security and privacy events. By using a shared language (*'reasonable expectations'*), we show how it was expected by participants that manufacturers would patch security vulnerabilities or at least respond in some visible way. As discussed in subsection 2.1, liability case law is based on a case-by-case assessment, yet our findings can serve as a reference for the design of IoT security and privacy regulations (which do play a role in courts,

see e.g., [91]) and provide new insights for legal scholars and practitioners on how the abstract notion of consumer expectations can be understood empirically.

What manufacturers *should ideally* do. Turning to **RQ2**, and how consumers prefer manufacturers *should* respond to emerging IoT events, we found that participants generally considered recalls and patching to be appropriate responses to security threats (Figure 1). Interestingly, patching was the only manufacturer response that was considered both appropriate *and* likely. Seeing patches as reasonable does rest on all security issues being resolvable by patches, without further manual fixes by the user, which in practice is often not the case [16, 73]. In contrast to patching, recalling was seen as the more appropriate response, yet also considered relatively unlikely, even less likely than simply notifying users. This suggests a gap between consumer preferences and expectations.

As patching is much more prevalent than product recalls, consumer expectations appear aligned with, and perhaps habituated to, observed market behavior. This also fits with seeing a car recall as more likely than for other consumer IoT devices. Thus, expectations might change in the next few years, where stricter regulations could trigger more frequent recalls (e.g., not complying with minimum security requirements as in the upcoming delegated EU Radio-Equipment Directive will lead to the IoT device's removal from the market [89]).

For privacy, participants favoured it when a manufacturer announced the release of a software update with more privacy controls while also judging a lack of response as least desirable (Figure 2) (reinforcing prior findings elsewhere [92]). Notably, announcing a privacy software update and updating the privacy policy were rated as similarly appropriate. As with security events, this requires notification to be visible – in this case, within the device and/or companion app itself. Prior work has indicated that more control does not necessarily lead to higher trust in privacy [92], with a view to governments needing to enforce what manufacturers can and cannot do. This could also hint at a general loss of trust towards manufacturers to handle personal data appropriately, where more privacy controls would not help to restore the trust.

Our results build on previous work on IoT consumers' expectations of the responsibility of manufacturers and users, in which users expressed uncertainty if manufacturers would realistically meet their preferences [40]. Our results indicate that there are indeed discrepancies between consumers' preferences and predictions, as well as more clearly expressed expectations about security (manufacturers will likely patch and are unlikely to do nothing) than for privacy (with less clarity as to how manufacturers will likely respond). We furthermore broaden prior research on users' preferences on IoT security and privacy (e.g., [55, 82, 40, 41]) by contrasting normative preferences with a 'reality check' of expectations of actual likelihood.

Managing *different* security and privacy circumstances. Regarding **RQ3**, we found that different IoT device classes had an effect on what responsibilities participants expected from manufacturers. For instance, expectations around smart washing

machines were less strict than for security cameras or smart speakers, which could be due to the device's less sensitive data. This matches prior work on privacy perceptions of IoT devices [82, 31]. For devices important for daily use (e.g., smartphones and connected cars), participants preferred a proactive response by the manufacturer beyond only informing them. Remarkably, connected cars did not cause a different effect. Compared to other device types, participants didn't see it as substantially less likely or less appropriate for a car manufacturer to not respond to security vulnerabilities, even though these can conceivably lead to safety hazards. For privacy events, manufacturer responses were rated as less appropriate for vignettes describing that data was harvested from the device without consent, which implies that this privacy violation reduced appraisals of manufacturer responses regardless of the actual response. Previous work has established the importance of user consent [78, 55, 3, 7, 23], and our results extend this notion by demonstrating how the breach of this fundamental privacy principle also negatively affects subsequent efforts of the manufacturer to remediate.

How best to involve users. For RQ4, the user's involvement in addressing security and privacy risks was assessed (Figure 3). For emerging security risks with IoT devices, participants deemed it most preferable for the user to return the device for a refund or replacement. Depending on local legislation, the warranty period, and the seller's leniency, this might constitute a feasible path. However, as paralleled by several participants' comments, this route is arguably rarely observed in real life, and the chances of a successful return depend on many factors outside of the user's control. A recall notice would signal the feasibility of the response, but manufacturers might not have a reliable way of getting the notice to users.

Simply keeping a device in use after learning about a security problem was generally judged as highly ill-advised for the user. This perception was different for privacy, where it was seen as much more acceptable to keep the device on, especially if the manufacturer updated the privacy policy or announced an update with more privacy controls, despite the same prior privacy violation. This contrasts with prior research implying that users would turn off a device as if 'stopping a leak' [92] and illustrates how perceptions of privacy change with manufacturer signaling, but also as how limited the user's options were perceived.

It may be that IoT users are simply lacking options for action and control (as has been seen for both security [16] and privacy [41, 45]), making it a conceivable response for users to continue using the device, as unplugging could be undesirable due to discontinued operation, demanding a refund is seen as futile, and personal technical mitigation as unpredictable. That said, users' technical attempts to mitigate privacy risks were seen as more suitable than for security vulnerabilities.

These results also broaden prior findings of instances of users stopping use of their devices after (suspected) security risks [16, 74, 84], as we observed that turning IoT devices off was seen as a generally suitable response for both privacy and security risks, and was most frequently mentioned by participants as a previously applied

response. That such a drastic step was seen as a suitable response illustrates how limited users' options appeared to be for a clear path to resolution, which highlights the necessity of actors better positioned to handle these risks to be involved.

If users were to stop using a device, this is difficult for those with expertise to detect, even if it at least stems some threats. This may also encourage a somewhat 'silent' departure from the smart device market (hinted at in subsection 4.2.2), where one 'bad actor' then tarnishes all reputations. This is arguably why consumer IoT devices are *generally* seen as lacking appropriate security (and requiring standards) although many devices exist which are already secure. Participants appeared just as amenable to stopping device use after a privacy issue as they were to demand a refund – this is then in the interests of manufacturers if they want to retain customers.

Prior work has also suggested that responsibility for protecting privacy of IoT devices was seen more with the manufacturer than with the user, while for security, the responsibility of the individual user was also central [40]. This could further explain why, in our study, participants seemed to have clearer expectations of appropriate ways for the user to handle security risks (try to get a refund, and avoid continue using a device) than for privacy, as the manufacturer is seen as responsible for remedying technical problems.

5.1 Recommendations

Here we list future directions and recommendations for ecosystem stakeholders.

Establish post-purchase maintenance and support. IoT users generally expect and appreciate explicit responses from manufacturers, preferably more than just a warning, which might remain unseen and be perceived as insufficient. Participants also voiced how they would switch brands or return devices in case manufacturer handling of security and privacy would lag behind their expectations. To establish user support and trust for the post-market phase, manufacturers should follow standards such as from NIST [35] and keep an active communication channel with their customers. While effective communication is not trivial to achieve, a collaboration with ISPs to reach identifiable customers could also be a fruitful direction.

Smooth the path for predictable outcomes. As governments are also seen to hold responsibility for IoT security and privacy [40], our findings furthermore provide regulators with insights into consumers' expectations. We recommend that regulators support users with routes for resolution that are coherent and predictable, such as specific and easily accessible advice. Furthermore, it is paramount to provide robust consumer protection laws to reduce incidents in the first place, but also to have regulatory or economic processes in place to incentivize appropriate and effective responses by device manufacturers, including smoothing the path for potential product returns.

Gather evidence with a view to its wider uses in law. In law, reasonable expectations are a fluid concept. There are no objective thresholds; the EU and US jurisdiction rely on the judge to interpret consumer expectations in each case. Our study offers concrete measurements of this construct to both legal practitioners and legal scholars in the product liability field, who might face questions surrounding consumer expectations of IoT devices in their work. A multi-disciplinary approach, in which empirical computer and social sciences support legal scholars with insights around assumptions about technology and its users, could constitute a promising future direction of academic work.

5.2 Limitations

While this study's sample is considerable in size, it is not representative of any specific national or global population. Due to Prolific's participant base, participants were mostly from 'western' countries. Furthermore, the sample was skewed towards younger cohorts, which is also typical of Prolific samples [83]. During sampling, we were interested in gathering a breadth of different regions and legislations and not in modeling any specific population. This limits the generalizability of the results yet nonetheless provides novel insights into consumer expectations across different regions.

The vignettes were bound to a limited number of factors, yet other aspects could also influence expectations. In all vignette permutations the user learns about security or privacy risks from a news post, while there are several other sources for users to learn about possible security and privacy issues [31, 70], such as word-of-mouth, unusual device behaviour, or direct notifications (e.g., by ISPs [22]). We opted for the news post as this is a common channel for home users [26, 70] and may be communicated itself by word-of-mouth or analogy [71]. Furthermore, including the price of the IoT device could have influenced expectations, with cheaper devices perhaps being seen as more vulnerable and premium products leading to higher expectations. However, adding more contextual factors to the vignettes' factorial design would have led to an explosion of factor level combinations. Thus, we encourage future work to explore such directions.

Finally, participants had to judge a fictional user's actions, such that it needs to be determined if this judgement would translate into actual behaviour on their side, though text answers imply that participants had similar experiences to those captured in our vignettes, as presented in subsection 4.3.

6 Conclusion

Using a vignette survey with 862 participants, we found differing expectations around the responsibilities of users and manufacturers how arising security and privacy events would and should be handled. Future work should look at other factors related to product liability law however, such as the state of the market and behavior

of competitors. Future work should also go beyond the vignette factors considered here, to explore the impact of other factors on expectations, e.g., duration of device ownership and price, warranty conditions, and timeliness of manufacturer response.

Acknowledgments

This work has been partially supported by the INTERSCT project, Grant No. NWA.1160.18.301, funded by Netherlands Organisation for Scientific Research (NWO). The findings reported herein are solely responsibility of the authors.

References

- [1] Denielle Abaquita et al. "Privacy norms within the internet of things using contextual integrity". In: *Companion of the 2020 ACM International Conference on Supporting Group Work*. 2020, pp. 131–134.
- [2] Noura Abdi, Kopo M Ramokapane, and Jose M Such. "More than smart speakers: security and privacy perceptions of smart home personal assistants". In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 2019, pp. 451–466.
- [3] Noura Abdi et al. "Privacy norms for smart home personal assistants". In: *Proceedings of the 2021 CHI conference on human factors in computing systems*. 2021, pp. 1–14.
- [4] Lawrence Abrams. QNAP force-installs update after DeadBolt ransomware hits 3,600 devices. en-us. 2022. URL: <https://www.bleepingcomputer.com/news/security/qnap-force-installs-update-after-deadbolt-ransomware-hits-3-600-devices/>.
- [5] Sara Amini and Chris Kanich. "Characterizing the impact of malware infections and remediation attempts through support forum analysis". In: *2017 APWG Symposium on Electronic Crime Research (eCrime)*. 2017, pp. 70–78. DOI: 10.1109/ECRIME.2017.7945056.
- [6] District Court of Appeal of the State of Florida. *Grieco v. Daiho Sangyo, Inc.* 2022. URL: <https://law.justia.com/cases/florida/fourth-district-court-of-appeal/2022/20-2294.html>.
- [7] Noah Apthorpe et al. "Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity". en. In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2.2 (2018), pp. 1–23. ISSN: 2474-9567. DOI: 10.1145/3214262.
- [8] Katrin Auspurg and Thomas Hinz. *Factorial survey experiments*. Vol. 175. Sage Publications, 2014. ISBN: 1-4833-1289-5.
- [9] An Baeyens and Tom Goffin. "Boston Scientific Medizintechnik GmbH v. AOK Sachsen-Anhalt". In: *European journal of health law* 22.3 (2015), pp. 301–307. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62013CJ0503>.
- [10] Paritosh Bahirat et al. "Overlooking Context: How do Defaults and Framing Reduce Deliberation in Smart Home Privacy Decision-Making?" en. In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, 2021, pp. 1–18. ISBN: 978-1-4503-8096-6. DOI: 10.1145/3411764.3445672.
- [11] Natã M Barbosa, Zhuohao Zhang, and Yang Wang. "Do Privacy and Security Matter to Everyone? Quantifying and Clustering User-Centric Considerations About Smart Home Device Adoption". In: *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. 2020, pp. 417–435.
- [12] A. Barth et al. "Privacy and contextual integrity: framework and applications". In: *2006 IEEE Symposium on Security and Privacy (S&P'06)*. 2006, 15 pp.–198. DOI: 10.1109/SP.2006.32.
- [13] Adam Beaument et al. "Productive security: A scalable methodology for analysing employee security behaviours". In: *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. 2016, pp. 253–270.

- [14] Ingolf Becker, Simon Parkin, and M Angela Sasse. "Measuring the Success of Context-Aware Security Behaviour Surveys". In: *The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER 2017)*. 2017, pp. 77–86.
- [15] John M. Blythe, Lynne Coventry, and Linda Little. "Unpacking security policy compliance: The motivators and barriers of employees' security behaviors". In: *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security*. SOUPS '15. USENIX Association, 2015, pp. 103–122. ISBN: 978-1-931971-24-9.
- [16] Brennen Bouwmeester et al. "'The Thing Doesn't Have a Name': Learning from Emergent Real-World Interventions in Smart Home Security". In: *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. 2021, pp. 493–512.
- [17] Virginia Braun and Victoria Clarke. "One size fits all? What counts as quality practice in (reflexive) thematic analysis?" In: *Qualitative research in psychology* 18.3 (2021), pp. 328–352.
- [18] Michael Brown. *Ring announces 6 new products, along with measures to quiet criticism of its privacy practices*. en. 2020. URL: <https://www.techhive.com/article/584254/ring-announces-6-new-products-along-with-measures-to-quiet-criticism-of-its-privacy-practices.html>.
- [19] Jonathan Bundy and Michael D. Pfarrer. "A Burden of Responsibility: The Role of Social Approval at the Onset of a Crisis". In: *Academy of Management Review* 40.3 (2015), pp. 345–369. ISSN: 0363-7425. DOI: 10.5465/amr.2013.0027.
- [20] Jonathan Bundy et al. "Crises and Crisis Management: Integration, Interpretation, and Research Development". en. In: *Journal of Management* 43.6 (2017), pp. 1661–1692. ISSN: 0149-2063. DOI: 10.1177/0149206316680030.
- [21] State of California. "California Consumer Privacy Act". In: (2018). URL: https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.
- [22] Orçun Çetin et al. "Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai." In: *NDSS*. 2019.
- [23] George Chalhoub et al. "'It did not give me an option to decline': A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products". en. In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, 2021, pp. 1–16. ISBN: 978-1-4503-8096-6. DOI: 10.1145/3411764.3445691.
- [24] Catalin Cimpanu. *Hackers are hijacking smart building access systems to launch DDoS attacks*. en. 2020. URL: <https://www.zdnet.com/article/hackers-are-hijacking-smart-building-access-systems-to-launch-ddos-attacks/>.
- [25] Sauvik Das, Laura A Dabbish, and Jason I Hong. "A Typology of Perceived Triggers for End-User Security and Privacy Behaviors". In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 2019, pp. 97–115.
- [26] Sauvik Das et al. "Breaking! A typology of security and privacy news and how it's shared". In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 2018, pp. 1–12.
- [27] Wendy Davis. *Vizio Hit With Privacy Lawsuit Over Connected TVs*. en. 2015. URL: <https://www.mediapost.com/publications/article/262835/vizio-hit-with-privacy-lawsuit-over-connected-tvs.html>.

- [28] Mattt Day, Giles Turner, and Natalia Drozdiak. *Thousands of Amazon Workers Listen to Alexa Users' Conversations*. en. 2019. URL: <https://time.com/5568815/amazon-workers-listen-to-alexa/>.
- [29] Benjamin Dean. *An Exploration of Strict Products Liability and the Internet of Things*. en. Tech. rep. Center for Democracy and Technology, 2018. URL: <https://cdt.org/wp-content/uploads/2018/04/2018-04-16-IoT-Strict-Products-Liability-FNL.pdf> (visited on 09/28/2022).
- [30] Department for Digital, Culture, Media and Sport (UK Government). "Code of Practice for Consumer IoT Security". In: (2018). URL: <https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security>.
- [31] Pardis Emami-Naeini et al. "Exploring How Privacy and Security Factor into IoT Device Purchase Behavior". en. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 2019, pp. 1–12. ISBN: 978-1-4503-5970-2. DOI: 10.1145/3290605.3300764.
- [32] Pardis Emami-Naeini et al. "Ask the Experts: What Should Be on an IoT Privacy and Security Label?" In: *2020 IEEE Symposium on Security and Privacy (SP)*. 2020, pp. 447–464. DOI: 10.1109/SP40000.2020.00043.
- [33] Pardis Emami-Naeini et al. "Which Privacy and Security Attributes Most Impact Consumers' Risk Perception and Willingness to Purchase IoT Devices?" In: *2021 IEEE Symposium on Security and Privacy (SP)*. 2021, pp. 519–536. DOI: 10.1109/SP40001.2021.00112.
- [34] ENISA. "Good Practices for Security of IoT - Secure Software Development Lifecycle". In: (2019). URL: <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1>.
- [35] Michael Fagan et al. *Foundational Cybersecurity Activities for IoT Device Manufacturers*. en. Tech. rep. NIST Internal or Interagency Report (NISTIR) 8259. National Institute of Standards and Technology, 2020. DOI: 10.6028/NIST.IR.8259. URL: <https://csrc.nist.gov/publications/detail/nistir/8259/final> (visited on 08/04/2022).
- [36] Nathan Favero and Minjung Kim. "Everything Is Relative: How Citizens Form and Use Expectations in Evaluating Services". In: *Journal of Public Administration Research and Theory* 31.3 (2021), pp. 561–577. ISSN: 1053-1858. DOI: 10.1093/jopart/muaa048.
- [37] Alisa Frik et al. "Privacy and security threat models and mitigation strategies of older adults". In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 2019, pp. 21–40.
- [38] Sandra Gabriele and Sonia Chiasson. "Understanding Fitness Tracker Users' Security and Privacy Knowledge, Attitudes and Behaviours". en. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, 2020, pp. 1–12. ISBN: 978-1-4503-6708-0. DOI: 10.1145/3313831.3376651.
- [39] Andy Greenberg. "After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix". en-US. In: *Wired* (2015). ISSN: 1059-1028. URL: <https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/> (visited on 09/27/2022).

- [40] Julie Haney, Yasemin Acar, and Susanne Furman. ““It’s the Company, the Government, You and I”: User Perceptions of Responsibility for Smart Home Privacy and Security”. In: *30th USENIX Security Symposium (USENIX Security 21)*. 2021, pp. 411–428.
- [41] Julie M. Haney, Susanne M. Furman, and Yasemin Acar. “Smart Home Security and Privacy Mitigations: Consumer Perceptions, Practices, and Challenges”. en. In: *HCI for Cybersecurity, Privacy and Trust*. Ed. by Abbas Moallem. Lecture Notes in Computer Science. Springer International Publishing, 2020, pp. 393–411. ISBN: 978-3-030-50309-3. DOI: 10.1007/978-3-030-50309-3_26.
- [42] Ayako A Hasegawa et al. “Understanding Non-Experts’ Security-and Privacy-Related Questions on a Q&A Site”. In: *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 2022, pp. 39–56.
- [43] Bronwyn Higgs, Michael Jay Polonsky, and Mary Hollick. “Measuring expectations: forecast vs. ideal expectations. Does it really matter?” In: *Journal of retailing and consumer services* 12.1 (2005), pp. 49–64.
- [44] Sijia Jiang and Jim Finkle. “China’s Xionghai to recall up to 10,000 webcams after hack”. en. In: *Reuters* (2016). URL: <https://www.reuters.com/article/us-cyber-attacks-china-idUSKCN12P1TT> (visited on 09/27/2022).
- [45] Haojian Jin et al. “Exploring the Needs of Users for Supporting Privacy-Protective Behaviors in Smart Homes”. en. In: *CHI Conference on Human Factors in Computing Systems*. ACM, 2022, pp. 1–19. ISBN: 978-1-4503-9157-3. DOI: 10.1145/3491102.3517602.
- [46] Kat Krol et al. “Towards robust experimental design for user studies in security and privacy”. In: *The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER 2016)*. 2016, pp. 21–31.
- [47] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. “Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers”. en. In: *Proceedings of the ACM on Human-Computer Interaction* 2.CSCW (2018), pp. 1–31. ISSN: 2573-0142. DOI: 10.1145/3274371.
- [48] Ye Li et al. “The More You Ask, the Less You Get: When Additional Questions Hurt External Validity”. en. In: *Journal of Marketing Research* (2021). ISSN: 0022-2437. DOI: 10.1177/00222437211073581.
- [49] Karola Marky et al. ““I don’t know how to protect myself”: Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments”. In: *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*. 2020, pp. 1–11.
- [50] Kirsten Martin and Katie Shilton. “Why experience matters to privacy: How context-based experience moderates consumer privacy expectations for mobile applications”. en. In: *Journal of the Association for Information Science and Technology* 67.8 (2016), pp. 1871–1882. ISSN: 2330-1643. DOI: 10.1002/asi.23500.
- [51] Clayton J Masterman and W Kip Viscusi. “The Specific Consumer Expectations Test for Product Defects”. In: *Ind. LJ* 95 (2020), p. 183.
- [52] Joseph Menn, Jim Finkle, and Dustin Volz. “Cyber attacks disrupt PayPal, Twitter, other sites”. In: *Reuters* (2016). URL: <https://www.reuters.com/article/us-usa-cyber-idUSKCN12L1ME> (visited on 09/27/2022).

- [53] Philipp Morgner et al. "Security Update Labels: Establishing Economic Incentives for Security Patching of IoT Consumer Products". In: *2020 IEEE Symposium on Security and Privacy (SP)*. 2020, pp. 429–446. DOI: 10.1109/SP40000.2020.00021.
- [54] Mozilla. **Privacy not included*. <https://foundation.mozilla.org/en/privacynotincluded/>. 2021.
- [55] Pardis Emami Naeini et al. "Privacy expectations and preferences in an IoT world". In: *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. 2017, pp. 399–412.
- [56] RVO Netherlands Enterprise Agency. "Supplying updates is mandatory". In: (2022). URL: <https://business.gov.nl/amendment/supplying-updates-to-become-mandatory/>.
- [57] BBC News. "Google seeks permission for staff to listen to Assistant recordings". en-GB. In: *BBC News* (2019). URL: <https://www.bbc.com/news/technology-49796207> (visited on 09/27/2022).
- [58] Geoff Norman. "Likert scales, levels of measurement and the "laws" of statistics". en. In: *Advances in Health Sciences Education* 15.5 (2010), pp. 625–632. ISSN: 1573-1677. DOI: 10.1007/s10459-010-9222-y.
- [59] Norbert Nthala and Ivan Flechais. "Informal support networks: an investigation into home data security practices". In: *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 2018, pp. 63–82.
- [60] Lindsey O'Donnell. *EU Recalls Children's Smartwatch That Leaks Location Data*. 2019. URL: <https://threatpost.com/eu-recalls-childrens-smartwatch-that-leaks-location-data/141511/>.
- [61] Lindsey O'Donnell. *Unpatched Security Flaws Open Connected Vacuum to Takeover*. en. 2020. URL: <https://threatpost.com/unpatched-security-flaws-open-connected-vacuum-to-takeover/153142/>.
- [62] Charlie Osborne. *Remote code execution flaw allowed hijack of Motorola Halo+ baby monitors*. en. 2021. URL: <https://portswigger.net/daily-swig/remote-code-execution-flaw-allowed-hijack-of-motorola-halo-baby-monitors> (visited on 09/27/2022).
- [63] Charlie Osborne. *Researcher discloses alleged zero-day vulnerabilities in NUUO NVRmini2 recording device*. en. 2022. URL: <https://portswigger.net/daily-swig/researcher-discloses-alleged-zero-day-vulnerabilities-in-nuuo-nvrmini2-recording-device> (visited on 09/27/2022).
- [64] Pierluigi Paganini. *Watch out, FLocker Ransomware targets Android smart TVs*. en-US. 2016. URL: <https://securityaffairs.co/wordpress/48383/iot/flocker-ransomware-smart-tvs.html> (visited on 09/27/2022).
- [65] Simon Parkin et al. "Security when it is welcome: Exploring device purchase as an opportune moment for security behavior change". In: *Proceedings of the Workshop on Usable Security and Privacy (USEC'19)*. Internet Society. 2019.
- [66] Erika Shehan Poole et al. "Computer help at home: methods and motivations for informal technical support". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2009, pp. 739–748.

- [67] Lutz Preuss et al. "Corporate Scandals: Firm Response Strategies and Subsequent Media Coverage". In: *Academy of Management Proceedings* 2018.1 (2018), p. 18369. ISSN: 0065-0668. DOI: 10.5465/AMBPP.2018.18369abstract.
- [68] Prolific. en. URL: <https://www.prolific.co/> (visited on 09/21/2022).
- [69] Qualtrics. en. URL: <https://www.qualtrics.com>.
- [70] Emilee Rader and Rick Wash. "Identifying patterns in informal sources of security information". In: *Journal of Cybersecurity* 1.1 (2015), pp. 121–144.
- [71] Emilee Rader, Rick Wash, and Brandon Brooks. "Stories as informal lessons about security". In: *Proceedings of the Eighth Symposium on Usable Privacy and Security*. 2012, pp. 1–17.
- [72] Elsa Rodriguez et al. "Super-Spreaders: Quantifying the Role of IoT Manufacturers in Device Infections". In: *20th Annual Workshop on the Economics of Information Security (WEIS 2021)*. 2021.
- [73] Elsa Rodríguez et al. "Difficult for Thee, But Not for Me: Measuring the Difficulty and User Experience of Remediating Persistent IoT Malware". In: *arXiv preprint arXiv:2203.01683* (2022).
- [74] Asreen Rostami et al. "Being Hacked: Understanding Victims' Experiences of IoT Hacking". In: *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 2022, pp. 613–631.
- [75] Carsten Sauer, Katrin Auspurg, and Thomas Hinz. "Designing Multi-Factorial Survey Experiments: Effects of Presentation Style (Text or Table), Answering Scales, and Vignette Order". In: *Methods, data, analyses: a journal for quantitative methods and survey methodology (mda)* 14.2 (2020), pp. 195–214.
- [76] Bruce Schneier. *Ring Gives Videos to Police without a Warrant or User Consent - Schneier on Security*. 2022. URL: <https://www.schneier.com/blog/archives/2022/08/ring-gives-videos-to-police-without-a-warrant-or-user-consent.html> (visited on 09/27/2022).
- [77] Irina Shklovski et al. "Leakiness and creepiness in app space: Perceptions of privacy and mobile app use". en. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2014, pp. 2347–2356. ISBN: 978-1-4503-2473-1. DOI: 10.1145/2556288.2557421.
- [78] Yan Shvartzshnaider, Madelyn Rose Sanfilippo, and Noah Apthorpe. "Contextual Integrity as a Gauge for Governing Knowledge Commons". In: *Governing Privacy in Knowledge Commons*. Ed. by Madelyn Rose Sanfilippo, Brett M. Frischmann, and Katherine J. Strandburg. Cambridge Studies on Governing Knowledge Commons. Cambridge University Press, 2021, pp. 220–244. ISBN: 978-1-108-48514-2. DOI: 10.1017/9781108749978.010.
- [79] Yan Shvartzshnaider et al. "Learning Privacy Expectations by Crowdsourcing Contextual Informational Norms". en. In: *Proceedings of the AAAI Conference on Human Computation and Crowdsourcing* 4 (2016), pp. 209–218. ISSN: 2769-1349.
- [80] Dan Su and Peter M. Steiner. "An Evaluation of Experimental Designs for Constructing Vignette Sets in Factorial Surveys". en. In: *Sociological Methods & Research* 49.2 (2020), pp. 455–497. ISSN: 0049-1241. DOI: 10.1177/0049124117746427.

- [81] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. ““I don’t own the data”: End User Perceptions of Smart Home Device Data Practices and Risks”. In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 2019, pp. 435–450.
- [82] Madiha Tabassum et al. “Investigating Users’ Preferences and Expectations for Always-Listening Voice Assistants”. en. In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3.4 (2019), pp. 1–23. ISSN: 2474-9567. DOI: 10.1145/3369807.
- [83] Jenny Tang, Eleanor Birrell, and Ada Lerner. “Replication: How Well Do My Results Generalize Now? The External Validity of Online Privacy and Security Surveys”. In: *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 2022, pp. 367–385.
- [84] Huixin Tian et al. “Tech Pains: Characterizations of Lived Cybersecurity Experiences”. In: *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. 2020, pp. 250–259. DOI: 10.1109/EuroSPW51379.2020.00040.
- [85] Alan J. Tomassetti, Reeshad S. Dalal, and Seth A. Kaplan. “Is Policy Capturing Really More Resistant Than Traditional Self-Report Techniques to Socially Desirable Responding?” en. In: *Organizational Research Methods* 19.2 (2016), pp. 255–285. ISSN: 1094-4281. DOI: 10.1177/1094428115627497.
- [86] European Union. “Product Liability Directive”. In: (1985). URL: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31985L0374:en:HTML>.
- [87] European Union. “Radio Equipment Directive”. In: (2014). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0053>.
- [88] European Union. “General Data Protection Regulation”. In: (2016). URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.
- [89] European Union. *Questions and Answers: Strengthening cybersecurity of wireless devices and products*. 2021. URL: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_5635.
- [90] District Court for the Western District of Pennsylvania. *Cohen v. Johnson & Johnson*. 2022. URL: <https://law.justia.com/cases/federal/district-courts/pennsylvania/pawdce/2:2020cv00057/262978/68/>.
- [91] Daniel W Woods and Aaron Ceross. “Blessed Are The Lawyers, For They Shall Inherit Cybersecurity”. In: *New Security Paradigms Workshop*. 2021, pp. 1–12.
- [92] Yaxing Yao et al. “Defending my castle: A co-design study of privacy mechanisms for smart homes”. In: *Proceedings of the 2019 chi conference on human factors in computing systems*. 2019, pp. 1–12.
- [93] Eric Zeng, Shrirang Mare, and Franziska Roesner. “End user security and privacy concerns with smart homes”. In: *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. 2017, pp. 65–80.
- [94] Eric Zeng and Franziska Roesner. “Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study”. In: *28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association, 2019, pp. 159–176. ISBN: 978-1-939133-06-9.

- [95] Shikun Zhang et al. ““Did you know this camera tracks your mood?”: Understanding Privacy Expectations and Preferences in the Age of Video Analytics”. en. In: *Proceedings on Privacy Enhancing Technologies* 2021.2 (2021). DOI: 10.2478/popets-2021-0028.

4.

The Cyber Resilience Act and Open-Source Software: A Fine Balancing Act

This article was published in JIPITEC on 26 March 2025. The text was last revised on 14 January 2025, with some minor textual corrections for inclusion in this dissertation.

Mattis van 't Schip, 'The Cyber Resilience Act and Open-Source Software: A Fine Balancing Act' (2025) 16 JIPITEC 73.

In March 2026, the European Commission published a draft version of their guidance for the Cyber Resilience for public consultation. I point to the need for this guidance, specifically on the scope of the CRA regarding open-source software, in the following article.

Abstract

Open-source software, a type of software that can be publicly accessed, shared, and modified, is an integral part of the modern digital infrastructure. Many ICT products, from personal computers to internet-connected devices, run on open-source systems (e.g., Linux). Developers may work voluntarily or for limited compensation on such software. The character of this work, however, does not reduce the impact of cybersecurity incidents within open-source software. Proprietary software, meaning software with restrictive license models, regularly implements open-source software: a vulnerability in the open-source software thus directly affects proprietary software too. Recent large-scale vulnerabilities (e.g., Log4j) highlighted this dual nature of open-source software: developers work on projects based on personal passion or ideologies, while the software is often equally as critical as software created and maintained by larger technology enterprises.

The Cyber Resilience Act, the recently proposed European cybersecurity legislation for products, aims to offer a legal response to cybersecurity problems in modern software and hardware. This paper addresses the role of open-source software cybersecurity in the Cyber Resilience Act with specific attention to the difficulties of reconciling cybersecurity responsibilities and open-source products. The paper shows that the Cyber Resilience Act does achieve a balance between regulation for open-source software and advancing cybersecurity, but only through a narrowly applicable and, at times, complex legislative approach.

1 Introduction

Behind the facade of giant technology enterprises exists an ecosystem of ‘open-source software’. The source code of this type of software is publicly accessible and developers write the code under licenses that allow for use, redistribution, modification, and sharing by third parties. ‘Open source’ does not merely mean public access to source code. The Open Source Initiative (OSI), a body responsible for the generally accepted definition of ‘open source’, indicates that the concept holds certain additional criteria.¹ For instance, open-source software licenses should not discriminate based on intended use.²

Many types of open-source software support today’s largest software packages: Linux, an open-source operating system, powers many modern ICT products, from desktop computers to Internet of Things devices; millions of websites rely on Apache, an open-source web server. Open-source software is thus an important cornerstone of the modern digital infrastructure.³

The advantages of open-source software align with recent regulatory efforts in the EU that aim to curtail the market power of the major digital enterprises. For instance, the Digital Services Act regulates online platforms (and especially the “very large” online platforms, i.e., the major social media platforms), while the Digital Markets Act imposes responsibilities on “gatekeepers” (e.g., Microsoft, Meta).⁴ Open-source software can serve as transparent, public alternatives to these dominant platforms.

Like other types of software, open-source software comes with cybersecurity risks.⁵ For example, Log4j, a piece of open-source software for logging purposes, suffered a critical vulnerability which allowed hackers to remotely access systems.⁶ Some experts held that the vulnerability affected virtually every digital service globally.⁷ The Log4j vulnerability was

1 Open Source Initiative, ‘The Open Source Definition’ (22 March 2007) <<https://opensource.org/osd>> accessed 19 January 2024.

2 <<https://opensource.org/licenses/>>.

3 Chinmayi Sharma, ‘Tragedy of the Digital Commons’ (2023) 101 North Carolina Law Review 1129.

4 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC [2022] OJ L277/1 (Digital Services Act); Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 [2022] OJ L265/1 (Digital Markets Act).

5 Jaap-Henk Hoepman and Bart Jacobs, ‘Increased Security through Open Source’ (2007) 50 Communications of the ACM 79.

6 For an extensive overview, see Raphael Hiesgen and others, ‘The Log4j Incident: A Comprehensive Measurement Study of a Critical Vulnerability’ [2024] IEEE Transactions on Network and Service Management 1.

7 Sean Lyngaas, ‘US Warns Hundreds of Millions of Devices at Risk from Newly Revealed Software Vulnerability’ (CNN, 13 December 2021) <<https://www.cnn.com/2021/12/13/politics/us-warning-software-vulnerability/index.html>> accessed 19 January 2024; Ars Technica spoke of ‘arguably the most severe vulnerability ever’, see Dan Goodin, ‘As Log4Shell Wreaks Havoc, Payroll Service Reports Ransomware Attack’ (Ars Technica, 13 December 2021) <<https://arstechnica.com/information-technology/2021/12/as-log4shell-wreaks-havoc-payroll-service-reports-ransomware-attack/>> accessed 19 January 2024; Similarly, see the Guardian Associated Press, ‘Recently Uncovered Software Flaw “Most Critical Vulnerability of the Last Decade”’ *The Guardian* (11 December 2021) <<https://www.theguardian.com/technology/2021/dec/10/software-flaw-most-critical-vulnerability-log-4-shell>> accessed 19 January 2024.

critical because open-source software is often incorporated in larger proprietary software packages; the vulnerability in Log4j thus directly affected numerous other products.⁸

In September 2022, the European Commission introduced a new legislative proposal for the cybersecurity of software and hardware products, the Cyber Resilience Act.⁹ At the end of 2024, the Act came in effect.¹⁰ The Act applies when manufacturers and/or software developers place software or hardware products on the market of the European Union “in the course of a commercial activity”.¹¹ If they place these products on the market, software developers must implement certain cybersecurity requirements in their product and, in certain cases, follow strict assessment procedures.

Although this requirement potentially excludes open-source software, the ‘commercial activity’ condition offers few assurances, as evident from the legislative discussions surrounding its interpretation.¹² The commerciality of open-source software projects can range from monetising other services on the open-source software platform (e.g., Android) to occasional donations from end users (e.g., hobby projects).¹³ The Commission proposal merely mentioned these examples, but did not offer a further clarification of what “supplying in the course of a commercial activity” entails.

The text adopted by the Parliament, instead, includes a rather comprehensive set of Recitals, which cover many open-source software development and financing methods. The compromise text therefore exempts nearly every known type of open-source software development from the scope of the Cyber Resilience Act. This exemption helps developers, who do not have to comply with legal burdens for software that they provide openly to the public. At the same time, these broad exemptions could undermine the overall aim of the Cyber Resilience Act to improve the state of cybersecurity for software and hardware.

This paper analyses the difficulties of reconciling open-source software development with cybersecurity risk management responsibilities. The research question is: To what extent does the Cyber Resilience Act impose responsibilities on open-source software

8 Sharma (n 4) 1131–1133.

9 Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 COM(2022) 454 final [Cyber Resilience Act].

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

11 Art 3(22) CRA.

12 See the calls for support from the open source community when the Cyber Resilience Act proposal was published in, inter alia, Maarten Aertsen, ‘Open-Source Software vs. the Proposed Cyber Resilience Act’ (*The NLnet Labs Blog*, 14 November 2022) <<https://blog.nlnetlabs.nl/open-source-software-vs-the-cyber-resilience-act/>> accessed 20 December 2023; Deb Nicholson, ‘Python Software Foundation News: The EU’s Proposed CRA Law May Have Unintended Consequences for the Python Ecosystem’ (*Python Software Foundation News*, 11 April 2023) <<https://pyfound.blogspot.com/2023/04/the-eus-proposed-cra-law-may-have.html>> accessed 20 December 2023; Simon Phipps, ‘What Is the Cyber Resilience Act and Why It’s Dangerous for Open Source’ (*Voices of Open Source*, 24 January 2023) <<https://blog.opensource.org/what-is-the-cyber-resilience-act-and-why-its-important-for-open-source/>> accessed 20 December 2023.

13 David A Wheeler, ‘F/LOSS Is Commercial Software’ [2009] Open Source Business Resource <<http://timreview.ca/article/229>>.

developers that achieve a balance between stimulating open-source software development and, simultaneously, mitigating cybersecurity problems within open-source software?

This paper proceeds as follows. Section 2 summarises the history and meaning of open-source software and its cybersecurity implications. Section 3 discusses the Cyber Resilience Act, with specific attention to the definition of supplying a product ‘in the course of a commercial activity’ for open-source software products. Section 4 highlights, using several examples, how difficult an assessment of ‘supplying in the course of a commercial activity’ is under the current legal terminology in the Recitals. Section 5 then looks at specific rules pointed at open-source software within the Cyber Resilience Act, such as the special regulatory regime for ‘open-source software stewards’. On the basis of this legal framework, Section 6 questions whether the Cyber Resilience Act now achieves a balance between encouraging open-source software development and mitigating cybersecurity problems. Based on this balance, Section 7 looks at the future of open-source software under EU law. Section 8 concludes.

2 Open-source software

Open-source software originates in an academic environment. At MIT, Richard Stallman intended to design a free operating system that opposed the barriers developing against sharing software in the 1980’s.¹⁴ To support the GNU project, Stallman established the Free Software Foundation (FSF). The FSF focused on free access and usability of software (‘a matter of liberty’¹⁵) instead of ‘free of charge’ software.¹⁶ A decade later, the quickly growing community surrounding ‘free software’ moved towards a new label: ‘open source’. The ‘free’ label was unattractive to many companies, which prevented larger enterprises from becoming involved in the development of ‘free’ software.¹⁷ Therefore, under the Open Source Initiative, the community created a definition for ‘open-source’ software next to ‘free’ software.¹⁸

Open-source software is a type of software with source code that is publicly accessible. The use of open-source software comes with some requirements, which different developers have formalised in specific licenses.¹⁹ Some developers, for instance, specify that users accept that they receive the software ‘as-is’, so that the developers cannot be held liable for damages caused by the software.²⁰ At the same time, the licenses also formalise that the developers cannot discriminate based on the envisioned use of the software: any type of user (e.g., large technology companies, hobby developers) can freely access and use the code how they desire (e.g., modification, sharing).²¹

14 Richard Stallman, ‘Initial Announcement’ (GNU, 27 September 1983) <<https://www.gnu.org/gnu/initial-announcement.html>> accessed 19 January 2024.

15 ‘What Is Free Software? - GNU Project - Free Software Foundation’ <<https://www.gnu.org/philosophy/free-sw.html.en>> accessed 13 January 2025.

16 Moreno Muffatto, *Open Source: A Multidisciplinary Approach* (Imperial College Press 2006) 7.

17 ‘History of the OSI’ (*Open Source Initiative*, 19 September 2006) <<https://opensource.org/history/>> accessed 19 January 2024.

18 Open Source Initiative (n 2); Muffatto (n 17) 14.

19 P McCoy Smith, ‘Copyright, Contract, and Licensing in Open Source’ in Amanda Brock (ed), *Open Source Law, Policy and Practice* (2nd edn, Oxford University Press 2022).

20 See, as an example, the 1-clause BSD license: <<https://opensource.org/license/bsd-1-clause>>.

21 Open Source Initiative (n 2).

This Section analyses open-source software and its unique characteristics in comparison to its counterpart, proprietary/closed-source software. In addition, the Section highlights the cybersecurity characteristics of both software development methods.

2.1 The development and ideologies of open-source software

Open-source software is published on a diverse set of platforms by equally diverse developers. Developers participate to different degrees (e.g., occasional code change to full-time work), receive different types of remuneration (e.g., full salary, donations), and contribute based on diverse motivations (e.g., passion, peer recognition). This diversity laid the groundwork for ‘open source’ as a community of people involved with all types of projects that aim at providing open access to information and knowledge, such as open-source software and open access science.

The counterparts to open-source software exists in two forms: proprietary software (restrictive licensing) and closed-source software (restricted access to source code). Proprietary software works with licenses that severely restrict the user in their use of the software (e.g., no modifying the source code). Proprietary software can thus also be open-source software, as software with publicly accessible source code but a restrictive license.²² In addition, proprietary software exists as closed-source software, where the source code is not available *and* the license restricts the user. Open-source or closed-source software is thus a choice during the development phase of a software package, while proprietary software refers to the distribution phase.

The dichotomy between open-source and proprietary/closed-source software can be illustrated through the Linux and Microsoft Windows operating systems: Linux is an open-source operating system, with many different versions existing today, because the license allows modification of the code (e.g., Linux Mint, Ubuntu, Arch Linux).²³ Microsoft develops the proprietary and closed-source Windows operating system; its source code is not publicly available and its license restricts any modification to the Windows source code. Microsoft thus solely develops and controls the different Windows versions.

Open-source software exists in many forms. Linux is a prominent example because, as a popular operating system, it has millions of users. However, open-source software also exists on a smaller scale, for example as a small web app that maybe a hundred people may use. When the software license complies with the open source definition of the Open Source Initiative (OSI),²⁴ the open source community considers it open-source software.²⁵

There is no singular form of organization behind open-source software development.²⁶ Since open-source software is usually – but certainly not always – free for users, open-source software developers often rely on smaller financial resources to build their software. Open-source developers often have other intrinsic and extrinsic motives. Intrinsic motives rely on “the tendency to seek out novelty and challenges” (e.g., improving knowledge of a certain

22 For some examples, see <https://en.wikipedia.org/wiki/List_of_proprietary_source-available_software>.

23 For an extensive list of Linux distributions, see <https://en.wikipedia.org/wiki/List_of_Linux_distributions>.

24 <<https://opensource.org/licenses/>>.

25 This does not mean that there are no open-source software licenses outside the OSI’s list, but merely that the OSI has not (yet) classified them as compliant with the open source definition.

26 Muffatto (n 17) ch 3.

programming language), while extrinsic motives focus on the outcome of certain conduct (e.g., improving reputation among peers in the development community).²⁷ Some developers therefore band together under a non-commercial entity and offer technical support to their largest users for a fee, while other developers work on projects completely voluntarily or based on small donations from end users.

In connection to the structure of different open-source software, the users of the software differ considerably, as anyone can access the software's source code. Major technology enterprises frequently use open-source software as a foundation on which they build their proprietary software packages; individuals might instead use open-source software because of its lower cost or as an alternative to the monopoly power of large technology enterprises.²⁸

In line with these different structures and users of software, I identify three types of open-source software projects: 1) a standalone open-source project (e.g., a developer publishing some personal code); 2) open-source software incorporated into other proprietary and/or open-source software (e.g., Log4j);²⁹ 3) commercialized open-source software (e.g., where the organisation requires a fee for usage).³⁰ The difference between a standalone project (1) and an integrated project (2) largely relies on the use case of the software package, since some packages do not offer standalone functionalities.³¹ Section 3 illustrates the meaning of this categorization within the legal framework of the Cyber Resilience Act.

Open-source developers often publish the source code of their software on online repositories (e.g., GitHub, SourceForge, personal websites). Other developers can access the code there, and download it for further use, or review the code and offer feedback.³²

Open-source software is part of the broader 'open source' movement, which is based on certain philosophical (e.g., about information and knowledge) or pragmatic beliefs (e.g., free alternatives for users) about the need for open-source software.³³ These beliefs explain the altruistic nature of open source and relate back to the Free Software Foundation: many developers offer their software to the public because they are part of a wider community movement which aims to keep knowledge, in a broad sense, publicly accessible and shareable.³⁴

27 Jürgen Bitzer, Wolfram Schrettl and Philipp JH Schröder, 'Intrinsic Motivation in Open Source Software Development' (2007) 35 *Journal of Comparative Economics* 160; Muffatto (n 17) 58–62.

28 Muffatto (n 17) 62–64.

29 For instance, on Microsoft's evolving stance towards open-source software, see Benjamin J Birkinbine, *Incorporating the Digital Commons: Corporate Involvement in Free and Open Source Software* (University of Westminster Press 2020) 49–72.

30 RedHat is the most prolific example of such projects, see also *ibid* 73–88; Although Red Hat recently changed its company policies, to the dismay of the open source community, Kevin Purdy, 'Red Hat's New Source Code Policy and the Intense Pushback, Explained' (*Ars Technica*, 30 June 2023) <<https://arstechnica.com/information-technology/2023/06/red-hats-new-source-code-policy-and-the-intense-pushback-explained/>> accessed 13 December 2023.

31 The Cyber Resilience Act also speaks of certain types of open-source software 'intended for integration by other manufacturers'. Recital 18 CRA.

32 GitHub had more than 400 million contributions to open-source projects in 2022. See <<https://github.blog/news-insights/research/octoverse-2022-10-years-of-tracking-open-source/>>.

33 Ian Walden, 'Open Source as Philosophy, Methodology, and Commerce: Using Law with Attitude' in Amanda Brock (ed), *Open Source Law, Policy and Practice* (2nd edn, Oxford University Press 2022).

34 Charlotte Hess and Elinor Ostrom (eds), *Understanding Knowledge as a Commons: From Theory to Practice* (MIT Press 2007).

2.2 Open-source software and cybersecurity

Open-source software represents a deliberate choice for transparency: the source code of the software is accessible and the developers are transparent about its inner workings. An alternative to such transparency is ‘security through obscurity’.³⁵ This dichotomy between ‘transparency’ and ‘obscurity’ forms the foundation for many security-related discussions about open-source software.³⁶

By hiding the inner workings of the software, closed-source software does not show its internal processes; attackers cannot view the source code to discover exploitable vulnerabilities.³⁷ In contrast, advocates for open-source software development believe transparency allows open-source software to be more secure.³⁸ In the following, I illustrate the security dynamics of open-source and closed-source software in two phases: 1) during the development of the software and 2) after publication of the software.

2.2.1 Development of software

Proponents often use the transparent nature of open-source software as an argument that open-source software is more secure; if developers can peer review source code, they can identify and patch vulnerabilities and similar problems quickly.³⁹

Raymond coined this view of security of open source code as ‘Linus’ Law’: “Given a large enough beta-tester and co-developer base, almost every problem will be characterized quickly and the fix obvious to someone.”⁴⁰ Thus, an open-source software package is more secure if – and only if – many developers view and co-operate on the source code as the project benefits from their diverse views.⁴¹

The prevention of backdoors is an example of the benefits of the ‘many eyeballs’ system. If attackers change the source code of open-source software to allow themselves backdoor access to the system, or if the backdoor existed from the start, other developers can easily notice such changes and prevent the attackers from exploiting the backdoor.⁴² This is not the case for closed-source systems, where such backdoors are not immediately visible to others.

An opposing view to the ‘many eyeballs’ principle of Linus’ Law is the view of ‘too many cooks in the kitchen’.⁴³ In the latter view, the security of open-source software diminishes because

35 Hoepman and Jacobs (n 6).

36 Charles-H Schulz, ‘Open Source Software and Security: Practices, Governance, History, and Perceptions’ in Amanda Brock (ed), *Open Source Law, Policy and Practice* (2nd edn, Oxford University Press 2022); Christian Payne, ‘On the Security of Open Source Software’ (2002) 12 *Information Systems Journal* 61.

37 Ross Anderson, ‘Open and Closed Systems Are Equivalent (That Is, in an Ideal World)’ in Joseph Feller and others (eds), *Perspectives on free and open source software* (MIT Press 2005).

38 Eric Raymond, ‘The Cathedral and the Bazaar’ (1999) 12 *Knowledge, Technology & Policy* 23.

39 *ibid.*

40 ‘Linus’ refers to the founder of the Linux operating system, Linus Torvalds. Raymond also more informally coins Linus’ Law as “Given enough eyeballs, all bugs are shallow”, see *ibid* 29.

41 Raymond (n 39).

42 Payne (n 37) 66–67.

43 Andrew Meneely and Laurie Williams, ‘Secure Open Source Collaboration: An Empirical Study of Linus’ Law’, *Proceedings of the 16th ACM conference on Computer and communications security* (ACM 2009) 453; Ann Barcomb and others, ‘Managing Episodic Volunteers in Free/Libre/Open Source Software Communities’ (2022) 48 *IEEE Transactions on Software Engineering* 260.

too many developers are working on the software simultaneously and in fragmented ways.⁴⁴ A single developer may decide to contribute solely to their preferred elements of the project, without contributing to the overall project goals. This ‘unfocused contribution’ forms a security risk.⁴⁵ Unfocused contributions disrupt the concept of Linus’ Law in large-scale open-source projects, as the additional ‘eyeballs’ do not necessarily improve the project.⁴⁶ Therefore, the idea that open-source software is more secure simply because a diverse set of developers can access the source code is not clearly proven.

2.2.2 Post-release vulnerabilities

Linus’ Law mainly relates to the development phase of open-source software projects. However, security problems can also develop in the post-release phase, after publication of the software or a new version release.

In a comprehensive study, Schryen found that there was no statistical significance in terms of the severity of vulnerabilities between open-source and closed-source software equivalents.⁴⁷ He also found that the type of patching behaviour, in terms of speed and type of vulnerabilities, differed significantly between different open-source and closed-source vendors. This difference existed across open-source and closed-source vendors: the mode of open-source or closed-source development seemed, therefore, not to influence patching behaviour.⁴⁸

Ransbotham analyses how threat actors exploit vulnerabilities differently between open-source and closed-source projects based on two years of log data from intrusion detection systems.⁴⁹ He holds that vulnerabilities of open-source software projects have a generally greater risk of exploitation and receive more exploitation attempts. These differences can be partially attributed to the difference in transparency between open- and closed-source software. If a vulnerability is discovered internally in a closed-source environment, the developers have some additional time to work on fixing the vulnerability before they make the changes public. In open-source projects, changes in the source code – and thus possible vulnerabilities – are immediately publicly accessible.⁵⁰

In general, there are thus small differences between open-source and closed-source software security, both in the development and post-release phase. Vulnerabilities exist in and impact both types of software.

44 Martin Pinzger, Nachiappan Nagappan and Brendan Murphy, ‘Can Developer-Module Networks Predict Failures?’, *Proceedings of the 16th ACM SIGSOFT International Symposium on Foundations of software engineering* (ACM 2008).

45 Meneely and Williams (n 44) 456.

46 Meneely and Williams (n 44); Andrew Meneely and Laurie Williams, ‘Strengthening the Empirical Analysis of the Relationship between Linus’ Law and Software Security’, *Proceedings of the 2010 ACM-IEEE International Symposium on Empirical Software Engineering and Measurement* (ACM 2010).

47 Guido Schryen, ‘Is Open Source Security a Myth?’ (2011) 54 *Communications of the ACM* 130, 136–137.

48 *ibid* 139.

49 Sam Ransbotham, ‘An Empirical Analysis of Exploitation Attempts Based on Vulnerabilities in Open Source Software’ [2010] *Workshop on the Economics of Information Security* 1.

50 *ibid* 5.

3 The Cyber Resilience Act and open-source software cybersecurity

European law did not consider cybersecurity rules for open-source software until 2022. This lack of regulation changed when the European Commission proposed the ‘Cyber Resilience Act’, which contained specific rules for open-source software cybersecurity.⁵¹ The Cyber Resilience Act was adopted at the end of November 2024 and comes into effect on 10 December 2024.⁵²

3.1 The Cyber Resilience Act in short

The Cyber Resilience Act imposes 1) *cybersecurity requirements* on 2) *manufacturers* of 3) *products with digital elements* that they 4) *place on the Union’s market* in the course of a 5) *commercial activity*.⁵³ Below, I briefly review these elements in light of the applicability of the Act to open-source software.⁵⁴

3.1.1 Cybersecurity requirements

The cybersecurity requirements for products with digital elements form the focal point of the Cyber Resilience Act. These requirements include security throughout the lifecycle of the product (security-by-design), releasing the product without known exploitable vulnerabilities, and protection of the integrity and authenticity of data.⁵⁵ Next to these requirements, the Act contains traditional product requirements (e.g., providing documentation) and security-specific duties (e.g., providing security updates).⁵⁶

There are two main methods for developers to show their compliance in the proposal: 1) performing a self-assessment; and 2) receiving a third-party audit.⁵⁷ In general, the choice for a specific route depends on the type of product. The Cyber Resilience Act categorises products with certain privileges in networks or computer systems (e.g., password managers, operating systems) as ‘important’ products.⁵⁸ Important products must, if they cannot follow certain European technical standards, perform a third-party audit to prove their compliance with the Act’s requirements.⁵⁹ Open-source software is exempted from a third-party audit, even if they are considered ‘important products’, as long as they provide technical documentation to the public.⁶⁰

51 Cyber Resilience Act proposal (n 10).

52 Cyber Resilience Act (n 11).

53 Art 1 CRA.

54 See also Liane Colonna, ‘The End of Open Source? Regulating Open Source under the Cyber Resilience Act and the New Product Liability Directive’ (2025) 56 Computer Law & Security Review 106105.

55 Annex I Part 1 CRA.

56 Art 13 CRA.

57 Art 32(1) CRA.

58 Art 7(1) CRA & Annex III CRA. The Commission proposal used the term ‘critical’ products, which is now an even more critical class above important products.

59 Art 32(2) CRA.

60 Art 32(5) & Recital 91 CRA.

The provision and the supporting Recital do not indicate a reason for this exemption. However, many open-source software packages have certain elevated privileges and would therefore be important products (e.g., Log4j). In that context, the Parliament and Council most likely wanted to prevent a ‘chilling effect’ on open-source software development in the face of possibly costly third-party audits.

A further category exists for ‘critical’ products with digital elements, with even stricter conformity requirements.⁶¹ The Act currently lists three critical products: hardware devices with security boxes; smart meter gateways; and smartcards.⁶²

3.1.2 Manufacturers

A manufacturer is a “natural or legal person who develops or manufactures products with digital elements”.⁶³ Both traditional hardware manufacturers and software developers are ‘manufacturers’ under the Cyber Resilience Act. In case manufacturers do not strictly produce the product themselves, but place their trademark on products produced by another actor, they remain the manufacturer of the final product.⁶⁴

As highlighted above, not all open-source software forms a standalone package. Some of the most prominent open-source software packages derive their popularity from integration by proprietary software developers. Google, for instance, uses numerous pieces of open-source software, such as databases,⁶⁵ for their own software packages (e.g., Google Maps). Google, in this example, creates and markets their end product and is thus the manufacturer for the end product under the Cyber Resilience Act.⁶⁶ The proprietary developers must thus also ensure that they securely integrate the open-source database system – the open-source developer is not responsible for compliance in this case.⁶⁷ I delve into this separation further in Section 5.2.

The Cyber Resilience Act includes a set of rules for importers and distributors too. These rules ensure that manufacturers cannot evade compliance by letting importers and distributors bring the product to the Union market.⁶⁸ An importer brings products with digital elements to the Union market of “a natural or legal person established outside the Union.”⁶⁹ A distributor is an actor that is not a manufacturer or importer, but who still places the product on the market.⁷⁰ Importers and distributors have separate responsibilities to ensure that the products they place on the Union market comply with the requirements of the Cyber Resilience Act.⁷¹

61 Art 8 & Art 32(4) CRA.

62 Annex IV CRA.

63 Art 3(13) CRA.

64 Art 3(13) CRA.

65 For instance, Google moved their database systems to the open-source MariaDB, see Jack Clark, ‘Google Swaps out MySQL, Moves to MariaDB’ *The Register* (12 September 2013) <https://www.theregister.com/2013/09/12/google_mariadb_mysql_migration/> accessed 14 August 2024.

66 Art 3(13) & Art 13(5) CRA.

67 Izquierdo Grau analyses this division between standalone open-source and integrated open-source in the context of the recent Product Liability Directive proposal, see Guillem Izquierdo Grau, ‘An Appraisal of the Proposal for a Directive on Liability for Defective Products’ (2023) 12 *Journal of European Consumer and Market Law* 198.

68 Art 19 & 20 CRA.

69 Art 3(16) CRA.

70 Art 3(17) CRA.

71 Art 19(2) & 20(2) CRA.

3.1.3 Product with digital elements

The provisions of the Cyber Resilience Act apply to ‘products with digital elements’, meaning “any software or hardware product”.⁷² Open-source software is thus a ‘product with digital elements’ if: 1) the open-source project develops *software* or *hardware*; and 2) that software or hardware is a *product* under the Cyber Resilience Act.

The Cyber Resilience Act defines open-source software as “software the source code of which is openly shared and [...] made available under a free and open-source license.”⁷³ From this definition, however, it is not immediately clear that open-source software is also a software *product*.

The Cyber Resilience Act itself does not define what a ‘product’ is. The EU’s Blue Guide, the Commission’s interpretation guide for product rules, offers some additional guidance for definitions related to European product legislation.⁷⁴ The Guide defines a product in relation to its placing on the market: “Union harmonisation legislation applies to products which are intended to be placed (and/or put into service) on the market.”⁷⁵ This element of ‘placing onto the market’ is thus an important qualifier for open-source software as a software *product* under the Cyber Resilience Act.

3.1.4 Placing on the market

The Cyber Resilience Act defines that a product is placed on the market when it is “made available” on the Union market, meaning “the supply of a product [...] for distribution or use [in the Union] *in the course of a commercial activity*, whether in return for payment or free of charge.”⁷⁶ These definitions highlight that open-source software can thus be offered on the market – and therefore be a product under the Cyber Resilience Act – even if the software is offered for free.

Additionally, open-source software is “placed on the market” in the sense of the Cyber Resilience Act if the developer supplies the product “in the course of a commercial activity”. Although this is an additional requirement, its abstract character caused much discussion after the Commission’s proposal.⁷⁷

3.1.5 Commercial Activity

The provisions of the Cyber Resilience Act do not clearly define ‘supplying a product in the course of a commercial activity’. Recital 18 of the Cyber Resilience Act states that “only free and open-source software made available on the market, and therefore supplied for distribution or use in the course of a commercial activity should be covered by this Regulation.” Although the

⁷² Art 3(1) CRA.

⁷³ Art 3(48) CRA.

⁷⁴ Commission notice – The ‘Blue Guide’ on the implementation of EU product rules [2022] OJ C247/1.

⁷⁵ Blue Guide (n 75), 17.

⁷⁶ Art 3(22). Emphasis mine.

⁷⁷ Aertsen (n 13); Webmink In Draft, ‘Fixing The CRA For Open Source’ (*Webmink In Draft*, 20 February 2023) <<https://the.webm.ink/fixing-the-cra-for-open-source>> accessed 21 February 2023; Nicholson (n 13).

Recitals are not legal provisions, they offer an interpretation of what ‘supplying in the course of a commercial activity’ means in the context of open-source software.⁷⁸

The Recitals note several examples of open-source software supplied in the course of a commercial activity. Open-source software is supplied in the course of a commercial activity if the developer 1) charges a price for a product; 2) charges a price for technical support services that does not serve the recuperation of actual costs; 3) provides a software platform where the manufacturer monetises other services; or 4) if the software requires as a condition for use the processing of personal data, unless for certain legitimate purposes (e.g., security).⁷⁹ The legislators seemingly had particular open-source projects in mind when drafting these examples. For instance, the provision of a software platform where the manufacturer monetises other services can relate to Android: the core of Google’s mobile operating system is open source, but Google integrates the Google Play Store, Google Drive, and other similar services into Android when providing the platform to smart phones.⁸⁰

This list is not exhaustive, as the Recital notes that supply within the course of a commercial activity “might be characterised” by the options mentioned above.⁸¹ Other activities and conditions can also bring the open-source software project in the context of a commercial activity, placing additional emphasis on the question when an activity is ‘commercial’ under the Cyber Resilience Act.

Many hobby developers add donation options to their open-source software (e.g., Patreon, PayPal). Developers often make such donation requests to cover the project’s maintenance costs (e.g., website costs).⁸² At the same time, research shows that, in certain large-scale open source projects, code contributions by companies can be ten times larger than contributions by volunteers.⁸³ Such large-scale contributions might lead to the conclusion that the entire open-source project falls into a ‘commercial activity’, as commercial parties maintain nearly the entire project. A strict dichotomy between open-source software and commerciality does not exist.⁸⁴ There are diverse ways in which an open-source project can obtain financial and/or organisational support.⁸⁵

The Commission proposal lacked insight into these diverse methods of commerciality, as the text only gave examples of open-source software supplied in the course of a commercial activity.⁸⁶ The Council and Parliament, in response, significantly expanded the Recitals, especially regarding open-source software. As a result, the legislators exempted many types of open-source software from the scope of the Act. For example, the amended Recitals state

78 See Llio Humphreys and others, ‘Mapping Recitals to Normative Provisions in EU Legislation to Assist Legal Interpretation’, *JURIX* (2015) 42–44 and cases cited therein.

79 Recital 15 CRA.

80 Ron Amadeo, ‘Google’s Iron Grip on Android: Controlling Open Source by Any Means Necessary’ (*Ars Technica*, 21 July 2018) <<https://arstechnica.com/gadgets/2018/07/googles-iron-grip-on-android-controlling-open-source-by-any-means-necessary/>> accessed 19 January 2024.

81 Recital 15 CRA.

82 Cassandra Overney and others, ‘How to Not Get Rich: An Empirical Study of Donations in Open Source’, *Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering* (ACM 2020).

83 Yuxia Zhang and others, ‘Companies’ Participation in OSS Development—An Empirical Study of OpenStack’ (2021) 47 *IEEE Transactions on Software Engineering* 2242, 2249.

84 Wheeler (n 14).

85 *ibid.*

86 Aertsen (n 13).

that asking for donations does not constitute supply in the course of a commercial activities, as long as the developers do not seek to gain profits from those donations.⁸⁷ Furthermore, the Recitals state that an open-source project is not supplied in the course of a commercial activity merely due to development support from commercial entities.⁸⁸ In sum, the role of open-source software within the Cyber Resilience Act largely depends on whether the software is supplied in the course of a commercial activity.

4 Assessing the commerciality of a project

The commerciality of open-source software largely determines whether the software falls under the scope of the Cyber Resilience Act. Therefore, the exact meaning of ‘supplying in the course of a commercial activity’ merits further examination.

Most activities are commercial if developers use them to earn a profit, i.e. the income from these actions exceed maintenance costs. For example, the Cyber Resilience Act lists charging a price for the software or for technical support, when this exceeds maintenance costs, as indicative of supplying the software in the course of a commercial activity.⁸⁹

In contrast, certain projects are not supplied in the course of a commercial activity. Again, developers of such projects mostly do not earn income that exceeds their maintenance costs, such as receiving small donations.

Table 1 shows how the Recitals include and exempt numerous open-source software projects from the scope of the Cyber Resilience Act. Based on this overview, a few questions remain.

The list of commercial activities in the Recitals is non-exhaustive; the Recital states that a commercial activity “*might be characterised*” by the options mentioned.⁹¹ In the future, courts may thus amend the list and determine that other activities are also commercial.

An assessment of other activities, however, is difficult, as the Recitals further state that “the mere circumstances under which the product has been developed, or how the development has been financed, should [...] not be taken into account” when assessing the commercial nature of the software.⁹² This limitation seems to directly contradict the Recitals themselves. As shown in Table 1, the Recitals explicitly exempt certain types of development (e.g., development by commercial entities) and financial models (e.g., receiving donations) from the scope of ‘supplying a product in the course of a commercial activity’. A court can thus seemingly not assess the commerciality of a project as the Recitals currently do.

Additionally, the Recitals contain an unclear role for the *intention* of gaining a profit. In the context of donations, the Recitals state that accepting donations “exceeding the costs [of] design, development and provision of a product” means that the software is supplied in the course of a commercial activity.⁹³ In contrast, when developers accept donations “without the *intention* of making a profit”, they do not supply the product in the course of a commercial

87 Recital 15 CRA.

88 Recital 18 CRA.

89 Recital 15 CRA.

91 Recital 15 CRA. Emphasis mine.

92 Recital 18 CRA.

93 Recital 15 CRA.

Table 1: The scope of the Cyber Resilience Act for open-source software⁹⁰

Indicative of a supplying the software <i>in</i> the course of a commercial activity	• An intention to monetise beyond the recuperation of actual costs • Charging a price for the product • Charging a price for technical support • Personal data processing as a condition for use of the software (except for certain justified purposes) • Accepting donations exceeding the costs of developing and maintaining the software, without the intention to make a profit.
Indicative of a supplying the software <i>outside</i> the course of a commercial activity	• Monetisation only to recuperate costs of maintenance, instead of making a profit (e.g., by public-administration entities) • Supply of software intended to be integrated by other manufacturers, without monetisation of the original software • Products which receive financial or developmental support from manufacturers • The mere presence of regular releases • Development by non-profit organisations, if they use their earnings after cost for non-profit objectives • Contributions to open-source software when not involved in project leadership/ ownership • Mere distribution on repositories
Special regulatory regime	Open-source software stewards, legal persons who “provide support on a sustained basis” for the development of open-source software and play a “main role in ensuring the viability” of open-source software

activity.⁹⁴ It is unclear from the Recitals when intent is measured: at the start of the project or when the developers introduce certain financing methods. A developer may not intend to make a profit initially, but, as the project grows, may consider it reasonable. Likewise, the developer may not intend to make a profit, but may receive such large donations from enthusiastic users that they completely exceed all maintenance costs. Such situations, which are not clearly determined in the Recitals, remain complex.

The Commission may still resolve some of the Recital's complexities. Pursuant to Article 26 of the Act, the Commission may publish guidance to support the application of the Cyber Resilience Act. The scope of the Act for free and open-source software is of particular importance when they provide such guidance.⁹⁵

In sum, the Recitals, in general, indicate clearly when open-source software is commercial. If developers publish open-source software for which consumers pay a commercial price or other consideration (e.g., personal data), they supply the software in the course of a commercial activity. If, in contrast, developers merely maintain or support open-source software, they do not supply the software in the course of a commercial activity. Simultaneously, when moving beyond a general assessment, the Recitals do contain certain conflicting statements. These statements might hinder clear answers to future questions surrounding the position of open-source software under the Cyber Resilience Act.

5 Specific provisions for open-source software within the Cyber Resilience Act

The Cyber Resilience Act does not only regulate open-source software developers in order to improve the cybersecurity of open-source software. The Act also prescribes specific rules for 'open-source software stewards', proprietary software developers, and other parties with the aim of improving the overall cybersecurity of the open-source software ecosystem.

5.1 Open-source software stewards

In the open-source software community, there are certain organisations that support the development of open-source software as part of their overall mission statement. In some cases, these organisations also develop core open-source software. An example of such an organisation is the Python Software Foundation, which aims to advance the Python programming language and its community. The foundation organises conferences, offers grants to developers, and "produces the core Python distribution".⁹⁶ Python is a core programming language for software worldwide; it ranks second, after JavaScript, in a recent study from Github on the open-source software hosted on their platform.⁹⁷ The Python Software Foundation thus offers core support to the open source community, both through development and support.

⁹⁴ Recital 15 CRA.

⁹⁵ Art 26(2)(a) CRA.

⁹⁶ <<https://www.python.org/psf/mission/>>.

⁹⁷ Kyle Daigle and GitHub Staff, 'Octoverse: The State of Open Source and Rise of AI in 2023' (*The GitHub Blog*, 8 November 2023) <<https://github.blog/news-insights/research/the-state-of-open-source-and-ai/>> accessed 13 August 2024.

The Cyber Resilience Act addresses organisations such as the Python Software Foundation as ‘open-source software stewards’.⁹⁸ A steward is a legal person that provides systematic support for the development of open-source software, which is *intended for commercial activities*, as part of their overall objectives.⁹⁹ Importantly, the definition states that a steward is *not* a manufacturer.

Open-source software stewards receive a special position within the supervision scheme of the Cyber Resilience Act. Stewards are subject to a “light-touch and tailor-made regulatory regime”.¹⁰⁰ The idea behind this scheme seems to be that open-source software stewards are vital to the continuation of the open source ecosystem; the legislators believe they have a “main role in ensuring the viability of [open-source software]”.¹⁰¹

Open-source software stewards have several obligations.¹⁰² First, stewards must put in place cybersecurity policies for secure development of open-source software and vulnerability handling by the developers of that software.¹⁰³ The Python Foundation, for instance, has a vulnerability handling system where users can contact the ‘Python Security Response Team’ for support.¹⁰⁴ Stewards cannot be fined for non-compliance with these obligations,¹⁰⁵ but they can be required to take certain corrective actions.¹⁰⁶ This exemption also means that stewards cannot affix a CE-mark to their product.¹⁰⁷

Stewards must also co-operate with market surveillance authorities to mitigate vulnerabilities in open-source software packages.¹⁰⁸ Market surveillance authorities are responsible for taking corrective measures when developers do not comply with the rules of the Act. This co-operation seems to be the essence of the steward role: providing communication between the open source community and authorities in cases such as Log4j. In that line, it is logical that open-source software stewards provide support for software *with commercial intent*, meaning integration into proprietary products or services.¹⁰⁹ Through commercial integration, these software packages – and their vulnerabilities – have considerable influence on the global software ecosystem.

Finally, there are obligations for stewards that are also involved with development of open-source software.¹¹⁰ They must also comply with certain notification obligations for developers, particularly the notification of actively exploited vulnerabilities.¹¹¹ However, as open-source software stewards are *not* manufacturers per the definition in Article 3(14), they do not have equal obligations to traditional manufacturers. Article 24(3) only lists notification obligations.

98 Recital 19 CRA: ‘open-source software stewards include certain foundations[.]’

99 Art 3(14) CRA.

100 Recital 19 CRA.

101 Recital 19 CRA.

102 Art 24 CRA.

103 Art 24(1) CRA.

104 <<https://www.python.org/dev/security/>>.

105 Art 64(10)(b) CRA.

106 Art 52(3) CRA.

107 Recital 19 CRA.

108 Art 24(2) CRA.

109 Recital 19 CRA.

110 Art 24(3) CRA.

111 Art 24(3) & 14(1) CRA.

It is imaginable that a strict delineation between open-source software stewards and manufacturers is not feasible in practice. Stewards, such as the Python Foundation, also develop software. Are such stewards then manufacturers for that software independently – assuming the software is supplied in the course of a commercial activity – or are they stewards – and thus *not* manufacturers – for both providing support and developing products? As described above, in the former they must comply with the Act’s many obligations for manufacturers, while in the latter they only carry the notification obligations of Article 24(3).

As with the Recitals above, the Commission may provide some answers to the role of open-source software stewards when it publishes guidance on the application of the Cyber Resilience Act.¹¹² Moreover, regulators could eventually solve such conflicts through the ‘tailor-made’ regulatory regime for open-source software stewards.

5.2 Proprietary manufacturers using open-source software

The Cyber Resilience Act applies to manufacturers of software and hardware products. This scope means that proprietary manufacturers are also responsible for improving open-source software cybersecurity, through several ways.

First, the Cyber Resilience Act the broad applicability of the Act means that proprietary software – and proprietary software developers – must adhere to certain cybersecurity requirements. Since open-source software is virtually always part of proprietary software, the requirements for the proprietary software package inherently involve the underlying open-source software.

This connection between the cybersecurity of the proprietary package and the open-source software is made explicit in the Act. The Cyber Resilience Act requires manufacturers to exercise due diligence when integrating third-party components, including open-source components, into their own product.¹¹³ This obligation seems to stem from cases such as the Log4j vulnerability, in which a vulnerability in an open-source component puts the entire (proprietary) software package at risk.

When exercising this due diligence, manufacturers may discover certain vulnerabilities. If a manufacturer identifies a vulnerability within an open-source component of their own software, they must, under the Act, report it to the open-source developers.¹¹⁴ The manufacturers must also remediate the vulnerability according to the vulnerability handling requirements of the Act.¹¹⁵ If, as part of this remedy, the manufacturers modify the code or hardware to address the vulnerability, they must also share this code with the open-source developer.

Other parties may help identify and remediate vulnerabilities in open-source software through voluntary security attestation programmes.¹¹⁶ The Commission can set-up such a programme through delegated acts. These programmes strive to improve the overall cybersecurity of

¹¹² Art 26(2)(a) CRA.

¹¹³ Art 13(5) CRA.

¹¹⁴ Art 13(6) CRA.

¹¹⁵ Art 13(6) & Annex I Part 2 CRA.

¹¹⁶ Art 25 CRA mentions ‘developers or users’ of open-source software and ‘other third parties’. See also Recital 21.

open-source software which is exempted from the scope of the Cyber Resilience Act.¹¹⁷ The exact content of a security attestation programme, i.e. if the Commission provides financial or organisational support, is not clear from the provisions.

The due diligence obligation and the voluntary security attestation programmes help to expand the parties which support the cybersecurity of open-source software packages.

6 Cybersecurity and open-source software: a problem solved?

There is a fine balance between enhancing open-source software cybersecurity and regulating the open source ecosystem which may rely on ad-hoc and voluntary work. The Cyber Resilience Act shows how delicate this balance is, with its many exemptions and categorisations of open-source software, to ensure that only software supplied within the course of a commercial activity is regulated. The question is then whether these considerations achieve a balance between mitigating cybersecurity risks of open-source software and introducing feasible legal obligations for the sector.

A project like Log4j, for instance, does not fall under the scope of the Cyber Resilience Act. The project does not charge a price for the software nor conducts any activities explicitly listed as commercial in the Cyber Resilience Act. The project is merely supported by certain donators and commercial entities, which are both explicitly exempted as commercial activities.¹¹⁸ Most likely, Log4j itself would, therefore, not fall within the scope of the Cyber Resilience Act. The only cybersecurity obligations related to Log4j exist for entities who integrate Log4j into their own proprietary software.

On a general level, the Cyber Resilience Act is a step in the right direction for cybersecurity, regardless of the rules imposed on open-source software. Many cybersecurity requirements introduced by the Act were not present in existing legislation.¹¹⁹ The Act thus, at minimum, might improve the cybersecurity of proprietary software, even if it would not cover open-source software.

In the specific context of open-source software, the Act aims to balance between improving cybersecurity of open-source software while not discouraging open-source software development. Broadly speaking, the Act only covers ‘commercial’ open-source software. Many types of open-source software are non-commercial, as evident by the Recitals, which means that most open-source software is not regulated by the Cyber Resilience Act. The balance seems, thus, to fall in favour of alleviating regulatory pressure on open-source software developers, instead of (fully) improving open-source software cybersecurity. However, the cybersecurity side is also supported by the responsibilities imposed on integrators of open-source software and the voluntary security attestation programmes.

117 Recital 21 CRA speaks of open-source software ‘not subject to the essential requirements’ of the Act.

118 Based on the assumption that the donations do not exceed the project’s maintenance costs. For further information, see <<https://logging.apache.org/log4j/2.x/support.html>>.

119 Pier Giorgio Chiara, ‘The Cyber Resilience Act: The EU Commission’s Proposal for a Horizontal Regulation on Cybersecurity for Products with Digital Elements: An Introduction’ [2022] International Cybersecurity Law Review.

In sum, the Cyber Resilience Act aims to make open-source software more secure than it is currently, without imposing responsibilities on developers that may discourage further open-source software development. The legislation certainly emphasizes not discouraging the development, but responsibilities on both developers and users of open-source software will likely help improve its cybersecurity.

7 The future of open-source software under EU law

The Cyber Resilience Act is the first piece of legislation that aims to strike a balance between responsibilities for open-source software and supporting its ecosystem.¹²⁰ This means that the legislative choices made in the Act will have consequences for the future of open-source software under EU law. However, the Cyber Resilience Act includes many of its considerations for open-source software in the Recitals. This legislative choice has two consequences: 1) there is no clear embedded legal framework for open-source software in the Cyber Resilience Act, due to the applicability of the Recitals and 2) many of the considerations are specific to the current landscape of open-source software and therefore overly restrictive when considering future developments.

Recitals only have legal power insofar as the Court of Justice of the European Union and supervisory authorities use them to interpret the provisions of the Cyber Resilience Act. In 1998, the Court held that “the preamble to a Community act has no binding legal force and cannot be relied on as a ground for derogating from the actual provisions of the act in question.”¹²¹ Recitals, therefore, can be useful for interpretation of ambiguous legal provisions (e.g., supplying in the course of a commercial activity) but are not separate legal provisions on which the Court will rely.

In addition, the Recitals are very specific and pinpoint different commercial modes within the current landscape of open-source software. Future developments may fall outside the scope of the current Recitals. For instance, a developer could place advertisements in their software, based on user consent to see them. These advertisements allow the developer to continue working full-time on the project and similar projects. Would this choice constitute an “intention to monetise”,¹²² which places the project inside the course of a commercial activity? Or is this just a circumstance under which “the development has been financed”,¹²³ although the developer also uses the money to work on other projects? European consumer law tackles this problem for ‘information society services’ by stating that they are “provided for remuneration”.¹²⁴ ‘Remuneration’ is a broad concept which involves advertisement income, but also the request for personal data by the service, as in the Cyber Resilience Act.¹²⁵ In comparison, the Cyber Resilience Act’s notion of a commercial activity then seems

120 Colonna (n 55).

121 Case C-162/97 *Nilsson and others* ECLI:EU:C:1998:554, [1998] ECR I-7477, para 54.

122 Recital 15 CRA.

123 Recital 18 CRA.

124 Art 1(b) Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules of Information Society services.

125 Recital 18 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

overly restrictive, while a concept such as ‘for remuneration’ more easily adapts to future developments.

It seems that the Cyber Resilience Act’s approach of placing virtually all considerations for open-source software in the Recitals might make the Act particularly vulnerable to future developments. This focus on the existing landscape, combined with the difficult method for assessing commerciality as described in Section 4, may impair the applicability of the Cyber Resilience Act in the future. An embedded legal framework for open-source products in product legislation, which could also adapt to future developments, remains missing.¹²⁶

8 Conclusion

This paper analysed the position of open-source software in the Cyber Resilience Act. The paper answered the following question: To what extent does the Cyber Resilience Act impose responsibilities on open-source software developers that achieve a balance between stimulating open-source software development and, simultaneously, mitigating cybersecurity problems within open-source software?

Open-source software stems from a unique development culture aimed at distributing knowledge freely. Simultaneously, the software is crucial for the modern digital infrastructure. As with any software, there are certain cybersecurity risks inherent in open-source software. The European Union aims to mitigate some of those risks through the Cyber Resilience Act.

The Cyber Resilience Act aims to regulate cybersecurity risks without discouraging open-source software development. The Act achieves this balance by covering only open-source software ‘supplied in the course of a commercial activity’. The Act also introduces several other mechanisms to support the cybersecurity of open-source software. First, the Act prescribes a special regulatory regime to open-source software stewards, legal persons who support and advance the open-source software ecosystem. Second, proprietary manufacturers may only integrate open-source software components in a diligent manner. Therefore, they must also fix vulnerabilities discovered in open-source components and share such fixes with the developers of the component. Through voluntary security attestation programmes, the Act also supports other parties interested in advancing open-source software cybersecurity.

At the same time, the Recitals contain complex legal terminology. The Recitals mention many modes of financing and development of open-source software and if those modes are ‘supplying in the course of a commercial activity’. However, the Recitals also note that an assessment of a project based merely on financing or development modes is not sufficient. It is currently unclear how this situation should be resolved in practice when an open-source project is neither an explicitly included or excluded commercial activity.

The Cyber Resilience Act, however, does certainly advance cybersecurity of open-source software compared to the current regulatory landscape. Through rules for proprietary integration, proprietary software developers are also responsible for the cybersecurity of open-source software. Such rules mean that, even when a project is exempted from the CRA’s scope, it will receive cybersecurity support through the Act’s obligations on other parties.

¹²⁶ See also Colonna on the role of open-source software in the new Product Liability Directive and the AI Act, Colonna (n 55).

The future position of open-source software under EU law remains somewhat unclear after the Cyber Resilience Act, especially since so many of its considerations for open-source software occur in the Recitals. In sum, the Cyber Resilience Act achieves a balance between encouraging open-source software development and mitigating cybersecurity risks within open-source software, but some key challenges remain for the future.

References

- Aertsen M, 'Open-Source Software vs. the Proposed Cyber Resilience Act' (*The NLnet Labs Blog*, 14 November 2022) <https://blog.nlnetlabs.nl/open-source-software-vs-the-cyber-resilience-act/> accessed 20 December 2023
- Amadeo R, 'Google's Iron Grip on Android: Controlling Open Source by Any Means Necessary' (*Ars Technica*, 21 July 2018) <https://arstechnica.com/gadgets/2018/07/googles-iron-grip-on-android-controlling-open-source-by-any-means-necessary/> accessed 19 January 2024
- Anderson R, 'Open and Closed Systems Are Equivalent (That Is, in an Ideal World)' in Joseph Feller and others (eds), *Perspectives on free and open source software* (MIT Press 2005)
- Barcomb A and others, 'Managing Episodic Volunteers in Free/Libre/Open Source Software Communities' (2022) 48 IEEE Transactions on Software Engineering 260
- Birkinbine BJ, *Incorporating the Digital Commons: Corporate Involvement in Free and Open Source Software* (University of Westminster Press 2020)
- Bitzer J, Schrettl W and Schröder PJH, 'Intrinsic Motivation in Open Source Software Development' (2007) 35 Journal of Comparative Economics 160
- Chiara PG, 'The Cyber Resilience Act: The EU Commission's Proposal for a Horizontal Regulation on Cybersecurity for Products with Digital Elements: An Introduction' [2022] International Cybersecurity Law Review
- Clark J, 'Google Swaps out MySQL, Moves to MariaDB' *The Register* (12 September 2013) <https://www.theregister.com/2013/09/12/google_mariadb_mysql_migration/> accessed 14 August 2024
- Colonna L, 'The End of Open Source? Regulating Open Source under the Cyber Resilience Act and the New Product Liability Directive' (2025) 56 Computer Law & Security Review 106105
- Daigle K and GitHub Staff, 'Octoverse: The State of Open Source and Rise of AI in 2023' (*The GitHub Blog*, 8 November 2023) <<https://github.blog/news-insights/research/the-state-of-open-source-and-ai/>> accessed 13 August 2024
- Goodin D, 'As Log4Shell Wreaks Havoc, Payroll Service Reports Ransomware Attack' (*Ars Technica*, 13 December 2021) <<https://arstechnica.com/information-technology/2021/12/as-log4shell-wreaks-havoc-payroll-service-reports-ransomware-attack/>> accessed 19 January 2024
- Grau GI, 'An Appraisal of the Proposal for a Directive on Liability for Defective Products' (2023) 12 Journal of European Consumer and Market Law 198
- Hess C and Ostrom E (eds), *Understanding Knowledge as a Commons: From Theory to Practice* (MIT Press 2007)
- Hiesgen R and others, 'The Log4j Incident: A Comprehensive Measurement Study of a Critical Vulnerability' [2024] IEEE Transactions on Network and Service Management 1
- 'History of the OSI' (*Open Source Initiative*, 19 September 2006) <<https://opensource.org/history/>> accessed 19 January 2024

Hoepman J-H and Jacobs B, 'Increased Security through Open Source' (2007) 50 Communications of the ACM 79

Humphreys L and others, 'Mapping Recitals to Normative Provisions in EU Legislation to Assist Legal Interpretation', *JURIX* (2015)

Lyngaas S, 'US Warns Hundreds of Millions of Devices at Risk from Newly Revealed Software Vulnerability' (CNN, 13 December 2021) <<https://www.cnn.com/2021/12/13/politics/us-warning-software-vulnerability/index.html>> accessed 19 January 2024

Meneely A and Williams L, 'Secure Open Source Collaboration: An Empirical Study of Linus' Law', *Proceedings of the 16th ACM conference on Computer and communications security* (ACM 2009)

—, 'Strengthening the Empirical Analysis of the Relationship between Linus' Law and Software Security', *Proceedings of the 2010 ACM-IEEE International Symposium on Empirical Software Engineering and Measurement* (ACM 2010)

Muffatto M, *Open Source: A Multidisciplinary Approach* (Imperial College Press 2006)

Nicholson D, 'Python Software Foundation News: The EU's Proposed CRA Law May Have Unintended Consequences for the Python Ecosystem' (*Python Software Foundation News*, 11 April 2023) <<https://pyfound.blogspot.com/2023/04/the-eus-proposed-cra-law-may-have.html>> accessed 20 December 2023

Open Source Initiative, 'The Open Source Definition' (22 March 2007) <<https://opensource.org/osd>> accessed 19 January 2024

Overney C and others, 'How to Not Get Rich: An Empirical Study of Donations in Open Source', *Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering* (ACM 2020)

Payne C, 'On the Security of Open Source Software' (2002) 12 Information Systems Journal 61

Phipps S, 'What Is the Cyber Resilience Act and Why It's Dangerous for Open Source' (*Voices of Open Source*, 24 January 2023) <<https://blog.opensource.org/what-is-the-cyber-resilience-act-and-why-its-important-for-open-source/>> accessed 20 December 2023

Pinzger M, Nagappan N and Murphy B, 'Can Developer-Module Networks Predict Failures?', *Proceedings of the 16th ACM SIGSOFT International Symposium on Foundations of software engineering* (ACM 2008)

Press A, 'Recently Uncovered Software Flaw "Most Critical Vulnerability of the Last Decade"' *The Guardian* (11 December 2021) <<https://www.theguardian.com/technology/2021/dec/10/software-flaw-most-critical-vulnerability-log-4-shell>> accessed 19 January 2024

Purdy K, 'Red Hat's New Source Code Policy and the Intense Pushback, Explained' (*Ars Technica*, 30 June 2023) <<https://arstechnica.com/information-technology/2023/06/red-hats-new-source-code-policy-and-the-intense-pushback-explained/>> accessed 13 December 2023

Ransbotham S, 'An Empirical Analysis of Exploitation Attempts Based on Vulnerabilities in Open Source Software' [2010] Workshop on the Economics of Information Security 1

Raymond E, 'The Cathedral and the Bazaar' (1999) 12 Knowledge, Technology & Policy 23

Richard Stallman, 'Initial Announcement' (GNU, 27 September 1983) <<https://www.gnu.org/gnu/initial-announcement.html>> accessed 19 January 2024

Schryen G, 'Is Open Source Security a Myth?' (2011) 54 Communications of the ACM 130

Schulz C-H, 'Open Source Software and Security: Practices, Governance, History, and Perceptions' in Amanda Brock (ed), *Open Source Law, Policy and Practice* (2nd edn, Oxford University Press 2022)

Sharma C, 'Tragedy of the Digital Commons' (2023) 101 North Carolina Law Review 1129

Smith PM, 'Copyright, Contract, and Licensing in Open Source' in Amanda Brock (ed), *Open Source Law, Policy and Practice* (2nd edn, Oxford University Press 2022)

Walden I, 'Open Source as Philosophy, Methodology, and Commerce: Using Law with Attitude' in Amanda Brock (ed), *Open Source Law, Policy and Practice* (2nd edn, Oxford University Press 2022)

Webmink In Draft, 'Fixing The CRA For Open Source' (*Webmink In Draft*, 20 February 2023) <<https://the.webm.ink/fixing-the-cra-for-open-source>> accessed 21 February 2023

'What Is Free Software? - GNU Project - Free Software Foundation' <<https://www.gnu.org/philosophy/free-sw.html.en>> accessed 13 January 2025

Wheeler DA, 'F/LOSS Is Commercial Software' [2009] Open Source Business Resource <<http://timreview.ca/article/229>>

Zhang Y and others, 'Companies' Participation in OSS Development—An Empirical Study of OpenStack' (2021) 47 IEEE Transactions on Software Engineering 2242

5.

The Internet of Forgotten Things: European cybersecurity regulation and the cessation of Internet of Things manufacturers

This article was published in Computer Law & Security Review on 30 May 2025. The text was last revised on 25 March 2025, with some minor textual corrections for inclusion in this dissertation. There have been no significant developments since the publication of the article.

Mattis van 't Schip, 'The Internet of Forgotten Things: European Cybersecurity Regulation and the Cessation of Internet of Things Manufacturers' (2025) 57 Computer Law & Security Review 106152.

Abstract

Many modern consumer devices rely on network connections and cloud services to perform their core functions. This dependency is especially present in Internet of Things (IoT) devices, which combine hardware and software with network connections (e.g., a 'smart' doorbell with a camera). This paper argues that current European product legislation, which aims to protect consumers of, inter alia, IoT devices, has a blind spot for an increasing problem in the competitive IoT market: manufacturer cessation. Without the manufacturer's cloud servers, many IoT devices cannot perform core functions such as data analysis. If an IoT manufacturer ceases their operations, consumers of the manufacturer's devices are thus often left with an obsolete device and, as the paper shows, hardly any legal remedies. This paper therefore investigates three properties that could support legislators in finding a solution for IoT manufacturer cessation: i) pre-emptive measures, aimed at ii) manufacturer-independent iii) collective control. The paper finally shows how these three properties already align with current legislative processes surrounding 'interoperability' and open-source software development and analyses whether these processes can provide an adequate remedy for consumers.

1 Introduction

Internet of Things devices are omnipresent. Organisations and individuals use these devices, which combine traditional hardware (e.g., a watch) with connected functionalities (e.g., WiFi, Bluetooth) for data recording, exchange, and transmission. For instance, individuals may use their ‘smart’ watch to track and analyse data on their sleep or they may automatically turn on their connected lights when the sun sets.

Many IoT devices rely on their connected functionalities (i.e., the ‘Internet’ in IoT) to perform core functions.¹ Virtually all IoT devices depend on a connection with the manufacturer’s servers to perform data analysis (e.g., indicating sleep health based on data from a smart watch).² At the same time, this dependency allows manufacturers to gain user insights and make users dependent on their product ecosystem, as devices can only fully function when connected to the manufacturer’s servers.³

Next to cloud dependencies, the IoT industry is characterised by a competitive market and fast development cycle. Many manufacturers of IoT devices are small or medium-sized enterprises (SMEs).⁴ These manufacturers often put devices on the market without adequate consideration for security and privacy, as they compete for consumers in a busy market.⁵ IoT devices can be rather small (e.g., plant sensors) and manufacturers can produce them without large investments. These market characteristics have, in certain cases, caused IoT manufacturers to discontinue product development or to cease operations entirely.⁶

If IoT manufacturers discontinue their support, the consumer is often left with little recourse. Consumers of VanMoof, an electric bike manufacturer, recently found themselves in this situation. Due to looming insolvency, the cloud-based key required for unlocking consumers’ bike locks was no longer accessible, leaving the consumers with doubts whether they could still use their bike at all.⁷ Consumers had virtually no legal remedies to maintain access to

-
- 1 Lachlan Urquhart, Tom Lodge and Andy Crabtree, ‘Demonstrably Doing Accountability in the Internet of Things’ (2019) 27 *International Journal of Law and Information Technology* 1; Jiahong Chen and others, ‘Who Is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllorship and the Household Exemption’ (2020) 10 *International Data Privacy Law* 15.
 - 2 See extensively on the role of the ‘cloud’ for IoT devices, Milan Milenkovic, *Internet of Things: Concepts and System Design* (Springer International Publishing 2020) 109–152 <<http://link.springer.com/10.1007/978-3-030-41346-0>> accessed 7 August 2024.
 - 3 W Kuan Hon, Christopher Millard and Jatinder Singh, ‘Twenty Legal Considerations for Clouds of Things’ (2016) 2016 Queen Mary University of London, School of Law Legal Studies Research Paper.
 - 4 Christopher Boniface, Lachlan Urquhart and Melissa Terras, ‘Towards a Right to Repair for the Internet of Things: A Review of Legal and Policy Aspects’ (2024) 52 *Computer Law & Security Review* 105934, 4.
 - 5 Jiahong Chen and Lachlan Urquhart, ‘“They’re All about Pushing the Products and Shiny Things Rather than Fundamental Security”: Mapping Socio-Technical Challenges in Securing the Smart Home’ (2022) 31 *Information & Communications Technology Law* 99.
 - 6 Jessica Rich, ‘What Happens When the Sun Sets on a Smart Product?’ (*Federal Trade Commission*, 13 July 2016) <<https://www.ftc.gov/business-guidance/blog/2016/07/what-happens-when-sun-sets-smart-product>> accessed 31 January 2024.
 - 7 Ingrid Lunden, ‘VanMoof, the e-Bike Startup, Officially Declared Bankrupt in The Netherlands’ (*TechCrunch*, 18 July 2023) <<https://techcrunch.com/2023/07/18/vanmoof-goes-vanpoof-bankruptcy/>> accessed 13 November 2023.

the decryption key required to unlock their bikes.⁸ Without an internet connection to the manufacturer, an Internet of Things device often ends up becoming a regular ‘Thing’ or entirely obsolete, depending on the product.

The EU legislator aims to significantly reduce the number of unsupported software and hardware devices, mainly by introducing update and support obligations for manufacturers of those devices. These obligations aim to keep products functional and secure for certain periods, so that the manufacturer cannot disregard them, for instance to focus on new product lines. These efforts are also in line with sustainability concerns across European policy. Consumers will more easily discard unsupported devices; continued update support means that devices will last longer and consumers will not require a new device.⁹

Certain legal problems, however, remain. Most update and support obligations do not account for the situation in which manufacturers cease to exist entirely. European law does not yet address this legal gap. Therefore, the main research question of this paper is: How does recent EU legislation regulate IoT manufacturer cessation and which properties from comparative provisions in EU digital policy could support filling any legislative gaps? In this paper, ‘manufacturer cessation’ refers to manufacturers that cease to exist or cease their business operations entirely, for instance due to bankruptcy.

This paper continues as follows. Section 2 sets out the emerging problem of IoT manufacturer cessation and its risks for consumers. Section 3 focuses on current EU legislation that might address those risks. It argues that current update obligations fall short of providing a framework which fully supports continuous updates and support for IoT devices. The main pitfall of current update obligations is their reliance on the manufacturer.¹⁰ Section 4 thus looks beyond existing solutions towards promising concepts in other recent EU digital policy, primarily those that focus on three tenets: i) pre-emptive work which allows ii) manufacturer-independent continuation of an IoT device within a system of iii) collective control. The section highlights how policies promoting interoperability, data portability, and open-source software fit well within these three tenets. Section 5 then builds on these policies to show how interoperability, data portability and open-source software may mitigate IoT manufacturer cessation problems. Section 6 concludes.

2 Manufacturer cessation and its risks in the context of the Internet of Things

Manufacturer cessation can take many shapes, depending on why the manufacturer ceases their operations and what type of IoT products they produce. In the following, I set out a few examples of IoT manufacturer cessation and how they affected consumers. Next, I categorise

8 A competitor even created an app to help VanMoof customers retrieve their bicycle encryption key from the VanMoof servers shortly before bankruptcy, see Thomas Ricker, ‘Cowboy Releases Cheeky App to Keep VanMoof E-Bike Riders on the Road’ (*The Verge*, 13 July 2023) <<https://www.theverge.com/2023/7/13/23793591/cowboy-vanmoof-key-app-download-ios-android>> accessed 31 January 2024.

9 Boniface, Urquhart and Terras (n 4); Susan Lechelt and others, ‘Designing for the End of Life of IoT Objects’, *Companion Publication of the 2020 ACM Designing Interactive Systems Conference* (ACM 2020) <<https://dl.acm.org/doi/10.1145/3393914.3395918>> accessed 24 April 2024.

10 See also Conner Bradley and David Barrera, ‘Escaping Vendor Mortality: A New Paradigm for Extending IoT Device Longevity’, *New Security Paradigms Workshop* (ACM 2023).

the impact of manufacturer cessation on various IoT products and how this impact ranges from a device becoming completely defunct to the device remaining capable of performing its core functions.

2.1 The shapes of manufacturer cessation

There are many shapes to manufacturer cessation. First, there are numerous reasons why a manufacturer might cease operations, ranging from an unviable business model to a lack of interest in continuing the business. Second, manufacturers might act differently when deciding to cease operations. Some manufacturers can decide to go through a legal insolvency procedure, while others might instead opt to just cease their operations entirely and liquidate their assets.¹¹

Several recent cases illustrate these problems, next to the VanMoof example illustrated above.

In 2024, Gigaset, a firm that provided smart security cameras, announced that they went into insolvency proceedings. As a result, all devices connected to the Gigaset cloud would no longer be supported and functional, per the Gigaset announcement.¹² Gigaset found a buyer for parts of the company, but the buyer was not interested in proceeding with the smart home products that Gigaset provided. Customers could simply no longer use their IoT devices.

In 2022, consumers of products made by Insteon took matters in their own hands. The company behind Insteon, SmartLights, took their servers offline after financial difficulties, leaving Insteon customers, literally, in the dark as they could no longer access their devices through the app.¹³ A group of passionate Insteon users then decided to take over the Insteon business and immediately worked on getting devices back online.

Another example of manufacturer cessation that attracted much attention is the ‘Jibo’ robot, which announced its own ‘death’ when the manufacturer shut down its servers: ‘Maybe someday when robots are way more advanced than today, and everyone has them in their homes, you can tell yours that I said hello.’¹⁴ Many consumers became emotionally attached to Jibo over time;¹⁵ they even considered burying Jibo.¹⁶ Additionally, as with Insteon, many Jibo

11 Cesare Bartolini and others, ‘Cloud Providers Viability: How to Address It from an IT and Legal Perspective?’ in Jörn Altmann, Gheorghe Cosmin Silaghi and Omer F Rana (eds), *Economics of Grids, Clouds, Systems, and Services*, vol 9512 (Springer International Publishing 2016).

12 The announcement was not provided in English, for the Dutch and German versions see ‘Gigaset Smart Home/Care Staakt Zijn Diensten Vanaf 29 Maart 2024’ <https://www.gigaset.com/nl_nl/cms/smart-home-overzicht.html> accessed 11 April 2024; Gigaset, ‘Gigaset Smart Home/Care Wurde Eingestellt’ <https://www.gigaset.com/ch_de/cms/smart-home-uebersicht.html> accessed 16 April 2024.

13 Jennifer Pattison Tuohy, ‘Insteon Customers Turned Insteon’s Lights Back on’ (*The Verge*, 9 June 2022) <<https://www.theverge.com/2022/6/9/23161803/insteon-customers-bought-company-restored-service>> accessed 31 January 2024.

14 Ashley Carman, ‘They Welcomed a Robot into Their Family, Now They’re Mourning Its Death’ (*The Verge*, 19 June 2019) <<https://www.theverge.com/2019/6/19/18682780/jibo-death-server-update-social-robot-mourning>> accessed 24 April 2024.

15 Lechelt and others (n 9).

16 Carman (n 14).

owners attempted to take over Jibo's code base to keep it up and running. In the end, Jibo was also bought by a competitor and kept alive.¹⁷

These diverse examples of IoT manufacturer cessation highlight the dynamics of manufacturer cessation in the Internet of Things sector. All companies suffered from financial difficulties. Consumers were often left without concrete legal remedies; the manufacturer simply disappeared and could no longer be held to any product support obligations (e.g., update requests).¹⁸ The Internet of Things concerns numerous devices, as evident from these examples too: losing access to a smart security camera (Gigaset) or rather expensive device (VanMoof and Jibo) can be more impactful than losing access to a smart light (Insteon) that, for instance, the consumer can still turn on manually.

2.2 Shapes of product end-of-support

The examples above show that manufacturers across a range of product types have ceased to exist in recent years. Manufacturer cessation does not impact all products equally. Below, I set out how the impact of manufacturer cessation differs between certain products, ranging from products becoming entirely defunct to products remaining capable of performing their core functions. The enormous scope of IoT products on the market means that this delineation is not exact; this Section mainly aims to illustrate precisely this heterogeneity of the IoT sector and its meaning in the context of IoT manufacturer cessation.

2.2.1 Product becomes entirely defective

Some products rely fully on connecting to the manufacturer's servers for their core functions. These products become entirely defective after the manufacturer ceases operations. There are multiple components within an IoT product that can render the device defective.

The device can lose access to critical hardware components. This is the case, for instance, when the device requires decryption of data and can only access the decryption key from the manufacturer's servers. As indicated above, customers of the VanMoof bike could not retrieve their decryption key after VanMoof went into bankruptcy proceedings, thus leaving the consumers unable to unlock their bicycle locks. With the bicycle permanently locked, the bike became unusable for consumers.

More often, software becomes defective after manufacturer cessation, leading to device failure. Imagine, for instance, that a consumer has a security camera that they can access when they are not home. The application for operating IoT devices is often developed and hosted by the device's manufacturer; data flows between the application and the manufacturer's servers.¹⁹ Without the manufacturer's servers, many of the application's functions, including,

17 Ashley Carman, 'Jibo, the Social Robot That Was Supposed to Die, Is Getting a Second Life' (*The Verge*, 23 July 2020) <<https://www.theverge.com/2020/7/23/21325644/jibo-social-robot-ntt-disruptionfunding>> accessed 4 September 2024.

18 See further in Section 3.

19 TJ OConnor, Dylan Jessee and Daniel Campos, 'Through the Spyglass: Towards IoT Companion App Man-in-the-Middle Attacks', *Cyber Security Experimentation and Test Workshop* (ACM 2021).

for instance, a log-in feature for authentication purposes, no longer work.²⁰ Consumers then lose access to and control over their devices due to software failure.

2.2.2 Products remain functional for a while

In the context of IoT manufacturer cessation, products exist in an array from defunct to functional. Smart TVs, for instance, lose some, but not all of their key functionalities.

Modern smart TVs function quite similarly to smartphones as they rely on applications developed by third-parties, such as video streaming apps. The TV can still turn on after manufacturer cessation and consumers can in principle use the TV for any content they desire. For example, they can watch analogue television or a streaming service.

However, in certain cases, they can no longer use the applications installed on the TV, because using, installing and updating these applications requires a connection with both the TV manufacturer's application store and the application developer's servers. These apps differ from the authentication app mentioned for fully defective products, since those authentication apps rely on the manufacturer. Third-party apps only partially rely on the manufacturer to remain functional. Netflix may, for example, update their interface, which requires interaction with the TV's operating system. Consequently, if the TV's operating system is no longer updated by the manufacturer, the Netflix application can no longer function on that TV. In this context, researchers recently found that less than 10% of mobile apps could be downloaded straight from the app store on end-of-support devices (and even fewer actually functioned).²¹

In a similar vein, manufacturers will no longer patch vulnerabilities after they cease their activities. The smart TV therefore becomes vulnerable to cyberattacks, as, over time, numerous vulnerabilities will be discovered in the device's software that attackers could exploit. In these cases, manufacturer cessation thus leads to both cybersecurity risks and a loss of functionalities.

Smart TVs and smart phones are examples of devices that thus remain partially functional, as they, respectively, allow the consumer to watch certain 'analogue' content and call others. In certain cases, applications downloaded from the application store may remain functional even after manufacturer cessation. However, the manufacturer's cessation does (eventually) cause cybersecurity risks and a loss of functionalities.

2.2.3 Products remain capable of performing core functions

There are also certain IoT products that still remain functional after manufacturer cessation.

This is primarily the case when the device can remain functional as a regular 'Thing', for instance in the case of smart lights. Consumers may lose access to the application through which they remotely operate the lights, but they can still turn them on with a regular wall switch. The wall switch can thus continue to perform the core functions of the lights – offering light – regardless of the manufacturer's cessation.

20 TJ OConnor, William Enck and Bradley Reaves, 'Blinded and Confused: Uncovering Systemic Flaws in Device Telemetry for Smart-Home Internet of Things', *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks* (ACM 2019).

21 Craig Goodwin and others, 'Quantifying Device Usefulness - How Useful Is an Obsolete Device?' in José AbdeInour Nocera and others (eds), *Human-Computer Interaction – INTERACT 2023*, vol 14145 (Springer Nature Switzerland 2023) 92.

At the same time, devices such as the smart light also return to a state where they do not differ from traditional, ‘dumb’ counterparts. In such cases, many consumers may still experience a loss of their device, as they bought it precisely because they did not want to manually toggle the lights any more.²²

Devices may also remain fully functional due to their network architecture. Devices may rely on Wi-Fi-based connections, but could contain local-only alternatives, so that a connection to the manufacturer is not required in the first place. Additionally, devices that do not require a network connection – and thus a connection to the manufacturer – by design will remain functional after manufacturer cessation.²³ Such devices often employ a communication protocol other than Wi-Fi, such as Bluetooth, Zigbee, or Z-Wave, which only enables exchange with other devices in their proximity. A Bluetooth audio speaker is a common example of such a proximity connection. The manufacturer is not within that proximity and thus has no influence over the connection between the consumer’s devices. Such a network architecture also reduces security risks, as attackers can also only access the devices when in their physical proximity.

3 Update obligations and manufacturer cessation: exemplification of a legal problem

Keeping products functional as long as possible is a key factor in recent European policy. This effort stems from cybersecurity policies, but also sustainability perspectives, where keeping a device functioning means that no new devices – and therefore natural resources – are necessary.²⁴ This article focuses on the former. Update obligations form the driving force behind recent EU efforts to extend product lifecycles. If manufacturers disregard their product and no longer provide updates, the product are more likely to become vulnerable to cyberattacks. Hence, the Commission considered ‘security support (updates and handling of vulnerabilities)’ as one of the three main pillars of the Cyber Resilience Act.²⁵ Given this direct connection between product lifecycle extension and update obligations, it seems logical that update obligations provide a response to issues presented by IoT manufacturer cessation. However, a further look at update obligations show the contrary; they exemplify how problems manifested by manufacturer cessation currently escape regulatory scrutiny.

22 In a recent study, researchers found that ‘feeling technologically advanced’ and having a ‘modern home’ were the most beneficial reasons for adopting smart home devices, see Daniel B Shank and others, ‘Knowledge, Perceived Benefits, Adoption, and Use of Smart Home Products’ (2021) 37 *International Journal of Human–Computer Interaction* 922, 927.

23 For examples on how these devices remain functional without network connectivity, see Poonam Yadav and others, ‘Network Service Dependencies in Commodity Internet-of-Things Devices’, *Proceedings of the International Conference on Internet of Things Design and Implementation* (ACM 2019) 208 <<https://dl.acm.org/doi/10.1145/3302505.3310082>> accessed 4 June 2024.

24 See for instance the recently enacted Right to Repair Directive: Directive (EU) 2024/1799 of the European Parliament and of the Council of 13 June 2024 on common rules promoting the repair of goods and amending Regulation (EU) 2017/2394 and Directives (EU) 2019/771 and (EU) 2020/1828 [2024] OJ L2024/1799.

25 European Commission, ‘Staff Working Document Impact Assessment Report Accompanying the Document Proposal for a Regulation on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020’ SWD (2022) 282 final 12.

3.1 The Cyber Resilience Act

At the end of 2024, the European legislators adopted the Cyber Resilience Act.²⁶ The Act brings the largest set of cybersecurity responsibilities for manufacturers of software and hardware products—including IoT devices—seen thus far in EU legislation.²⁷

The scope of the Cyber Resilience Act extends to software and hardware products and their ‘remote data processing’ capabilities (e.g., a cloud data processing service).²⁸ The Cyber Resilience Act thus applies to both the IoT device as a hardware/software product and to any cloud services on which the product relies.

The Cyber Resilience Act also points to different categories of IoT devices. Next to regular ‘products with digital elements’, the legislators identified products with additional risks for consumers. Annex III lists ‘important’ products, including smart virtual assistants (e.g., Amazon Alexa), smart home products with security functionalities (e.g., Gigaset’s cameras), internet connected toys with social or location tracking features (e.g., dolls with voice recognition) and personal wearable products for health monitoring (e.g., smart watches). Additionally, Annex IV lists a few ‘critical’ products, such as smart meter gateways within smart metering systems, that carry ‘significant risks of adverse effects’ as they have security functions.²⁹

The Cyber Resilience Act defines a certain ‘support period’ during which manufacturers must ensure that they handle vulnerabilities in their devices effectively, in line with the vulnerability handling requirements in the Annex.³⁰ The requirements in the Annex include, for example, addressing and remediating vulnerabilities without delay.³¹ Pursuant to Article 13(8), the exact period during which manufacturers must offer this support depends on the product, but is usually at least five years.

There are several problems with relying on the Cyber Resilience Act’s update requirements in cases of IoT manufacturer cessation. It is unclear how far this obligation extends if the manufacturer ceases to operate, especially if the manufacturer stops during the support period of the product. It is unlikely that a consumer can rely on market authorities to compel discontinued manufacturers to comply with support obligations. National law may provide some solutions. For example, provisions may exist that make the organisation’s directors liable if they take on obligations which they know they cannot comply with because of looming

26 Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) [2024] OJ L2024/2487.

27 Pier Giorgio Chiara, ‘The Cyber Resilience Act: The EU Commission’s Proposal for a Horizontal Regulation on Cybersecurity for Products with Digital Elements: An Introduction’ [2022] *International Cybersecurity Law Review*.

28 Art 2(1), 3(1), 3(2) & Recital 11-12 CRA.

29 Recital 46 CRA.

30 Art 3(20) & 10(6) CRA.

31 Annex I Part 1(3)(f) CRA.

bankruptcy.³² These provisions differ between Member States and are not harmonised,³³ so they do not (yet) provide a full solution for manufacturer cessation.

This lack of remediation points to the assumption of manufacturer longevity on which the support obligations rely. Without the manufacturer, most legal obligations become unviable. Update obligations can therefore only help in remediating problems caused by manufacturer cessation if such obligations operate independently from the manufacturer (see Section 5).

For instance, the Cyber Resilience Act states that, after the ‘support period’, i.e. the period determined by the manufacturer during which they publish updates for a device, the manufacturer should strive to share the source code of their product.³⁴ This option, which only occurs in the Recital and is not directly linked to obligations in the legal text, may allow manufacturer-independent product development, which I discuss further below (Section 5.2).

The update obligations in the CRA leave a second gap, due to their focus on patching security vulnerabilities. The CRA defines vulnerabilities as ‘weakness, susceptibility or flaw of a product [...] that can be exploited by a cyber threat.’³⁵ A cyber threat is an ‘event or action that could damage, disrupt, or otherwise adversely impact’ a product with digital elements.³⁶ For certain IoT products, this update obligation misses the mark in the context of manufacturer cessation: if users can still turn on their smart lights manually, they lose certain device functionalities, i.e. control through other network-connected devices, but the devices are not necessarily impacted by security vulnerabilities. The scope of the CRA update obligations therefore fall short in two areas: the type of updates covered and the reliance on manufacturer longevity.

3.2 Sale of Goods Directive

The Sale of Goods Directive (SGD) is in force since 2019.³⁷ The SGD ensures consumer protection concerning sale contracts between ‘sellers’ and ‘consumers’. Sellers are natural or legal persons who act on behalf of their business or trade, while consumers are natural persons who are not acting for purposes of their business or trade.³⁸ The SGD concerns contracts for the sale of ‘goods’, which also include Internet of Things devices, as ‘goods with digital elements’.³⁹

The SGD contains two categories of conformity requirements: subjective and objective. The seller must comply with both the subjective and objective requirements. Article 6 lists several subjective requirements, such as i) the possession of certain functionalities and compatibilities, as required by the sales contract, ii) conformity to the consumer’s purposes and iii) the supply of updates as stipulated by the contract. Subjective requirements thus depend on the sales contract between the seller and consumer.

32 See for instance the ‘Beklamel’ case law in the Netherlands, HR 6 oktober 1989 ECLI:NL:HR:1989:AB9521.

33 Carsten Gerner-Beuerle and Edmund-Philipp Schuster, ‘The Evolving Structure of Directors’ Duties in Europe’ (2014) 15 European Business Organization Law Review 191.

34 Recital 62 CRA.

35 Art 3(40) CRA.

36 Art 3(46) CRA & Art 2(8) Regulation 2019/881 (Cybersecurity Act).

37 Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC [2019] OJ L136/28.

38 Art 2(2) and 2(3) SGD.

39 Art 2(5)(b) SGD.

Article 7 lists objective requirements, which apply irrespective of what is stipulated in the sales contract. Update requirements are part of these objective requirements.⁴⁰ In contrast with subjective update requirements, the objective update requirements ensure that goods with digital elements remain in conformity. Conformity means that the goods comply with the subjective and objective requirements and certain installation requirements,⁴¹ for a period of time.⁴² This period is determined, *inter alia*, by the reasonable expectations of the consumer.⁴³

A key difference with the Cyber Resilience Act is that the SGD's update requirements refer to the conformity of the product with the sales contract.⁴⁴ The updates must thus ensure that the device keeps providing, *inter alia*, the functionality, compatibility, and interoperability as agreed in the sales contract.⁴⁵ The Directive also explicitly mentions security updates.⁴⁶ The CRA, in contrast, aims exclusively at mitigating security vulnerabilities. For manufacturer cessation, the SGD addresses another side of the manufacturer cessation problem: the degrading functionalities of the IoT device after the manufacturer ceases operations. Here, the SGD thus complements the CRA regarding the type of updates.

The SGD requires the seller to provide updates, instead of the manufacturer in the Cyber Resilience Act. If the seller is not the manufacturer, it lacks the necessary expertise to provide updates. The seller then depends on co-operation with the manufacturer.⁴⁷ Consequently, the update requirement in the SGD relies on the same assumption of manufacturer longevity as the Cyber Resilience Act. When the manufacturer ceases to exist, holding the *seller* responsible for updates is no longer a viable option. The consumer can hold the seller liable for the lack of updates or claim other remedies,⁴⁸ but that does not change the fact that the device is no longer supported. The consumer is thus left without updates regardless of the responsible party. The update requirements in the SGD and CRA thus highlight that the position of the consumer is not improved by update requirements which rely on manufacturer longevity in the case of IoT manufacturer cessation.

4 Moving away from manufacturer longevity based on existing digital policy

Update obligations assume that the manufacturer remains capable of supporting their products. In the case of manufacturer cessation, the manufacturer loses that capability. If the manufacturer cannot act after cessation (*ex post*), pre-emptive measures (*ex ante*) may

40 Art 7(3) SGD.

41 Art 5 SGD.

42 Art 7(3) SGD.

43 Art 7(3)(a) and (b) SGD. On consumer expectations, see Simon Geiregat, 'What Digital Content Consumers (Should) Want' in Anna K Bernzen, Karina Grisse and Katharina Kaesling (eds), *Immaterialgüter und Medien im Binnenmarkt* (Nomos Verlagsgesellschaft mbH & Co KG 2022).

44 Art 5 SGD.

45 Art 6(a) SGD.

46 Art 7(3) SGD.

47 See Piia Kalamees, 'Goods With Digital Elements And The Seller's Updating Obligation' (2021) 2 JIPITEC 131, 134; Hans Schulte-Nölke, 'Digital Obligations of Sellers of Smart Devices under the Sale of Goods Directive 771/2019' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Smart Products* (Nomos 2022).

48 Art 10 & 13 SGD.

offer a viable alternative.⁴⁹ At the same time, those pre-emptive measures only work if the manufacturer, after cessation, no longer carries responsibility for the device. Therefore, a solution to manufacturer cessation also requires *manufacturer-independence*.⁵⁰ This solution would be stronger within a system of *collective control*, as continuing to rely on a single responsible party retains the risks of manufacturer dependencies, i.e. cessation of the responsible party. This final requirement, however, is not as vital as the former two. To the best of my knowledge, there is a gap in research on the topic of IoT manufacturer cessation.⁵¹ These properties, thus, are based on a reflection on the problem of manufacturer longevity, as derived from several approaches in recent EU digital policy (Figure 1).⁵²

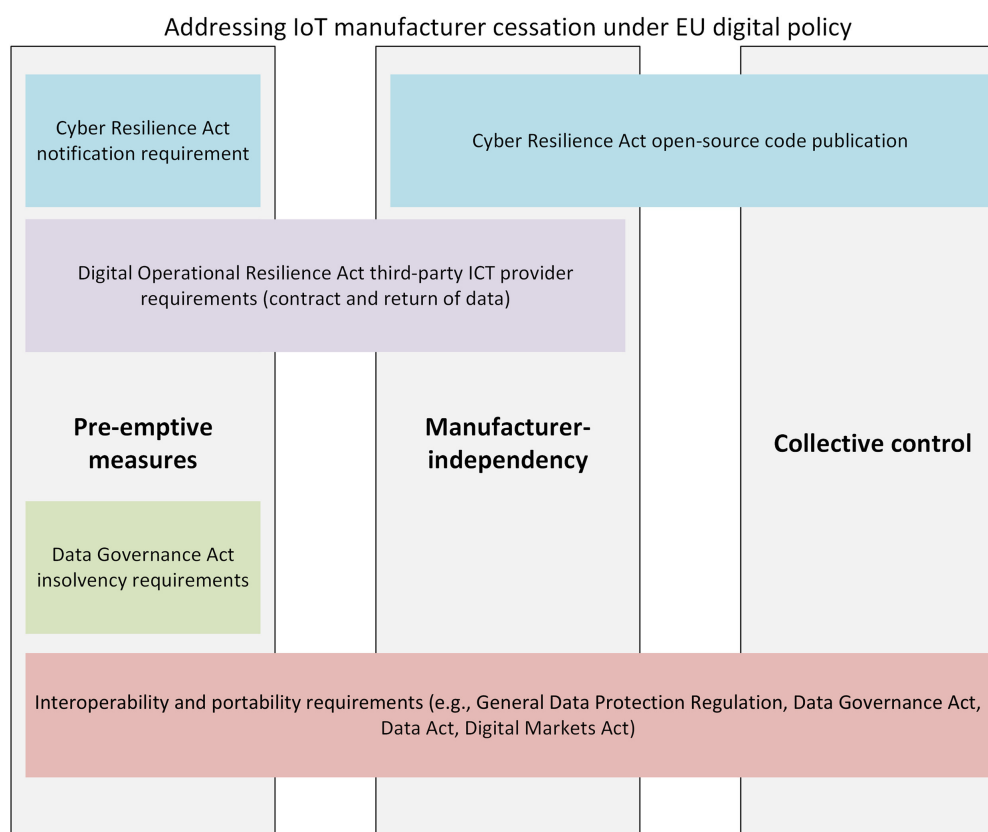


Figure 1: Addressing IoT manufacturer cessation under current EU digital policies

⁴⁹ See Bartolini and others (n 11) 289 stating: ‘if the problem is not addressed beforehand, the customer might incur serious trouble, because ex post remedies can be quite ineffective.’

⁵⁰ *ibid.*

⁵¹ Some studies exist, but they mainly address bankruptcy law, for instance in Tibor Tajti(Thaythy), ‘Unprotected Consumers in the Digital Age: The Consumer-Creditors of Bankrupt, Abandoned, Defunct and of Zombie Companies’ (2019) 24 Tilburg Law Review 3; Rebecca Parry and Roger Bisson, ‘Legal Approaches to Management of the Risk of Cloud Computing Insolvencies’ (2020) 20 Journal of Corporate Law Studies 421.

⁵² As an exception to this gap, see Bartolini and others (n 11) who also state ‘to the best of our knowledge, there does not appear to be a lot of literature addressing the issue of CSP viability’ (page 285).

4.1 Cyber Resilience Act

The Cyber Resilience Act requires manufacturers to inform relevant market surveillance authorities and, by any means available and to the extent possible, the consumers of their devices when they cease their operations.⁵³ This requirement only applies when the manufacturer, because it ceases to exist, can no longer comply with the Cyber Resilience Act. Importers and distributors of the manufacturer's devices have the same obligation when they receive information that the manufacturer ceases or has ceased to exist.⁵⁴ The Cyber Resilience Act thus contains a *pre-emptive measure* in the form of a notification mechanism. This notification mechanism, however, can only serve to reduce the risks of manufacturer cessation for consumers, as highlighted in Section 2.2, since the notification allows consumers to prepare and take measures (e.g., stop using their device).

The Recital of the Cyber Resilience Act suggests that manufacturers publish the source code of their product publicly after the end of the support period, or transfer it to another company for vulnerability handling.⁵⁵ Over the past decades of digital product development, some consumers with software development experience have advocated for publication of code, as the code enables them to continue product development even if the manufacturer decides to end their support.⁵⁶ Continued development of software regularly occurs, for instance, in the gaming industry; a game's fans keep the game running through regular open-source updates after the original developer moves on.⁵⁷ As such, open source code publication could serve a *manufacturer-independent* solution within a development framework of *collective control* as many open-source developers together build new software for the device. There is also some potential in transferring the source code to another company, as the Recital suggests, which I discuss further in Section 5.3. The Cyber Resilience Act thus also indicates options for device continuity after manufacturer cessation.

4.2 Digital Operational Resilience Act

The Digital Operational Resilience Act (DORA), the EU cybersecurity law for the financial sector, includes pre-emptive obligations for insolvency.⁵⁸ The DORA introduces a cybersecurity risk management framework for 'network and information systems' which financial entities

53 Art 13(23) CRA.

54 Art 19(8) CRA.

55 Recital 62 CRA.

56 See, for instance, the Stop Killing Games campaign: Federico Guerrini, 'Consumer Protection In Gaming: European Initiative Targets Video Game Publishers' (*Forbes*) <<https://www.forbes.com/sites/federicoguerrini/2024/08/30/consumer-protection-in-gaming-european-initiative-targets-video-game-publishers/>> accessed 27 February 2025.

57 Alice Jovanée, 'Four Classic Command & Conquer Titles Are Now Open Source' (*Polygon*, 27 February 2025) <<https://www.polygon.com/news/531365/command-and-conquer-open-source-code-ea>> accessed 3 March 2025; Kevin Purdy, 'Valve Releases Full Team Fortress 2 Game Code to Encourage New, Free Versions' (*Ars Technica*, 19 February 2025) <<https://arstechnica.com/gaming/2025/02/valve-releases-full-team-fortress-2-game-code-to-encourage-new-free-versions/>> accessed 3 March 2025.

58 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 [2022] OJ L333/1.

use.⁵⁹ Network and information systems involve a broad set of ICT products, including IoT devices.⁶⁰

Article 30 notes several contractual provisions that are mandatory when the financial entity (e.g., a bank) employs the services of a third-party ICT provider (e.g., a manufacturer of smart lightning used in a bank's office). The financial entity must include provisions which ensure that personal data processed by the third-party ICT provider is returned 'in the event of the insolvency, resolution or discontinuation of the business operations' of the provider.⁶¹ The financial entity and the third-party ICT provider must thus together consider the possible insolvency of the ICT provider when signing the contract.

As in the Cyber Resilience Act, the DORA thus requires certain *pre-emptive* considerations for insolvency of a party that provides ICT services. The CRA only imposes responsibilities on the manufacturer when they cease operations. The DORA insolvency rules are slightly stronger – given its focus on the banking industry – as parties must also consider insolvency upon signing the agreement, when insolvency is not a looming problem yet.

The return of data is a measure that could hold value for manufacturer cessation too. For example, the manufacturer could, at the very least, ensure that (personal) data processed by a device is sent back to the consumer when they cease their operations. This data holds value for device continuity, or at least the continuity of the service (e.g., transaction data over several years).

The Digital Operational Resilience Act introduces these obligations in the context of the financial sector, which holds other risks than the general IoT sector. However, the DORA illustrates that thinking *ex ante* about insolvency is part of European digital policy and data return also allows for a *manufacturer-independent* solution based on data.

4.3 Data Governance Act

The Data Governance Act (DGA) was enacted in 2022 and introduced rules for public, neutral, or altruistic data sharing, including for data produced by IoT devices.⁶² Most importantly, for manufacturer cessation, the DGA holds obligations for 'data intermediation services' when they become insolvent.

Data intermediation services are services which 'establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other'.⁶³ General IoT use does not constitute a data intermediation service – a data intermediation service covers IoT only when IoT data is generated specifically for neutral data intermediation purposes.⁶⁴

The DGA notes that data intermediation services must ensure continuity of their services in case of their insolvency.⁶⁵ There is no clarity in the DGA about how the services must ensure this continuity, leaving options open to the service itself. It is imaginable that services might

59 Art 1 DORA.

60 Art 3(2) DORA.

61 Art 30(2)(d) DORA.

62 Art 1(1) Data Governance Act.

63 Art 2(11) Data Governance Act.

64 Art 2(11)(d) Data Governance Act.

65 Art 12(h) Data Governance Act.

open a portal through which users can access their data for a limited period, or that they aim to co-operate with other, similar services that could continue to support their infrastructure. These actions also depend on the national insolvency procedures, because, in certain Member States, the service owner cedes authority to a liquidator or insolvency administrator once they enter into insolvency proceedings.⁶⁶ The DGA thus brings a pre-emptive measures that aims at continuation, where the CRA and the DORA consider insolvency the end of the service. The DGA therefore offers the most compelling type of *pre-emptive measure* in the context of manufacturer cessation: a measure that appreciates the lifespan of manufacturers.

4.4 Interoperability policies

In several pieces of legislation, the EU legislators emphasise the need for more interoperability in the current data economy. Interoperability, generally, refers to the capacity of systems to co-operate. Indeed, when systems can co-operate, it is easier to create a manufacturer-independent solution after their cessation. The consumer could, for instance, connect the device to another system for data exchange (e.g., a messaging service). This type of integration also creates a framework of collective control in which multiple devices, systems, and infrastructures co-operate. Interoperability in such terms is often termed as ‘federation’: people can choose their own digital service provider, without having to follow their peers or feel pressured by the network effects of dominant platforms.⁶⁷ I discuss this design more extensively below in Section 5.1.

The importance of interoperability in European digital policy is confirmed in a myriad of EU policies.⁶⁸ For instance, the EU recently adopted the aptly named Interoperable Europe Act, which aims to offer seamless exchange between trans-European public authorities (e.g., for driver’s licenses).⁶⁹ Next to interoperability, some policies refer to data ‘portability’. Where interoperability requires direct co-operation between diverse systems, data portability refers, instead, to a more direct relation between two systems, for instance in the form of data transfers. Below, I address both interoperability and portability obligations, as these policies aim to reduce (consumer) dependencies on manufacturer ecosystems.

Given the breadth of these policies, I address here the pieces most relevant for the (domestic) IoT context and the position of the consumer in case of manufacturer cessation.

66 As also identified in Lukas Von Ditzfurth and Gregor Lienemann, ‘The Data Governance Act: – Promoting or Restricting Data Intermediaries?’ (2022) 23 Competition and Regulation in Network Industries 270, 290.

67 Ian Brown, ‘Interoperability as a Tool for Competition Regulation’ (LawArXiv 2020) preprint 8 <<https://osf.io/fbvxd>> accessed 6 February 2024.

68 For instance the ‘Interoperability Regulations’ in the field of digital migration policy: Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa (Border Interoperability Regulation) [2019] OJ L135/27 or interoperability policies in the health sector: Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 [2025] OJ L 2025/327.

69 Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act) [2024] OJ L2024/903.

4.4.1 General Data Protection Regulation

The General Data Protection Regulation is the key EU policy for data protection. The GDPR prescribes specific rights to individuals whose data is ‘processed’, i.e. the consumer of IoT products. One of those rights is the right to data portability.⁷⁰

The GDPR introduces the right to data portability to strengthen the position of the data subject vis-à-vis the data controller.⁷¹ The right to data portability means that data subjects can receive the data concerning them from the entity holding that data, the ‘controller’ under the GDPR, in a ‘commonly used and machine-readable format’.⁷² This provision should, according to the Recital accompanying it,⁷³ encourage data controllers to adopt interoperable data formats.⁷⁴

Data portability holds potential for strengthening the position of the IoT consumer.⁷⁵ With data portability, the consumer can more easily switch between services, as they can transfer their data from one manufacturer to another, or from one ecosystem to another. This easier exchange also manifests *manufacturer-independency*. Importantly, however, the right to data portability under the GDPR only concerns the transfer of personal data that were ‘provided by’ the data subject.⁷⁶ Algorithmically inferred statistics, for instance, are not part of the right to data portability.⁷⁷ Furthermore, as mentioned before, data portability only covers directly transferring data to another provider, where interoperability requires more intensive co-operation between diverse systems.

4.4.2 Data Act

The Data Act addresses several elements of data availability and requires the interoperability of data between different entities.⁷⁸ The DA’s rules focus on the interoperability of ‘data processing services’, especially if they cover the same service type (e.g., Software as a Service).⁷⁹

The DA defines data processing services as services which enable ‘ubiquitous and on-demand network access to a shared pool of [...] computing resources’ (e.g., cloud services).⁸⁰ This definition, as the DA admits, ‘covers a substantial number of services with a broad range of different purposes’.⁸¹ In the context of the IoT, a data processing service, for instance, is the cloud service on which the IoT device stores data.

70 Art 20 GDPR.

71 Recital 68 GDPR.

72 Art 20(1) GDPR.

73 Recital 68 GDPR.

74 See more extensively, Paul De Hert and others, ‘The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services’ (2018) 34 Computer Law & Security Review 193.

75 Lachlan Urquhart, Neelima Sailaja and Derek McAuley, ‘Realising the Right to Data Portability for the Domestic Internet of Things’ (2018) 22 Personal and Ubiquitous Computing 317.

76 See on the ‘provided by’ condition the guidelines from the Article 29 Working Party: Article 29 Data Protection Working Party, ‘Guidelines on data portability’ 9-11.

77 Urquhart, Sailaja and McAuley (n 75) 326.

78 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

79 Art 35 DA. On service types, see Art 2(9) & Recital 81 DA.

80 Art 2(8) DA.

81 Recital 81 DA.

The DA introduces interoperability as a *manufacturer-independent* tool, which can ‘overcome vendor lock-in’,⁸² because interoperability allows two or more systems to ‘exchange and use data in order to perform their functions.’⁸³

Next to interoperability, the DA also introduces data portability rights.⁸⁴ These portability rights focus on making data and metadata ‘accessible [...] in a comprehensive, structured, commonly used and machine-readable format’ both to the device owner and third parties, upon request by the owner.⁸⁵ This portability requirement is broader than the GDPR’s right, since the DA also covers non-personal data.⁸⁶ The DA does not explicitly speak of ‘portability’, but this obligation is more in line with data portability – as offering a data export for use with another service – than interoperability – actual seamless co-operation between systems.

The Data Act thus follows the General Data Protection Regulation in introducing portability of data so that people can more easily switch between different competing services. The Data Act, additionally, requires interoperability, which not just concerns the transfer of data but also the actual co-operation of diverse systems.

4.4.3 Data Governance Act

The Data Governance Act is closely aligned with the Data Act and also provides certain interoperability obligations.

Mainly, the data intermediation services, as mentioned above, should integrate interoperability standards into their operations. Article 12 lists that the services must enhance interoperability across different sectors, for instance by converting data into certain formats.⁸⁷ They must also ensure interoperability between data intermediation services.⁸⁸ It is imaginable that such interoperability between services also helps the continuity of the data intermediation service after insolvency, as the other service can more easily work with the data processed by the insolvent service.

82 Recital 90 DA.

83 Art 2(40) DA.

84 For data portability: Art 4 (to the user) and Art 5 (to third parties) DA.

85 Art 4(1) & 5(1) DA. The DA uses the term ‘user’ to refer to the owner of a device, not the actual user, Art 2(12) DA.

86 Bárbara Lazarotto, ‘The Right to Data Portability: A Holistic Analysis of GDPR, DMA and the Data Act’ (2024) 15 European Journal of Law and Technology.

87 Art 12(d) DGA.

88 Art 12(i) DGA.

4.4.4 Digital Markets Act

The Digital Markets Act (DMA) applies since May 2023.⁸⁹ The DMA aims to curtail the market power of ‘gatekeepers’, i.e. the largest global online platforms (Meta, Google).⁹⁰ As part of this effort, the DMA introduces both data portability and interoperability obligations.

First, the DMA provides data portability rights to the end user for data generated ‘in the context of [...] the [...] core platform service’ (e.g., a virtual assistant).⁹¹ As in the Data Act, this data portability covers personal and non-personal data,⁹² but, in contrast, only covers a limited list of ‘core platform services’.⁹³ In the context of IoT, the most prominent core platform services are virtual assistants and cloud computing services.

Interoperability under the DMA directly addresses messaging apps, so that users can message through the platform they prefer, instead of being locked by specific vendors (e.g., Meta’s WhatsApp).⁹⁴ The DMA also contains more general interoperability requirements, which prevent gatekeepers from barring other services from their software, hardware, or operating systems.⁹⁵ Those latter general requirements also refer to IoT devices, such as ‘wearable devices’ and ‘virtual assistants’.⁹⁶ These devices provide platforms on which other developers build their applications (e.g., a running app for smart watches). Interoperability, in this context, does not merely cover seamless data exchange between systems, as in the DA and DGA. Instead, this form of interoperability focuses on access to the hardware and software necessary for other products to function. I delve further into these different types of interoperability in the following section.

5 Designing IoT in the face of manufacturer cessation

Existing update requirements that aim to ensure device maintenance rely on the longevity of the manufacturer, as shown by the Cyber Resilience Act and the Sale of Goods Directive. Such approaches do not offer a solution for consumers who are left with an Internet of Things device created by a non-existent manufacturer. Below, I further analyse how a legislative solution can circumvent manufacturer longevity, while employing pre-emptive measures.

Chapter 4 highlights that the insolvency of a service provider or manufacturer in the digital context is in fact a concern of the European legislators. The provisions show that the European legislators aim to alleviate some of the problems caused by insolvency by requiring pre-emptive measures, ranging from information obligations upon *looming* insolvency (Cyber

89 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L265/1 (DMA). For application date, see Art 54 DMA.

90 Art 1 & 2(1) DMA. European Commission, ‘Commission Designates Six Gatekeepers under the Digital Markets Act - European Commission’ <https://digital-markets-act.ec.europa.eu/commission-designates-six-gatekeepers-under-digital-markets-act-2023-09-06_en> accessed 9 February 2024.

91 Art 6(9) DMA. For a list of core platform services, see Art 2(2) DMA.

92 Recital 59 DMA.

93 Art 2(2) DMA.

94 Art 7(2) DMA.

95 Art 6(7) DMA.

96 Recital 55 DMA.

Resilience Act), to measures upon signing a contract for *possible future* insolvency (Digital Operational Resilience Act), and concerns for the continuity of the service *after* insolvency (Data Governance Act). In their work on cloud service provider insolvencies, Parry and Bisson also call for such an *ex ante* infrastructure ‘to minimise the impact of likely failures’.⁹⁷

Manufacturer-independence is the focal point of a pre-emptive solution for manufacturer cessation. The manufacturer ceasing operations is the exact cause of the problems for the consumer. Therefore, the manufacturer should set in place pre-emptive measures, but should not be primarily responsible for the continuation of the device after their cessation.⁹⁸ Ideally, as with current European product legislation (e.g., the Cyber Resilience Act), this system would take place within the rules set out for manufacturers, importers, and distributors, to ensure that products placed on the European market include these pre-emptive manufacturer-independent solutions.

Collective control refers to the capacity of a multitude of actors to shape the continuity of the device. The single dependency on the manufacturer has shown its pitfalls when the manufacturer ceases to exist and therefore a solution should rely on a more decentralised support model, without a single point of failure.⁹⁹

Based on the policies analysed in Chapter 4, there are two prominent options which offer pre-emptive, manufacturer-independent technical design within a framework of collective control: interoperability and open source code publication.

5.1 Interoperability

Interoperability relates to the capacity of systems to work together, regardless of their manufacturers or vendors.¹⁰⁰ As shown above, the EU legislator often utilises interoperability as a tool against platform power, for instance in the recently adopted Data Act (DA) and Digital Markets Act (DMA). Here, I address the core components of interoperability in the context of the Internet of Things.

5.1.1 A taxonomy of interoperability for the Internet of Things

The Data Act and Digital Markets Act highlight that interoperability is a dynamic concept. Interoperability exists across various dimensions. These three dimensions do not operate independently, but highlight which choices come to the fore when developers aim to implement interoperability.

Manufacturer interoperability

Interoperability can be horizontal or vertical. First, manufacturers can allow interoperability of the devices that they produce (e.g., Apple devices having access to Apple Messenger). This mode of interoperability is called ‘vertical’ interoperability. Second, manufacturers can

⁹⁷ Parry and Bisson (n 51) 28.

⁹⁸ Bradley and Barrera (n 10); Ghazaleh Shirvani and Saeid Ghasemshirazi, ‘Towards Sustainable IoT: Challenges, Solutions, and Future Directions for Device Longevity’ (arXiv, 2024) <<https://arxiv.org/abs/2405.16421>> accessed 25 June 2024.

⁹⁹ Bradley and Barrera (n 10).

¹⁰⁰ Brown (n 67); This is a general notion of interoperability. For further technical and non-technical definitions, see the discussion in Jörg Hoffmann and Begoña Gonzalez Otero, ‘Demystifying The Role Of Data Interoperability In The Access And Sharing Debate’ (2021) 11 JIPITEC 252, 255–257.

allow interoperability between their systems, devices, and platforms and those of other manufacturers, a mode called 'horizontal' interoperability. In the case of Apple Messenger, horizontal interoperability would mean that users could use devices (e.g., an Android phone) or services (e.g., Signal) from any manufacturer to communicate through Apple Messenger. The same goes for IoT: horizontal interoperability means that a smart voice assistant from Google can turn on a smart light from Philips.

Data exchange interoperability

If manufacturers aim to make their systems interoperable, they must consider how the interoperable systems exchange data. Two interconnected types of interoperability exist in the context of the technical design of interoperability: syntactic and semantic interoperability.

Syntactic interoperability generally refers to data exchange interoperability.¹⁰¹ To achieve syntactic interoperability in the Internet of Things, it is imperative that devices send and exchange data in commonly used data formats, such as XML or JSON.¹⁰² The intention of such formats is to display data in a machine-readable format, in contrast with data formats that aim to display data in a legible way for users (e.g., a PDF file). Through machine-readable formats, syntactic interoperability then allows data conversion between different units, such as temperatures recorded in Celsius by one device and in Fahrenheit by another.

Semantic interoperability refers to the capacity of systems to work with a common, shared vocabulary. Even when systems are syntactically interoperable, their definitions within the shared data sets can vary significantly. For instance, the manufacturer of one device might record temperature as 'heat', while the other records temperature as 'room_temperature'. Syntactic and semantic interoperability thus collaborate: through common machine-readable formats and vocabularies, devices and systems can more easily interoperate.

Methodology of interoperability

Interoperability can exist in a manufacturer's systems, processes, and devices. For Internet of Things devices, there are often two prevalent options: device interoperability and platform interoperability. Recently, researchers also suggested a third option in the context of device continuity: update interoperability.¹⁰³

Device interoperability depends on the actual device itself: the device can co-operate with other devices, for instance based on the use of similar wireless communication protocols. As mentioned earlier, Internet of Things devices exchange and transmit data through several protocols, such as Wi-Fi, Zigbee, and Z-Wave.¹⁰⁴ For device interoperability, it is thus necessary that, among such diverse protocols, devices can still communicate and exchange data.¹⁰⁵ Device interoperability thus depends on device-to-device co-operation.

Interoperability can depend on different levels of a device's software and hardware protocol stack. For instance, as mentioned above, interoperability can exist on the level of communication protocols, such as through standards like Zigbee or Bluetooth. Simultaneously,

101 Mahda Noura, Mohammed Atiquzzaman and Martin Gaedke, 'Interoperability in Internet of Things: Taxonomies and Open Challenges' (2019) 24 Mobile Networks and Applications 796, 799.

102 *ibid.*

103 Bradley and Barrera (n 10).

104 Eyhab Al-Masri and others, 'Investigating Messaging Protocols for the Internet of Things (IoT)' (2020) 8 IEEE Access 94880.

105 Noura, Atiquzzaman and Gaedke (n 101) 798.

the communication cannot be interoperable at all, but a USB-C port allows it to be charged with a USB-C charger, which works for a multitude of devices. There are thus also differences between hardware and software interoperability, with the former being easier than the latter, as evident from the transition to USB-C charging in the EU.¹⁰⁶

Platform interoperability is a method for interoperability that does not depend on the device, but on an integrated platform through which multiple systems can interoperate. This is the type of interoperability that the DMA mentions. The DMA mostly referred to operating systems as platforms on which applications are built, such as applications for virtual assistants or smart watches. However, there are also certain platforms that are specifically designed for IoT interoperability.

Smart home platforms such as Home Assistant and openHAB are examples of interoperable Internet of Things platforms.¹⁰⁷ These platforms allow users to exchange data between numerous devices from various manufacturers. Developers ensure that the data from device A is syntactically and semantically capable of interacting with device B. For this data conversion, the platform may rely on Application Programming Interfaces (APIs), a software interface that allows easy access to a device's data.¹⁰⁸ In addition, the platform allows communication between devices that transmit data using different communication protocols. For example, the platform ensures that a *Zigbee* motion sensor can enable a *Wi-Fi-based* light to turn on.

Through platform interoperability, the maintenance of IoT devices no longer relies on a single manufacturer. On an interoperable platform, data analysis happens through the platform. As such, platform interoperability offers an alternative independent from the manufacturer, as the platform's maintainers aim to ensure that they can read the device's data in the manner necessary for interoperability with the platform. For instance, a smart watch should send the correct sleep data, but the platform works with the data to indicate sleep level and health. In essence, the interoperable platform could thus replace the manufacturer's servers for data analysis.

In the case of IoT manufacturer cessation, Bradley and Barrera suggest a different type of interoperability: update pipeline interoperability.¹⁰⁹ In their framework, IoT software update pipelines are interoperable: devices can pull their updates from a range of repositories. Bradley and Barrera suggest that manufacturers pre-emptively ensure that their device is capable of detecting when they cease their support: 'instead of an unsupported device running progressively more outdated software, it can decide when to transition and switch to actively maintained software to avoid suffering from software degradation.'¹¹⁰ The device thus interoperates with multiple update pipelines, ensuring manufacturer-independent update continuity.¹¹¹

106 Directive (EU) 2022/2380 of the European Parliament and of the Council of 23 November 2022 amending Directive 2014/53/EU on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment [2022] OJ L315/30.

107 For an overview of these and similar open-source smart home platforms, see Brian Setz and others, 'A Comparison of Open-Source Home Automation Systems' (2021) 9 IEEE Access 167332.

108 For instance, many weather services are accessible through an API, which other software applications may use. For some examples, see <<https://github.com/public-apis/public-apis?tab=readme-ov-file#weather>>.

109 Bradley and Barrera (n 10) Bradley and Barrera do not define their framework within the context of 'interoperability' themselves, but their framework has a lot of interoperable characteristics.

110 *ibid* 11.

111 *ibid* 12.

Table 1: Dimensions of interoperability¹¹²

Manufacturer	Data exchange	Methodology
Vertical	Syntactical	Platform
Horizontal	Semantic	Device (software/hardware) Update

113

5.1.2 Designing interoperability as a solution to manufacturer cessation

Current practice shows that policies to stimulate interoperability between IoT systems has not yet been effective. Most IoT manufacturers do not yet offer sufficient co-operation between systems.¹¹⁴ The GDPR's right to data portability, for instance, strongly relies on data subjects to invest time into finding how a manufacturer allows them to port their data to another manufacturer.¹¹⁵ The GDPR shows that manufacturers are not eager to implement data portability policies and rights, especially as these rights are only required 'if technically feasible'.¹¹⁶ In conjunction with an overall lack of oversight and supervisory enforcement, the right to data portability in the GDPR thus did not meet its potential.

The interoperability taxonomy showed, in contrast with the current status of data portability in practice, that many options exist for creating interoperable IoT systems. Below, I address which of these components are key in the context of IoT manufacturer cessation, while acknowledging the shortcomings of the current practice.

First, preferably, the device can communicate with an interoperable platform, with device-to-device interoperability as a secondary option. An interoperable platform allows for the connection between heterogeneous devices and systems, thus simply covering a broader, horizontal scope than device-to-device interoperability. Through such heterogeneous communication, platform interoperability also inherently enables syntactic and semantic exchange between different devices, one of the key requirements raised by the right to data portability's issues.¹¹⁷ Home Assistant, one of the open-source interoperable IoT platforms mentioned in the taxonomy above, already offers a 'Works with Home Assistant' programme for devices that connect to the platform by design.¹¹⁸ Researchers have already pointed to the potential of such an approach in contrast to the current practice of IoT interoperability.¹¹⁹

113 These taxonomies are derived from Noura, Atiquzzaman and Gaedke (n 101).

114 Sarah Turner and others, 'The Exercisability of the Right to Data Portability in the Emerging Internet of Things (IoT) Environment' (2021) 23 *New Media & Society* 2861; Sarah Turner and Leonie Maria Tanczer, 'In Principle vs in Practice: User, Expert and Policymaker Attitudes towards the Right to Data Portability in the Internet of Things' (2024) 52 *Computer Law & Security Review* 105912.

115 Turner and Tanczer (n 113); Turner and others (n 113) 2875–2876.

116 Art 20(2) GDPR.

117 Laura Somaini, 'The Right to Data Portability and User Control: Ambitions and Limitations' (2018) 3 *MediaLaws*.

118 <https://partner.home-assistant.io/> accessed 4 March 2025.

119 Turner and others (n 113) 2876.

Second, and more complex, interoperability should help ensure device longevity through updates. There are two levels of updates required for the device: functionalities and security. In terms of functionality with the platform, the platform maintainers themselves could ensure that they keep the device functional with the platform. This is most likely only possible where the device's code base is open-source, as maintainers cannot ensure functionality without knowing how the device records and exchanges data. The maintainers should primarily address issues of data exchange, for example because of API changes, so that they keep access to the device's data for analysis on the platform.

Security updates, however, are most likely fully outside the reach of the platform maintainers, as they require knowledge of the device's code base. Here, the suggestions described above for update pipeline interoperability may come into play. A device can remain secure by pulling operating system updates, which include security updates, from sources other than the original manufacturer.¹²⁰ In an ideal situation, the manufacturer would pre-emptively support these capabilities for functionality and security updates, i.e. by setting up data conversion and update pipeline interoperability.

If we move back to the initial example of the VanMoof ebike, we can see the potential of interoperability and data portability for mitigating manufacturer cessation. The consumer can no longer rely on VanMoof to provide the decryption key; instead, the consumer now connects their ebike to, for instance, an interoperable platform. The platform is a software application which can extract simple data from the ebike, for instance its battery charge. This data exchange is provided through syntactic and semantic interoperability, so that the platform understands the data provided by the ebike. This system works for any type of data provision by smart home IoT products: the Insteon smart lights, for instance, could share their light status with the platform (on/off). In other words, the platform now provides the data visualisation previously available on the manufacturer's applications, because it can read the data in a similar, interoperable way.

There are, however, certain areas in which the role of interoperability remains unclear. When manufacturers require certain authentication protocols, an interoperable platform cannot simply bypass such authentication. VanMoof, for instance, kept the functionality for unlocking the ebike behind a login system, so that only the authenticated user – the assumed owner of the ebike – could unlock their ebike. This system design means that interoperable platforms must perform authentication through VanMoof's servers (e.g., using their API). When the manufacturer ceases their activities, such authentication becomes impossible, as was evident in the VanMoof case. Research shows some possible interoperable solutions to this authentication system, such as using the OAuth system (i.e., logging in through third parties, such as Google).¹²¹ The role for interoperability in this context is still developing.

Interoperability cannot offer a fully independent solution to IoT manufacturer cessation (yet): device updates and capabilities such as authentication remain currently remain largely outside the scope of (IoT) interoperability. A combination with other solutions could warrant further attention, such as with open source code publication.

¹²⁰ Bradley and Barrera (n 10) 12.

¹²¹ Se-Ra Oh and Young-Gab Kim, 'AFaaS: Authorization Framework as a Service for Internet of Things Based on Interoperable OAuth' (2020) 16 International Journal of Distributed Sensor Networks 155014772090638.

5.2 Open source code publication and development

Open source code publication holds potential in the context of IoT manufacturer cessation. For developers, the source code of a device reveals its inner workings. For instance, the source code tells developers how a device captures data, how it performs certain data analysis on the cloud, and what type of security measures the device uses. With the source code in hand, developers can therefore continue developing the device. For instance, a small IoT printer called ‘Little Printer’ was redesigned by a company in London after the original manufacturer ‘shut up shop’ and turned their servers off.¹²² With the help of an open source server, the developers were able to remove the dependency on the original manufacturer and thus resurrect devices that stopped functioning.

Open source code publication thus allows for manufacturer-independent collective control, as all interested developers (if they exist) can download the code and continue development according to their own needs and interests.

However, there are several barriers standing in the way of open source code publication.¹²³ As the CRA only includes code publication in the Recital, manufacturers do not have a legal *obligation* to release their source code online. For an IoT manufacturer, the device’s source code is often the foundational intellectual asset for the entire company. Manufacturers are thus generally hesitant to release it freely. It is imaginable that the manufacturer wants to keep the code secret so that they can, for instance, sell it during insolvency proceedings.

Additionally, source code release brings intellectual property considerations. The code could, for instance, partially rely on other software which is protected by intellectual property rights (e.g., copyright).¹²⁴ These intellectual property rights may stifle attempts to publish the source code publicly.

Open-source software is not a simple solution. Even if a developer agrees to work (voluntarily) on the code after the manufacturer ceases operations, the consumer will have to trust this developer and their security practices. Open-source software is often considered more secure than ‘proprietary’ software due to its transparent nature as anyone can audit the code.¹²⁵ However, open-source software security incidents have occurred in the past.¹²⁶ Furthermore, simply discovering and, even more, subsequently auditing open source code, is not a skill that the average consumer possesses.¹²⁷

122 Joe Rickerby, ‘Resilient Products — How Connected Devices Can Live On.’ (*Nord Projects*, 17 May 2019) <<https://medium.com/nord-projects/resilient-products-how-connected-devices-can-live-on-b9c0bb9534e6>> accessed 24 April 2024; Nord Projects, ‘Little Printers, a Friendly New Messaging App and Cloud Platform’ (*Nord Projects*) <<https://nordprojects.co/projects/littleprinters/>> accessed 27 February 2025; Lechelt and others (n 9).

123 Bradley and Barrera (n 10) 4–5.

124 P McCoy Smith, ‘Copyright, Contract, and Licensing in Open Source’ in Amanda Brock (ed), *Open Source Law, Policy and Practice* (2nd edn, Oxford University Press 2022).

125 Jaap-Henk Hoepman and Bart Jacobs, ‘Increased Security through Open Source’ (2007) 50 *Communications of the ACM* 79.

126 A prominent example is the Log4j incident, see Raphael Hiesgen and others, ‘The Log4j Incident: A Comprehensive Measurement Study of a Critical Vulnerability’ [2024] *IEEE Transactions on Network and Service Management* 1.

127 For an overview of the factors influencing the health of an open-source project, see Johan Linåker, Efi Papatheocharous and Thomas Olsson, ‘How to Characterize the Health of an Open Source Software Project? A Snowball Literature Review of an Emerging

In face of these challenges, some researchers have suggested that software escrows might offer a solution for software business continuity.¹²⁸ Software escrow exists in different forms. Some software escrows exist in the form of ‘source code escrow’, where the escrow agency releases the software’s source code after the developer ceases to exist. This form is very rarely seen, given the complex demands of source code publication.¹²⁹

However, given the challenges posed by IoT manufacturer cessation and the interest in source code publication in the Cyber Resilience Act, source code escrow could be re-considered. Source code escrow requires pre-emptive action: the manufacturer works with an escrow agency to ensure the release of their source code based on certain conditions, such as bankruptcy. Within this agreement, they can also pre-emptively ensure the correct transfer of intellectual property rights with any rights holders, or that certain parts of the code are adjusted so that intellectual property issues are prevented.

Software escrow can also exist as a form of insurance.¹³⁰ For instance, for the software-as-a-service industry, escrows mainly ensure that the developer’s hosting costs are paid for a certain period after they cease their activities.¹³¹ In this role, software escrow works more as an insurance fund for business continuity, depending on the contracts agreed by the manufacturer.

An insurance fund also covers the need for a hosting solution for the open-source software after code publication. There are several possibilities here: first, developers not only continue development, but also host a server that offers similar functions to the insolvent manufacturer’s servers; second, the escrow insurance fund ensures that hosting costs are paid, but this only covers hosting for a certain time, thus eventually standing in the way of device continuity; third, consumers can connect to a local server, such as the interoperable smart home platforms mentioned earlier, and download the open-source software there or transfer the software from another system to their IoT device (e.g., from their computer with a cable).

Source code publication offers a method that fits well within the framework suggested in this paper: it is a measure that manufacturers can i) pre-emptively set in place, for instance through source code escrow. After cessation, the source code allows other developers to sustain the device’s software or create new software: a ii) manufacturer-independent mode of iii) collective software development. The legislators can move forward from the Cyber Resilience Act’s nudge towards source code publication by overcoming the challenges posed above, particularly through concrete legal obligations for manufacturers. Furthermore, the legislators could explore the potential of combining interoperability (as an alternative data platform) and open source code publication (for device longevity through updates). In the end, it most likely a combination of efforts that can mitigate manufacturer cessation issues in the future.

Practice’, *Proceedings of the 18th International Symposium on Open Collaboration* (ACM 2022) <<https://dl.acm.org/doi/10.1145/3555051.3555067>> accessed 21 February 2025.

128 Tommy Van De Zande and Slinger Jansen, ‘Business Continuity Solutions for SaaS Customers’ in Björn Regnell, Inge Van De Weerd and Olga De Troyer (eds), *Software Business*, vol 80 (Springer Berlin Heidelberg 2011); Bartolini and others (n 11).

129 See also more concerns in Jonathan L Mezrich, ‘Source Code Escrow: An Exercise in Futility?’ (2001) 5 *Marquette Intellectual Property Law Review* 117.

130 Bartolini and others (n 11) 291–293.

131 Van De Zande and Jansen (n 127) 23.

5.3 Suggestions for future research

Above, I proposed a framework for future legislative solutions to the IoT manufacturer cessation problem. Given recent regulatory efforts, it seems that interoperability and open source code publication, ideally in conjunction, hold most potential as a solution to manufacturer cessation. However, these solutions have certain shortcomings, as IoT manufacturer cessation is a complex multi-faceted issue. Therefore, I propose several other directions for future research.

The framework suggested in this paper does not fully cover the diversity of the IoT. Devices range from MRI scanners in hospitals to tiny plant humidity sensors. The framework suggested in this paper may therefore require adjustment based on the specific device or its use case. Pre-emptive protection could only apply to manufacturers of certain sizes, while other contexts may necessitate interoperability without open source code development. These details will inadvertently differ depending on the IoT product and its use case.

Researchers and legislators could consider the option of a mandated local-only alternative for Internet of Things devices.¹³² This mandate would mean that devices must also have the capability to function without a connection to the manufacturer, through local-only connections. In the smart home context, there are already plenty of examples of such devices (e.g., Zigbee lights). With a local-only mode, the cessation of a manufacturer poses less of a threat to consumer devices, as the consumer can switch to the local-only alternative to keep the device functional. At the same time, the consumer still requires a solution for the lack of updates stemming from the manufacturer's cessation.

A mandated local-only alternative keeps devices connected, thus maintaining some security risks. An alternative approach could also be to mandate that IoT products can also be used as a 'dumb' version without connected capabilities, completely eliminating connected functionalities and thus security and dependency risks.¹³³ However, it is questionable whether this alternative is realistic or desirable. It is not likely that IoT consumers are interested in a 'dumb' version. Consumers deliberately choose IoT devices to feel technologically advanced.¹³⁴ They would thus rather not disconnect their devices, even for privacy reasons.¹³⁵ For this reason, consumers are likely to replace the dumb product with a new IoT device. In this light, the mandated dumb version does not substantially prolong the lifespan of a product or protect its consumers.

Second, within the realm of open source code publication, there are multiple cases for future research. Primarily, future research could focus on options for hosting after open source code publication, based on some of the examples mentioned above. In addition, given the barriers posed to open source code publication by intellectual property rights, more research is possible in this area to find how intellectual property can accommodate IoT manufacturer cessation solutions.

132 Urquhart, Sailaja and McAuley (n 75) 329–330.

133 Nathaniel Kim and Paul Ohm, 'Legacy Switches: A Proposal to Protect Privacy, Security, and the Environment from the Internet of Things' (2023) 84 Ohio State Law Journal 101.

134 Birgul Basarir-Ozel, Hande Bahar Turker and Vesile Aslihan Nasir, 'Identifying the Key Drivers and Barriers of Smart Home Adoption: A Thematic Analysis from the Business Perspective' (2022) 14 Sustainability 9053.

135 Marco Ghiglieri, Melanie Volkamer and Karen Renaud, 'Exploring Consumers' Attitudes of Smart TV Related Privacy Risks' in Theo Tryfonas (ed), *Human Aspects of Information Security, Privacy and Trust*, vol 10292 (Springer International Publishing 2017).

Finally, the different possible solutions to IoT manufacturer cessation leads to potential for different regulatory schemes per IoT device. For instance, given the diverse impact of manufacturer cessation on IoT devices, a local-only alternative may fit certain devices (or impacts) better than mandated source code escrow, which brings certain financial requirements for the manufacturer. The Cyber Resilience Act already categorises IoT devices based on their cybersecurity risk. A differentiation in pre-emptive obligations per type of IoT device, or perhaps based on price or other factors, could also be further explored.¹³⁶

6 Conclusion

Internet of Things devices combine hardware and software and operate across diverse sectors. The EU legislators have recently regulated many aspects of Internet of Things products, primarily in relation to their overall cybersecurity and privacy practices. However, this paper shows that a legal gap remains: the position of the consumer after the IoT device's manufacturer ceases their operations.

The manufacturer's cessation is a complex problem, since manufacturers have diverse reasons to cease their operations. Additionally, cessation impacts IoT products in different ways. A smart light system may still work manually after cessation, while other products fully rely on mobile applications hosted by the developer which become unavailable. This paper focused on manufacturers that have financial reasons for ceasing their operations (as this is most prevalent in practice) and products that ceased to function entirely (as, in this case, a solution is most pressing to protect consumer interests).

Most EU legislation contains update obligations for modern products, to ensure that manufacturers do not simply ignore their devices when they want to focus their attention elsewhere. However, these update obligations, as exemplified by the Cyber Resilience Act and Sale of Goods Directive, rely on a key assumption: longevity of the manufacturer. Instead, when the manufacturer ceases to exist, their responsibility for updating or supporting their product disappears with them.

Other measures do show a hint of promise for consumers in the context of IoT manufacturer cessation, in the form of pre-emptive measures. The Cyber Resilience Act, Digital Operational Resilience Act and Data Governance Act include such pre-emptive measures, which require entities to concern themselves with the situation after they or third parties cease operations. This paper explores the potential of pre-emptive measures as a cornerstone for solving the IoT manufacturer cessation problem.

Pre-emptive measures are not sufficient by themselves. This paper adds two properties for these measures: manufacturer-independency and collective control. The consumer should no longer have to rely on the manufacturer for the solution, because the manufacturer ceases to exist. Furthermore, a system of collective control should ensure that there is no longer a single point of failure: the consumer should not be stuck in a loop of failing organisations.

¹³⁶ See for instance the differing expectations surrounding privacy and security based on certain device characteristics in Lorenz Kustosch and others, 'Measuring Up to (Reasonable) Consumer Expectations: Providing an Empirical Basis for Holding IoT Manufacturers Legally Responsible', *Proceedings of the 32nd USENIX Security Symposium* (2023).

Based on recent EU digital policy initiatives, the paper offers two examples of such manufacturer-independent collective control: interoperability and open source code publication. First, interoperability is the capacity of the IoT device to exchange data with other devices and platforms. Interoperability is now also found in legal policies, often together with data ‘portability’, which generally refers to data transfers between two systems. Data portability is an important right under the General Data Protection Regulation and is found, together with interoperability, in the recently enacted Data Act, Data Governance Act and Digital Markets Act. Based on a taxonomy of current interoperability research in the IoT domain, this paper suggests that platform interoperability could solve many of the issues brought by IoT manufacturer cessation. However, interoperability alone cannot ensure that devices remain updated. Some limitations thus remain.

Second, the paper explores open source code publication, which allows developers other than the manufacturer to continue working on the device’s code base. Source code publication currently faces several barriers, such as intellectual property rights, that require further research or legislative progress. However, the paper considers open source code publication as a possible alternative to, or companion of, interoperability in the future. Given the limitations of both options, the paper closes with some suggestions for future research.

References

- Al-Masri E and others, 'Investigating Messaging Protocols for the Internet of Things (IoT)' (2020) 8 IEEE Access 94880
- Bartolini C and others, 'Cloud Providers Viability: How to Address It from an IT and Legal Perspective?' in Jörn Altmann, Gheorghe Cosmin Silaghi and Omer F Rana (eds), *Economics of Grids, Clouds, Systems, and Services*, vol 9512 (Springer International Publishing 2016)
- Basarir-Ozel B, Turker HB and Nasir VA, 'Identifying the Key Drivers and Barriers of Smart Home Adoption: A Thematic Analysis from the Business Perspective' (2022) 14 Sustainability 9053
- Boniface C, Urquhart L and Terras M, 'Towards a Right to Repair for the Internet of Things: A Review of Legal and Policy Aspects' (2024) 52 Computer Law & Security Review 105934
- Bradley C and Barrera D, 'Escaping Vendor Mortality: A New Paradigm for Extending IoT Device Longevity' *New Security Paradigms Workshop* (ACM 2023)
- Brown I, 'Interoperability as a Tool for Competition Regulation' (LawArXiv 2020) preprint <<https://osf.io/fbvxd>> accessed 6 February 2024
- Carman A, 'They Welcomed a Robot into Their Family, Now They're Mourning Its Death' (*The Verge*, 19 June 2019) <<https://www.theverge.com/2019/6/19/18682780/jibo-death-server-update-social-robot-mourning>> accessed 24 April 2024
- , 'Jibo, the Social Robot That Was Supposed to Die, Is Getting a Second Life' (*The Verge*, 23 July 2020) <<https://www.theverge.com/2020/7/23/21325644/jibo-social-robot-ntt-disruptionfunding>> accessed 4 September 2024
- Chen J and others, 'Who Is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption' (2020) 10 International Data Privacy Law 15
- Chen J and Urquhart L, '“They'Re All about Pushing the Products and Shiny Things Rather than Fundamental Security”: Mapping Socio-Technical Challenges in Securing the Smart Home' (2022) 31 Information & Communications Technology Law 99
- Chiara PG, 'The Cyber Resilience Act: The EU Commission's Proposal for a Horizontal Regulation on Cybersecurity for Products with Digital Elements: An Introduction' [2022] International Cybersecurity Law Review
- De Hert P and others, 'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services' (2018) 34 Computer Law & Security Review 193
- European Commission, 'Commission Designates Six Gatekeepers under the Digital Markets Act - European Commission' <https://digital-markets-act.ec.europa.eu/commission-designates-six-gatekeepers-under-digital-markets-act-2023-09-06_en> accessed 9 February 2024
- , 'Staff Working Document Impact Assessment Report Accompanying the Document Proposal for a Regulation on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020' SWD (2022) 282 final

Geiregat S, 'What Digital Content Consumers (Should) Want' in Anna K Bernzen, Karina Grisse and Katharina Kaesling (eds), *Immaterialgüter und Medien im Binnenmarkt* (Nomos Verlagsgesellschaft mbH & Co KG 2022)

Gerner-Beuerle C and Schuster E-P, 'The Evolving Structure of Directors' Duties in Europe' (2014) 15 *European Business Organization Law Review* 191

Ghiglieri M, Volkamer M and Renaud K, 'Exploring Consumers' Attitudes of Smart TV Related Privacy Risks' in Theo Tryfonas (ed), *Human Aspects of Information Security, Privacy and Trust*, vol 10292 (Springer International Publishing 2017)

Gigaset, 'Gigaset Smart Home/Care Wurde Eingestellt' <https://www.gigaset.com/ch_de/cms/smart-home-uebersicht.html> accessed 16 April 2024

'Gigaset Smart Home/Care Staakt Zijn Diensten Vanaf 29 Maart 2024' <https://www.gigaset.com/nl_nl/cms/smart-home-overzicht.html> accessed 11 April 2024

Goodwin C and others, 'Quantifying Device Usefulness - How Useful Is an Obsolete Device?' in José Abdelnour Nocera and others (eds), *Human-Computer Interaction – INTERACT 2023*, vol 14145 (Springer Nature Switzerland 2023)

Guerrini F, 'Consumer Protection In Gaming: European Initiative Targets Video Game Publishers' (*Forbes*) <<https://www.forbes.com/sites/federicoguerrini/2024/08/30/consumer-protection-in-gaming-european-initiative-targets-video-game-publishers/>> accessed 27 February 2025

Hiesgen R and others, 'The Log4j Incident: A Comprehensive Measurement Study of a Critical Vulnerability' [2024] *IEEE Transactions on Network and Service Management* 1

Hoepman J-H and Jacobs B, 'Increased Security through Open Source' (2007) 50 *Communications of the ACM* 79

Hoffmann J and Gonzalez Otero B, 'Demystifying The Role Of Data Interoperability In The Access And Sharing Debate' (2021) 11 *JIPITEC* 252

Hon WK, Millard C and Singh J, 'Twenty Legal Considerations for Clouds of Things' (2016) 2016 *Queen Mary University of London, School of Law Legal Studies Research Paper*

Jovanée A, 'Four Classic Command & Conquer Titles Are Now Open Source' (*Polygon*, 27 February 2025) <<https://www.polygon.com/news/531365/command-and-conquer-open-source-code-ea>> accessed 3 March 2025

Kalamees P, 'Goods With Digital Elements And The Seller's Updating Obligation' (2021) 2 *JIPITEC* 131

Kim N and Ohm P, 'Legacy Switches: A Proposal to Protect Privacy, Security, and the Environment from the Internet of Things' (2023) 84 *Ohio State Law Journal* 101

Kustosch L and others, 'Measuring Up to (Reasonable) Consumer Expectations: Providing an Empirical Basis for Holding IoT Manufacturers Legally Responsible' *Proceedings of the 32nd USENIX Security Symposium* (2023)

Lechelt S and others, 'Designing for the End of Life of IoT Objects' *Companion Publication of the 2020 ACM Designing Interactive Systems Conference* (ACM 2020) <<https://dl.acm.org/doi/10.1145/3393914.3395918>> accessed 24 April 2024

Linåker J, Papatheocharous E and Olsson T, 'How to Characterize the Health of an Open Source Software Project? A Snowball Literature Review of an Emerging Practice' *Proceedings of the 18th International Symposium on Open Collaboration* (ACM 2022) <<https://dl.acm.org/doi/10.1145/3555051.3555067>> accessed 21 February 2025

Lunden I, 'VanMoof, the e-Bike Startup, Officially Declared Bankrupt in The Netherlands' (*TechCrunch*, 18 July 2023) <<https://techcrunch.com/2023/07/18/vanmoof-goes-vanpoof-bankruptcy/>> accessed 13 November 2023

Mezrich JL, 'Source Code Escrow: An Exercise in Futility?' (2001) 5 *Marquette Intellectual Property Law Review* 117

Milenkovic M, *Internet of Things: Concepts and System Design* (Springer International Publishing 2020) <<http://link.springer.com/10.1007/978-3-030-41346-0>> accessed 7 August 2024

Nord Projects, 'Little Printers, a Friendly New Messaging App and Cloud Platform' (*Nord Projects*) <<https://nordprojects.co/projects/littleprinters/>> accessed 27 February 2025

Noura M, Atiquzzaman M and Gaedke M, 'Interoperability in Internet of Things: Taxonomies and Open Challenges' (2019) 24 *Mobile Networks and Applications* 796

OConnor T, Enck W and Reaves B, 'Blinded and Confused: Uncovering Systemic Flaws in Device Telemetry for Smart-Home Internet of Things' *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks* (ACM 2019)

OConnor T, Jessee D and Campos D, 'Through the Spyglass: Towards IoT Companion App Man-in-the-Middle Attacks' *Cyber Security Experimentation and Test Workshop* (ACM 2021)

Parry R and Bisson R, 'Legal Approaches to Management of the Risk of Cloud Computing Insolvencies' (2020) 20 *Journal of Corporate Law Studies* 421

Purdy K, 'Valve Releases Full Team Fortress 2 Game Code to Encourage New, Free Versions' (*Ars Technica*, 19 February 2025) <<https://arstechnica.com/gaming/2025/02/valve-releases-full-team-fortress-2-game-code-to-encourage-new-free-versions/>> accessed 3 March 2025

Rich J, 'What Happens When the Sun Sets on a Smart Product?' (*Federal Trade Commission*, 13 July 2016) <<https://www.ftc.gov/business-guidance/blog/2016/07/what-happens-when-sun-sets-smart-product>> accessed 31 January 2024

Ricker T, 'Cowboy Releases Cheeky App to Keep VanMoof E-Bike Riders on the Road' (*The Verge*, 13 July 2023) <<https://www.theverge.com/2023/7/13/23793591/cowboy-vanmoof-key-app-download-ios-android>> accessed 31 January 2024

Rickerby J, 'Resilient Products — How Connected Devices Can Live On.' (*Nord Projects*, 17 May 2019) <<https://medium.com/nord-projects/resilient-products-how-connected-devices-can-live-on-b9c0bb9534e6>> accessed 24 April 2024

Schulte-Nölke H, 'Digital Obligations of Sellers of Smart Devices under the Sale of Goods Directive 771/2019' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Smart Products* (Nomos 2022)

- Setz B and others, 'A Comparison of Open-Source Home Automation Systems' (2021) 9 IEEE Access 167332
- Shank DB and others, 'Knowledge, Perceived Benefits, Adoption, and Use of Smart Home Products' (2021) 37 International Journal of Human–Computer Interaction 922
- Shirvani G and Ghasemshirazi S, 'Towards Sustainable IoT: Challenges, Solutions, and Future Directions for Device Longevity' (arXiv, 2024) <<https://arxiv.org/abs/2405.16421>> accessed 25 June 2024
- Smith PM, 'Copyright, Contract, and Licensing in Open Source' in Amanda Brock (ed), *Open Source Law, Policy and Practice* (2nd edn, Oxford University Press 2022)
- Somaini L, 'The Right to Data Portability and User Control: Ambitions and Limitations' (2018) 3 MediaLaws
- Tajti(Thaythy) T, 'Unprotected Consumers in the Digital Age: The Consumer-Creditors of Bankrupt, Abandoned, Defunct and of Zombie Companies' (2019) 24 Tilburg Law Review 3
- Tuohy JP, 'Insteon Customers Turned Insteon's Lights Back on' (*The Verge*, 9 June 2022) <<https://www.theverge.com/2022/6/9/23161803/insteon-customers-bought-company-restored-service>> accessed 31 January 2024
- Turner S and others, 'The Exercisability of the Right to Data Portability in the Emerging Internet of Things (IoT) Environment' (2021) 23 New Media & Society 2861
- Turner S and Tanczer LM, 'In Principle vs in Practice: User, Expert and Policymaker Attitudes towards the Right to Data Portability in the Internet of Things' (2024) 52 Computer Law & Security Review 105912
- Urquhart L, Lodge T and Crabtree A, 'Demonstrably Doing Accountability in the Internet of Things' (2019) 27 International Journal of Law and Information Technology 1
- Urquhart L, Sailaja N and McAuley D, 'Realising the Right to Data Portability for the Domestic Internet of Things' (2018) 22 Personal and Ubiquitous Computing 317
- Van De Zande T and Jansen S, 'Business Continuity Solutions for SaaS Customers' in Björn Regnell, Inge Van De Weerd and Olga De Troyer (eds), *Software Business*, vol 80 (Springer Berlin Heidelberg 2011)
- Von Ditzfurth L and Lienemann G, 'The Data Governance Act: – Promoting or Restricting Data Intermediaries?' (2022) 23 Competition and Regulation in Network Industries 270
- Yadav P and others, 'Network Service Dependencies in Commodity Internet-of-Things Devices' *Proceedings of the International Conference on Internet of Things Design and Implementation* (ACM 2019) <<https://dl.acm.org/doi/10.1145/3302505.3310082>> accessed 4 June 2024

6.

Regulating Smart Device Support Periods: User Expectations and the European Cyber Resilience Act

This article was published in the Proceedings of the 32nd USENIX Conference on Security Symposium on 13 August 2025. The text was last revised on 16 May 2025, with some minor textual corrections for inclusion in this dissertation.

Lorenz Kustosch, Carlos Gañán, Mattis van 't Schip, Michel van Eeten and Simon Parkin, 'Regulating Smart Device Support Periods: User Expectations and the European Cyber Resilience Act' Proceedings of the 34th USENIX Security Symposium (2025).

Abstract

Supporting consumer IoT devices with updates is crucial to ensure their security. However, this support period is usually shorter than the device's actual lifespan, resulting in millions of unsupported and vulnerable devices. The upcoming European Cyber Resilience Act (CRA) addresses this by requiring manufacturers to support their products for the expected use time, which should be based on reasonable user expectations. In this work, we thus empirically explore the concept of user expectations regarding smart devices' use times and security provisions by conducting a large-scale survey in five EU countries ($n = 993$). We find that respondents' smart device use times and lifetime expectations exceed the CRA's baseline of five years for a majority of device categories and vary substantially across device categories, their "smartness", and individuals. Respondents also consider different factors for the lifetimes of smart and conventional devices. Surprisingly, a majority of respondents expected update support to correspond with devices' full lifetimes, highlighting how the current market dynamics of short support times seem to contrast expectations. Our results provide novel insights for manufacturers and market authorities who will need to determine support periods for smart products in the coming years.

1 Introduction

To secure the growing population of consumer IoT devices from an evolving threat landscape, continuous support over the product’s lifecycle is crucial. However, security updates for such smart devices often end prematurely and their presence or duration is often not disclosed to consumers at purchase. A recent report from the US Federal Trade Commission found that for 89% of the reviewed smart products, no disclosure on the duration of updates support was provided [18], seemingly a status-quo in the smart device market [40, 43].

Various regulatory and policy initiatives aim to increase transparency of the software support duration to provide certainty to consumers about the security capabilities of the devices that they purchase. Within this, there is an expectation that consumers will gravitate toward more secure devices within purchase decisions. The US Cyber Trust Mark announced in 2023 is a voluntary product labeling scheme where manufacturers of smart devices disclose the support period as part of the label [1, 32]. In the UK, the PSTI act *requires* manufacturers to disclose a minimum support period for security updates [47] to comply with the law, instead of the voluntary label approach in the US.

While *disclosing* information to consumers for a more informed purchase is an important step, the question then arises of *how long* this support should actually be provided. The approach of the European Commission is embodied in the Cyber Resilience Act (CRA) [50], launched in 2024 and coming into force in 2027; to the best of our knowledge, the CRA is the first regulation that explicitly sets legal product requirements on a *duration* for how long security measures must be provided across a broad range of products. Specifically, security vulnerabilities of “products with digital elements” must receive security updates for their *expected use time* but at least five years¹.

In the determination of the expected use time, that is, device lifetime, reasonable user expectations play a crucial role. Manufacturers will have to actively determine this period based on users’ expectations and disclose how they considered this in the product’s technical documentation. Similarly, market surveillance authorities will check such documentation and, in turn, determine what they see as a reasonable user expectation to determine compliance with the CRA. If they find that the support duration for a product violates expectations, they could remove the device from the EU market.

Thus, the user perspective, previously an afterthought in security support duration, suddenly takes center stage in the regulatory realm with global implications. Manufacturers sell the same smart devices in other markets than the EU and could streamline global compliance efforts and release the same security updates as in the EU, following the “Brussels Effect” [7, 38, 31]. However, the abstract concept of reasonable user or consumer expectations regarding a product’s expected use time bears uncertainty for smart device manufacturers and market surveillance authorities. For instance, is it reasonable to expect that a smart washing machine will be used for longer than a smartwatch and should thus be patched for longer?

Prior research only provides limited insights into the use time or update support duration of smart devices. While [25] studied smart home users’ perspectives on the end of support and [29] empirically measured reasonable consumer expectations regarding security and privacy incidents with consumer IoT devices, the expected or observed *duration* of device use or update

1 With exceptions possible (Article 13(8) and Recital 60).

support has not been directly measured, although [34, 36] find that longer support periods were generally preferred by consumers.

As the CRA explicitly links the duration for security support to users' expectations of the product's lifetime, we aim to fill this gap by conducting a large survey among EU consumers to empirically assess their expectations and behaviors regarding smart device use times. We ask the following Research Questions: (i) How do consumers use their smart devices, and for how long?; (ii) How long do consumers expect different smart device categories to last, and which factors influence these expectations?; (iii) How do consumers perceive security and software update support over smart devices' lifespans?; and; (iv) Are there differences among EU member states regarding consumers' smart device usage, expectations, and security and software support perceptions?

We make the following contributions:

- We conduct an online survey with 993 participants in five different EU member states and collect empirical data on and explain a methodological approach to a concept of high relevance in the coming years: Smart device use times and users' expectations regarding them. Thus, we provide an empirical basis for manufacturers and market surveillance authorities how to conceptualize and approach users' expectations regarding smart product lifetimes.
- We measure smart device *use times* by studying 2485 individual smart devices and measure lifetime *expectations* via smart device vignettes. While expectations varied across devices and individuals, we find that, in aggregation, almost all studied smart products were expected to last longer than the CRA's baseline of five years, despite respondents factoring in aspects like fast innovation and replacement, incompatibility, or planned obsolescence. Additionally, a majority of respondents expected update support to correspond to the device's full lifetime, highlighting how the CRA's provisions seem to meet expectations already.
- We extend previous work on smart devices' end of support by focusing on the concept of security support *duration*. We find that respondents were aware of security updates being crucial to mitigate security risks, although updates were generally opaque (non-perceptible), and their eventual end was not a strong trigger to stop device usage - better alternatives or declining functional performance were much stronger motivators.

In the remainder of the paper, we first consider the regulatory underpinnings and related work on users' expectations regarding smart devices, followed by our survey methodology and results. We then contextualize our findings in the wider regulatory and academic field and provide recommendations for manufactures and market authorities.

2 Background and Related Work

Here we frame existing IoT users' experiences with IoT security and privacy against legal processes involving reasonable expectations. These are then considered alongside the expectations then placed upon other actors in the market, such as manufacturers and retailers.

2.1 EU support duration regulations

User or “consumer” expectations are often part of legal considerations. In the context of cybersecurity, the most prominent piece of current legislation in the EU is the Cyber Resilience Act (CRA), adopted at the end of 2024. It regulates manufacturers that place “products with digital elements” (i.e., software and hardware products) on the EU market. It thus has global impact, as any manufacturer must adopt its measures when placing products on the EU market, regardless of their location. Internet of Things (IoT) devices are prominent examples of products with digital elements; they must adhere to numerous cybersecurity requirements (e.g., security-by-default, (Annex I(2)(a)). The CRA reserves a special position for certain categories of IoT devices. For instance, smart home security devices and virtual assistants are an “important” category due to larger security risks than average products with digital elements.

The manufacturer must, as part of a comprehensive list of requirements, ensure that any detected vulnerabilities are swiftly mitigated for the entire “support period” of their device. Manufacturers must determine this support period themselves, based on several criteria provided in the CRA (Article 13(8)). The manufacturers *shall* (i.e., must) consider in this determination: “reasonable user expectations”, the nature of the product (including its intended purpose), and other EU legislation that may already determine lifetimes for the product category. Additionally, manufacturers *may* take into account support periods of similar products, the availability of operating environments, the support period for integral components of the product created by third-parties and guidance provided by administrative authorities (the “ADCO”). Manufacturers are thus obligated to take into account how long users would reasonably expect their product to remain in use, i.e., the product’s expected lifetime.

Manufacturers must include the chosen support period with the product’s documentation (Article 13(19)). Furthermore, they must share the information on which they base the chosen support period (Article 13(8)). Market authorities must monitor chosen support periods and take corrective action when they consider the support period incorrect.

European product legislation often connects product support periods and user expectations. For instance, the Sale of Goods Directive (SG Directive) offers another example of this approach [49], aiming to protect consumers when signing a sales contract. It requires that goods with digital elements (e.g., smart products) remain in conformity with the sales agreement. For instance, a video app on a smart TV cannot suddenly lower its picture quality, if the initial contract noted a higher quality. It thus requires the product to receive updates, including security updates, “for the period of time [...] that the consumer may reasonably expect” to conform with the contract (Article 7(3)). However, in contrast to the CRA, the SG Directive does not place a burden on the seller to provide how they assessed their support period and to share it with consumers and market authorities.

Thus, the support period determined by the manufacturer plays a key role for smart devices in the EU. Manufacturers and market authorities must know what support periods are reasonable for a breadth of product categories. Consumers, at the same time, can compare support periods so they can make informed purchase decisions. Given these dynamics introduced by the CRA, it is vital to understand user expectations regarding support periods of products with digital elements.

2.2 Consumer expectations and perspectives of IoT security and product lifespans

Prior work has studied consumer expectations of security support for IoT devices [29] – this included manufacturer liability and responses in case of particular incidents, finding that expectations differ per device and that, when measuring expectations in the legal context, it is important to distinguish between reasonable (realistic) and normative expectations (ideal). Here we study conformity to update support commitments, as in the CRA.

Concerning software support for IoT specifically, there is great uncertainty among users, even when directly presented with pertinent information (such as “security labels”) [25, 23], for instance that users say updates are important, but do not understand the implications of using unsupported devices or what end of support means [16], all the while lacking clarity as to the purpose of updates [22]. These outcomes point to users needing assurance in a market that is full of uncertainty – this suggests there could be value in not only setting a support duration, but strengthening assurances that it will remain over time, as a reliable “minimum” duration.

Further, when software support duration is considered as a product label attribute during device selection [15], prior work suggests there is a demand among consumers for the delivery of security updates for IoT devices for a longer period of time than they are accustomed to (e.g., [34, 36]). Thus, where previous work has suggested that support assurances would be valued, it lacks a clear connection to the expected duration of update support and, most importantly in the context of the CRA, the *expected* lifetime of IoT products, as [34, 36] measured *preferred* update support duration with predetermined values by the researchers (e.g., 2 years, 6 years, and lifetime).

However, consumers’ expectations of products’ lifetimes have been measured before, just not in the context of security and privacy, but in the domain of sustainability [20, 19, 39, 37, 52, 12]. For instance, [12, 20] and [39] measure expected lifetime or perceived longevity importance for product categories like mobile phones or vacuum cleaners. However, smart devices and the role of software updates and security were not directly studied. This research highlights different forms of product lifetime expectations, namely *intended* lifetime (how long a product is intended to be in use by its current owner), *ideal* lifetime (how long a product should ideally last), and *predicted* lifetime (how long a product will likely last). A conceptual piece by Bradley et al. examines similar concerns [8], outlining the conflicting interests between continued security patching and device longevity, proposing a paradigm shift: an architecture and differential responsibilities for different actors to keep devices running and secure for as long as possible. Here, we examine how user perceptions inform the provisions needed in determining support duration relative to the CRA.

In examining the electronics repair industry, Ceci et al. [10] found that 12% of their 112 survey participants stated that a smartphone or tablet never broke; however, the cost and hassle of getting a device repaired were major factors where participants had a device that developed problems but that they did not seek to get repaired. In studying views on IoT device obsolescence, Vats et al. [51] found that when interview participants were faced with external events such as an IoT device ceasing to function, needing an update, or losing smart features, they would try to find terms in the user agreement that would force the manufacturer to take responsibility (and feel a lack of agency if they could not); this indicates an existing gap that CRA assurances could fill. The interview participants of Haney et al. [21] referred to an unspoken agreement at device purchase, that a manufacturer should protect buyer security

and privacy, but that participants differed in how sure they were that a manufacturer could uphold those expectations, trusting larger firms as being more competent to do so.

3 Method

To explore user expectations regarding smart devices' lifetimes, we conducted an online survey with 993 participants recruited on the crowdsourcing platform Prolific [41] during November and December 2024. As the CRA is an EU legislation, we recruited an EU-based sample from France, Germany, Poland, Spain, and The Netherlands. We selected this subset as countries belong to the largest member states, together account for over half of the full EU population, vary in geographic location, culture, and markets, and to retain an appropriate sample size per country for robust statistical comparison. Due to the CRA requiring an EU-wide uniform approach, we were interested to study the potential variety of market dynamics across countries, such as user journeys, purchase channels, and experiences with smart devices and their security, potentially requiring differentiated support structures for users.

In the following, we detail our survey design, data collection and analysis, and the resulting sample.

3.1 Survey Design

We first explain some of our conceptual considerations around the notions of consumer expectations and device lifetime, followed by survey design and preparation for publication in different countries.

3.1.1 Conceptualizing device lifetime expectations

We aimed to align with the CRA definition of product lifetime, which is “the length of time during which the product is expected to be in use”, which should be based on “reasonable user expectations, the nature of the product, including its intended purpose”. Previous empirical work on consumer expectations provided a solid methodological basis for phrasing this question in a survey. Gnanapragasam et al. [19] stress the importance of clearly differentiating between three forms of expected product lifetimes: *Intended* (how long a product is intended to be in use by its current owner), *ideal* (how long a product should ideally last), and *predicted* (how long a product will likely last). Other related work on smart devices' consumer expectations highlights the necessity to differentiate *normative* (ideal) and *reasonable* (realistic) expectations and argues that realistic expectations correspond more closely to the legal notion of reasonableness, rather than normative ideals [29].

Thus, we conceptualized user expectations about product lifetimes according to the following two criteria:

- The expectation is about a *predicted* period of time for how long a given smart device will remain functional to be used for its intended purpose, not what is desired for how long it *ideally* should last. i.e., the expectation should be reasonable.
- This period should be independent of ownership, as devices can be sold or gifted onward [30], and we did not want to measure the initial use cycle, i.e., a user's preference when to move to a newer device.

Thus, when asking about the expected lifetime of a smart device, our question was: “*If you had to predict, for how many years do you expect such a device to last?*” (Q5.1.1). However, we also considered *intended* product lifetimes (how long a product is intended to be in use by its current owner) by inquiring with participants about how long they plan to continue using their *own* smart devices to then form a measure of their use time, adding up the durations of past use and intended future use.

3.1.2 Measuring device lifetime expectations

To quantify expectations about smart devices’ lifespans, we designed vignettes for several prototypical devices and presented survey participants with a random subset of them to measure how long they would expect the device to last. Table 1 depicts our selection of devices and vignettes can be found in Appendix A.

Vignettes are short descriptions or scenarios, to provide respondents with context to elicit a response and are commonly used in security and privacy research [35, 2, 5, 3, 29]. Our vignettes described the device at hand, its high-level features, how it can be used, and its smart capabilities to ensure that respondents without any experience with it could also form a picture of this product. We followed common practice in security user research [25, 22, 29, 34], and selected a diverse range of smart devices with varying use cases, price points, and security and privacy implications and perceptions, which should all fall under the CRA.

As many white goods products become increasingly smart, we also tested whether expected lifetimes would differ between smart and conventional versions. We were interested in how participants would factor in the additional aspects introduced by the “smartness” into their expectations, such as software updates, online connectivity, and security or privacy risks.

We did not include a conventional version for all smart devices, as for some, we considered them an entirely different product based on their primary use case. For instance, we did not consider a regular watch (primary use: showing the time) a fair comparison to a smartwatch (primary use: running applications like health tracking, or messaging/notification).

3.1.3 Survey design process

We drafted the initial survey based on our research questions and the content examined for the literature review (Section 2). We also gathered feedback during a workshop with thirteen experts working in the fields of IoT security and law where the survey draft was presented, jointly discussed in the group, and subsequently improved regarding clarity, wording, and specificity of the IoT devices.

At this point, we involved policymakers and conducted four online meetings with policymakers from different EU member states, all involved in the drafting or future enforcement of the CRA. In the meetings, we inquired about their interpretations of the CRA’s support period provisions and asked for their involvement in the study. We received feedback on our survey and suggestions for questions relevant to their work from 3 of the 4 organizations and then improved the survey regarding wording and flow and added a question about the purchase channels of respondents’ own devices (Q2.4 & Q2.5), as this was of interest for several policymakers.

A pilot run of the survey was conducted with 25 participants recruited on Prolific to check for any technical problems, question understanding, completion time, or any answer options

Table 1: Selection of devices used in the vignettes. ‘Conv. Comp.’ = If a comparison to the conventional version of that product was made.

Device type	Product category	Conv. Comp.
Smart speaker	Entertainment	No
Smart thermostat	Home / Energy management	Yes
WiFi Solar inverter	Home / Energy management	Yes
Smart camera	Home security	No
Smart doorlock	Home security	No
Home router	Network equipment	No
Connected printer	Office equipment	Yes
Smart Smoke Detector	Sensors	Yes
Smart watch	Wearables	No
Smart washing machine	White Goods	Yes
Robot vacuum	White Goods	Yes

not provided in our multiple-choice questions (i.e., Q4.3, Q4.4, Q7, Q9.1, Q9.2). Participants took 14.8 minutes on average and no technical issues emerged. Only minor adjustments were necessary for some questions for clarity, despite the pilot survey allowing respondents to indicate where they felt unsure about their answer.

After the pilot study, the survey was translated from English into the five countries’ respective languages (French, German, Polish, Spanish, and Dutch), by first being translated using Qualtrics’ native automatic translation tool based on Google Translate [42]. This automatic translation was then checked and adjusted by five different native speakers (where this included names of popular online stores). The final survey can be found in the appendix A.

3.2 Recruitment and participants

Participants were recruited on the crowd-sourcing platform Prolific with the following screening criteria: Participants should reside in one of the five member states, be fluent in the respective official language, have an approval rate in prior studies of at least 95%, and completed at least five other submissions on the platform. We opened a separate survey invite for each age group to avoid bias towards younger cohorts, as Prolific samples tend to be younger [45]. In each age group, we also applied a quota for gender to get an even split. For the highest age brackets, we were not able to attain the full target sample size or an even gender split in all countries, as the number of available participants on Prolific for this target group was too small. We redistributed the remaining slots across the different age groups. The final sample consisted of 993 respondents and Table 2 depicts the demographic information.

We decided against screening for smart device ownership, given that the expectations of consumers without smart devices have legal relevance – they might be future users, or have their own particular reasons for not engaging with such products. Thus, we were able to compare expectations and perspectives between experienced and less experienced users of

Table 2: Demographic overview. *Other responses possible were "Non-binary/ Third gender" and "Prefer not to say"

Demographic		FR	DE	PO	ES	NL	Total
Age	18-24	39	41	48	39	43	210
	25-34	41	40	46	40	44	211
	35-44	43	41	43	42	45	214
	45-54	38	40	43	42	41	204
	55-64	25	29	14	33	20	121
	65+	11	9	2	3	8	33
Gender	Female	95	97	93	94	96	475
	Male	98	100	99	100	102	499
	Other response*	4	3	4	5	3	19
		197	200	196	199	201	993

smart devices. We followed methodological literature for comparable experimental designs (i.e., factorial designs and choice experiments) to find sample sizes with sufficient statistical power for our planned device and country comparisons. [4] and [6] suggest a range of at least 5 to 50 observations per vignette as a general guideline for such designs with repeated measures (vignettes) per respondent and deploying multi-level regression for analysis. As we wanted to compare lifetime expectations of a total of 17 different device vignettes within each of the five countries, we aimed at 200 participants per country, as this would provide 35.3 responses on average per device per country, well above the minimum recommendation of five observations.

During data collection, we noticed that many respondents interpreted the survey questions about their own devices (Q2.1 - Q2.8) differently as intended by us, i.e., as asking about the general device category, not the particular device they were using right now (i.e., asking when they started using smartphones *in general*, instead of when they started their *currently used* smartphone). We thus added a clarification to Q2.2 to focus responses on the currently used devices, changed the wording of Q2.2 to Q2.8 accordingly, and then did a follow-up survey only with these specific questions with all respondents participating so far. We contacted them directly via Prolific and paid a higher hourly rate to incentivize participation. In total, 95% (552 of 579) did the survey with only the updated questions again. We conducted consistency checks against original responses and included an attention check. We discarded the responses from the remaining 5% when analyzing responses to Q2.1 to Q2.8, as their question interpretations might have been inconsistent with ours.

3.3 Survey procedure

The survey was advertised on Prolific as “Your use of and perspectives on smart devices” together with a short, high-level description of the task in the respective language. Participants could access the survey after agreeing to the informed consent. The survey was run on Qualtrics

(hosted by the research institution) and structured into four sections, which we describe in the following.

Participants' own smart device usage. To collect concrete, device-level data on respondents' own smart device usage and duration, the survey began with questions about their own devices. The survey started with a general description of smart devices to provide context, especially for respondents without much experience with such devices. Respondents then indicated the types of smart devices they used and owned and which specific devices they currently used, followed up with more targeted questions about these specific devices, including the model/brand, the condition (new / previously owned), the purchase channel, when it was started being used and for how long looking ahead, and the software updates status (Q2.1 - Q2.8). We asked these follow-up questions only for a maximum of three of their devices (chosen randomly) to keep response time manageable. We also asked if respondents had recently stopped using any smart devices to find out more about their use time, device disposal, and the reasons for ending use (Q4 - Q4.4).

Eliciting lifetime expectations via device vignettes. Respondents were presented with vignettes about different devices to move from their own devices' usage to eliciting their expectations regarding stereotypical device categories. We asked them to imagine they would buy such a device today and emphasized our concept of product lifetime (Q5). Then they were presented with one conventional and two smart device vignettes, both selected randomly from the respective list of devices (see Table 1). The first vignette was a non-smart device to set a baseline and avoid ordering effects by first showing smart devices, as this could easily lead to confusing the subsequent conventional device as being smart.

After each device vignette, participants answered the question: *"If you had to predict, for how many years do you expect such a device to last?"* (Q5.1.1) by entering a whole number in years. We opted for an open-ended response format to avoid potential biases introduced by scale anchors (*anchoring effect* [46]). For instance, an upper anchor such as *"More than 10 years"* might implicitly suggest that 10 years is a long lifespan, thereby lowering lifetime estimates [44]. To capture more contextual data for these numerical lifetime estimations, we also followed up with *"What aspects did you take into account when estimating the number of years?"* (Q5.1.2), where respondents could input their reasoning in an open text field.

Software update and security considerations. In this section, we were interested in respondents' understanding of software support and security aspects for smart devices. As previous work implied that consumers did not fully understand the implications of unsupported smart devices [25], we asked how the end of update support would impact smart devices (Q7) and to what extent respondents had first-hand experience with this (Q7.1), followed by their expectations how long software support would last for the two smart devices they saw earlier in the vignettes (Q8) to see how this estimate would compare to the device's lifetime expectation in Q5.1.1. We then explicitly introduced the concept of security for smart devices with a short explanation (Q9) to then measure respondents' security concerns (Q9.1), mitigation actions (Q9.2), and if a continued provision of security updates would lead them to use their smart devices for longer (Q9.3).

Demographics and survey conclusion After filling out some final demographic questions, respondents were thanked, debriefed, and sent back to Prolific with a completion code to receive payment. The survey included two attention checks (Q3 and Q6). The median completion time was 11.83 minutes. The full survey instrument is provided in Appendix A.

3.4 Data analysis

We first checked the data for suspicious responses by reviewing attention checks, completion time, and spurious patterns like providing the same response continuously or nonsensical open text responses. All respondents who failed both attention checks were removed ($n = 5$). 64 respondents failed one of the two, and after manually reviewing their responses, we removed three due to failing at least one of our removal criteria; repeated scale responses, nonsensical text responses, inconsistencies in responses, such as having started using a device model that was not released yet at this time, or rapid completion times. We also checked the responses of the fastest (< 5 minutes) and slowest (> 1 hour) completion times, but did not find any indications of bogus answers (i.e., they passed both attention checks and gave legitimate text responses). Thus, response quality was generally high, as we only had to remove data from eight respondents.

Quantitative analysis To analyze the data, we first calculated descriptive statistics of survey responses to get an indication of patterns and trends as well as inferential statistics to detect statistically significant differences across responses or countries.

To assess which factors influenced respondents' expectations of devices' lifetimes in the vignettes, we ran a multi-level regression model with maximum-likelihood estimation, allowing us to test for significant differences between devices (both smart and conventional) and account for respondent-level characteristics, respondent-level variance, and model fit. Assumption checks for homoscedasticity, multicollinearity, overfitting, and influential datapoints indicated that lifetime expectations were not normally distributed and displayed a skew towards higher values (e.g., 20 years was not an uncommon response). We thus log-transformed the outcome variable *Lifetime*. For better interpretability, we transformed the resulting coefficient estimates to express percentage changes in the outcome variable (by exponentiation with $e^{\beta} - 1$).

After iteratively adding predictors to the model to assess if goodness of fit improved significantly, we concluded with the final model predicting *Lifetime* with *Device* (the different device vignettes), *Device Experience* (if the respondent used the smart device described in the vignette themselves), *Country*, an interaction between *Country* and *Smartness* (if the device was smart or conventional), and a random effect of respondent to account for individual differences between them. The number of smart device categories used, Age, and Gender showed no effect, as including those predictors did not contribute significantly to the model's fit. The model is presented in Table 2 in the Appendix.

Qualitative analysis Open-text answers were translated into English using the translation tool DeepL [13]. In our Ethical Considerations statement, we detail to how we protected respondents' sensitive data. To ensure quality, the native speakers who were also involved in the survey translation checked a random sample of the resulting translations. The automatic translation performed satisfactorily, with no native speaker reporting any translation errors.

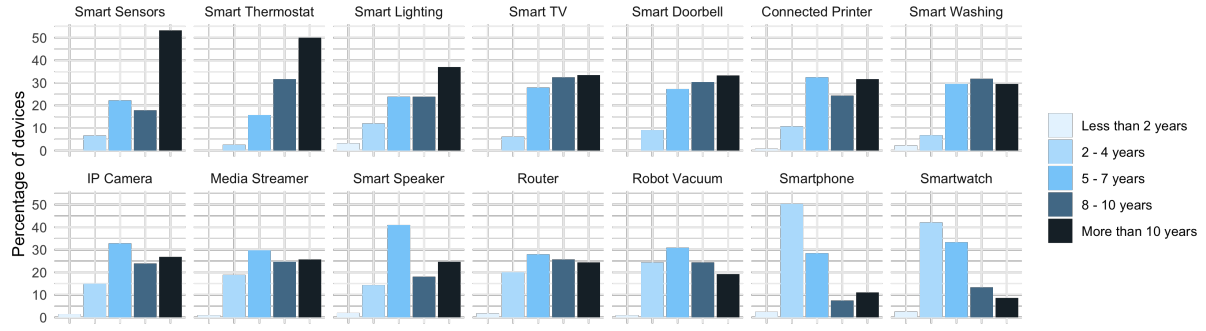


Figure 1: Sum of past use and intended future use duration across respondents’ smart devices ordered by decreasing rate of durations of more than 10 years. Devices with less than 20 observations are not depicted.

Translated text data was then analyzed using thematic analysis [9], where the primary researcher identified and assigned codes to the text answers. After coding a subset of the responses, the resulting initial codebook was discussed at regular intervals with co-authors and refined. After coding approximately one-third of the open text data, we reached theoretical saturation, where no new themes emerged [33], and the codebook was discussed one last time to finalize it. Previous codes were adjusted according to the final codebook, which is provided in Table 4.

4 Results

4.1 Individual use of smart devices

To address RQ (i) (*How do consumers use their smart devices, and for how long?*) and understand what is a reasonable use time for smart devices and how they are used and purchased, we collected data on survey participants’ use of their own smart devices, which resulted in data on 2485 individual IoT devices currently used, and 398 devices used in the past. We also report on relevant country differences throughout this and the following subsections to address Research Question (iv) (*Are there differences among EU member states regarding consumers’ smart device usage, expectations, and security and software support perceptions?*).

4.1.1 Devices currently used

On average, respondents indicated using five different smart device categories, with smartphones being the most common, followed by Smart TVs and Routers. Table 3 provides an overview of devices’ popularity in the sample. Devices’ most popular brands were all from international companies, who will need to comply to the CRA to sell these products in the EU. For some smart devices, especially routers, sensors, doorlocks, doorbells, and solar inverters, a sizable proportion of participants did not know the brand of their currently used device. We added smartphones as an option due to their widespread use and importance in the smart device ecosystem (e.g., due to companion apps).

To assess how long respondents used their devices, we shifted the level of analysis from device categories used to the particular devices participants were currently using. We asked if these

Table 3: Prevalence and brands of smart device categories owned and used by respondents. If fewer than three brands are listed, there are too few observations for a pattern. % *Unk.* is the share of respondents not knowing their device's brand.

Device Category	Number	Most common brands	% Unk.
Smartphone	984	Apple, Samsung, Xiaomi	0%
Smart TV	680	Samsung, LG, Sony	3%
Router	611	Fritzbox, TP-Link, Vodafone	37%
Connected printer	582	HP, Canon, Epson	7%
Smartwatch	503	Apple, Samsung, Xiaomi	5%
Media streaming	290	Google, Amazon, Xiaomi	14%
Smart lighting	281	Philips, Ikea, Xiaomi	27%
Smart speaker	281	Amazon, Google, Apple	4%
Robot vacuum cleaner	264	iRobot, Xiaomi, Roborock	11%
Smart security camera	192	Ring, Xiaomi, TP-Link/tapo	27%
Smart sensors	150	Eufy, Kidde, Philips	59%
Smart thermostat	111	Honeywell, Remeha, Tado	34%
Smart washing mach.	108	Samsung, LG, Beko	9%
Smart doorbell	88	Ring, Eufy	33%
Smart hub	48	Google, Philips	21%
WiFi solar inverter	48	Enphase, Solaredge	39%
Smart fridge	42	LG, Samsung, Bosch	5%
Smart doorlock	15	–	43%
Smart baby monitor	14	–	17%

devices were acquired in new or second-hand condition, as we could not control for the use duration of the previous owner when measuring device use times. This also provided us with valuable insights into the prevalence of the second-hand use of smart devices, as their lifecycle can span different users. The vast majority of smart devices (90%) were reported to have been in new condition, while only 9% were previously owned. The devices with the highest rate of second-hand use were smartphones (16%), smartwatches (11%), and smart TVs (9%). For the devices that were new when usage commenced, the majority were purchased in online stores (60%), while physical stores were less popular yet still a sizable amount (30%), highlighting the importance of considering both online and offline sales channels when disclosing support durations to consumers.

There were significant differences between countries regarding smart device purchase channels. Regarding second hand use ($X^2(4) = 28.39$, $p < 0.001$), the highest prevalence was observed in France with 14% of devices being acquired in used condition and the lowest in Spain (5%). Similarly, France had the highest rate of participants selling their previous devices onward (16%). For devices acquired new, the highest proportion of devices bought online was

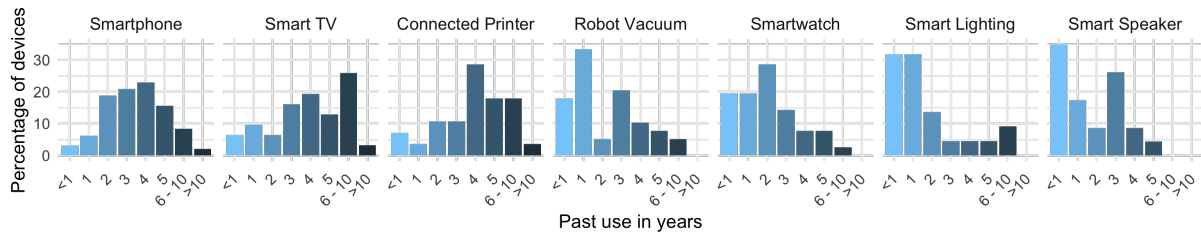


Figure 2: Duration of device usage before stopped being used ordered by increasing rate of durations below 1 year.

in Poland (69%) and The Netherlands (66%), while the countries with the highest rate of devices bought in physical stores were France (37%) and Spain (35%) ($X^2(8) = 33.47, p < 0.001$).

To gauge how long respondents use their current devices, we added the time since they started using them (Q2.2) and for how long they plan to keep using them (Q2.6). We consider this a measure of intended use duration, as it pertains to planned future use, which bears some level of uncertainty. Figure 1 depicts the distributions of past and intended use time across respondents' smart devices. Second-hand devices were not included. Thus, a first differentiation across smart devices in intended use times became evident. Smartwatches and smartphones were clearly skewed towards shorter use times (i.e., mainly in the 2 - 4 years range), while Smart TVs, smart Lighting devices, or smart thermostats showed substantially longer use times on average. Indeed, we found that for the majority of devices except for smartphones and watches, a sizable number of users indicated more than a total of 10 years, indicating long intended use times in terms of smart product standards.

4.1.2 Devices recently stopped to be used

As intended future use can be difficult for individuals to forecast, we also asked respondents about their recently stopped smart devices to assess their recent experience with a device they finished using (Q4.1 - Q4.4), independently whether it was replaced with a newer device or not. In total, respondents reported 398 smart devices they had recently stopped using. The most commonly stopped devices were smartphones ($n = 98$), smartwatches ($n = 81$), and robot vacuum cleaners ($n = 40$). Figure 2 presents the distributions of devices' use times (devices with less than 20 observations are not depicted) and shows that robot vacuum cleaners, smart lighting, smart speakers, and smartwatches were skewed towards shorter use times while smart TVs and printers were often used for longer. Smartphones were approximately normally distributed around a middle point of four years of use.

The most common reasons why respondents quit using their previous devices were wanting a newer device ($n = 97$, 20% of all reasons provided) and experiencing flaws with the old device ($n = 93$, 19%). Reasons implying a more terminal cause for stopping device use were less common, with 57 (12%) instances of devices stopping working altogether, and 34 (8%) in which incompatibility with other devices or services was the reason. The end of update support ($n = 23$, 5%) and privacy ($n = 26$, 5%) and security concerns ($n = 16$, 3%) were the least common reasons to stop device use.

Similar motivations for device replacement also emerged for respondents who indicated that they already planned to only continue using their current devices for less than a year into the future, in Q2.6. When asked about their motivations, the most prominent reasons were

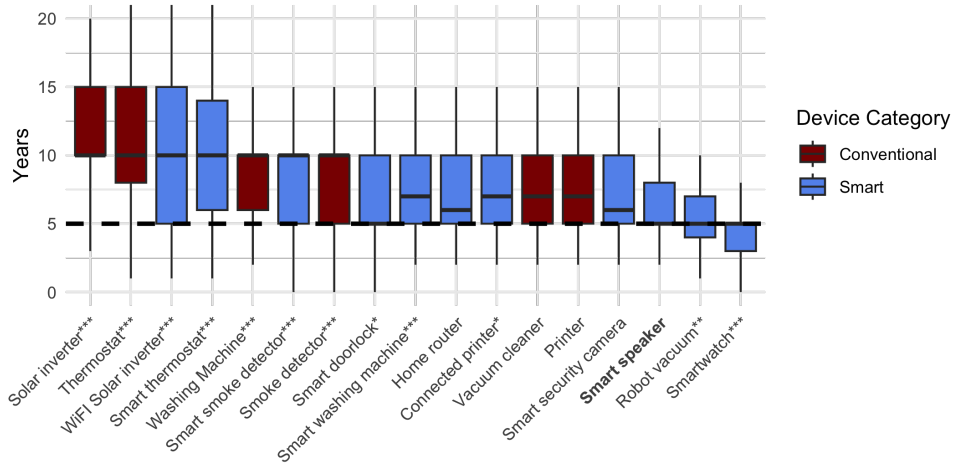


Figure 3: Expected lifetimes for different smart and conventional device categories ordered by mean expected lifetime. Responses were given as whole numbers. The dashed horizontal line denotes the CRA's five-year baseline, and asterisks significant differences to the reference level *Smart speaker*.

experiencing issues and flaws ($n = 62, 34\%$) and desire for a newer device ($n = 48, 27\%$). Only 14 participants indicated the end of update support as a reason, and even fewer were due to security and privacy concerns. Thus, users' preference for better alternatives and experiencing functional issues with the current product were the main drivers to stop using their smart devices, rather than update support or security concerns.

Considering what happened to the 398 discontinued devices, the vast majority of respondents indicated they still have them while not actually using them ($n = 190, 48\%$). Gifting it to others ($n = 54, 14\%$), selling it ($n = 48, 12\%$), or discarding it ($n = 33, 8\%$) were substantially less likely responses, implying that handing devices on (i.e., gifting or selling it) and subsequent re-use were not common while the vast majority of devices appear to remain with their owner's without being used.

4.2 Lifetime expectations of smart devices

4.2.1 Device level differences

As a respondent's use time of their own device does not necessarily correspond to its expected lifetime (e.g., they could opt to replace and sell it after a short while), we pivot to what respondents expected for how long different device types would generally last for whoever was using them by presenting vignettes of these products. To answer RQ (ii) (*How long do consumers expect different smart device categories to last, and which factors influence these expectations?*) we aimed at learning for how many years participants predicted a range of different smart and conventional device types would last, as elaborated in Section 3.1.1. We supplement these results with qualitative commentary given by respondents when asked what they took into account when estimating devices' lifespans. Table 3 provides the five most commonly mentioned factors per device type taken into account.

Figure 3 presents the expected lifetimes provided for different smart and conventional device categories. The highest expected lifetimes had solar inverters (Conventional: $M = 12.65$ years, $SD = 6.60$, Smart: $M = 10.75$ years, $SD = 6.81$) and thermostats (Conventional: $M = 11.37$ years, $SD = 5.68$, Smart: $M = 10.35$ years, $SD = 6.29$). For solar inverters, respondents commonly considered their use case and high expected price as factors (e.g., *"It is an expensive product and should last according to its cost."* PID678), and for thermostats their usage or perceived lower complexity (e.g., *"That it is a simple device"* PID685), as seen in Table 3.

Devices with the lowest expected lifetimes were consistently smart. The lowest lifespans were expected for smartwatches ($M = 4.84$ years, $SD = 1.96$) and robot vacuum cleaners ($M = 5.74$ years, $SD = 2.51$). For both, their continuous use was commonly considered (e.g., a robot vacuum cleaning the floor regularly, a smartwatch worn continuously), while for robot vacuums, environmental factors like animal hair often came up. For smartwatches, however, factors more related to smart device market dynamics were mostly considered: fast innovation cycles, software updates, degrading batteries, and planned obsolescence (e.g., *"Technology changes so fast, it is likely to be obsolete in 5 years"*, PID80). Expectations also generally showed less variability for these devices, as evidenced by lower standard deviations and error bars in Figure 3, indicating that expectations reached a stronger consensus among respondents for those products. This was likely due to respondents' more common experience with smartwatches and robot vacuums than for solar inverters and thermostats, as evidenced in their respective prevalence of use (Table 3).

The multi-level regression analysis (Table 2) revealed that differences in expected lifetimes across devices were statistically significant. Taking smart speakers as the reference level (due to their central role in many smart home set-ups and their "important" categorization in the CRA), we found the largest differences to conventional solar inverters (expected to last 56.90% longer) and thermostats (52.70% longer), but also significant differences to other smart devices such as smart washing machines (expected to last 23.20% longer) or smartwatches (expected to last 22.10% shorter). Significant differences thus correspond to the visual trend in Figure 3, where also significant differences are highlighted.

We also found that smart devices had a consistently shorter expected lifetime than their conventional counterparts when considered as a factor. Most smart devices (except for smoke detectors and printers, with a marginal difference) had a lower average reported lifetime, an effect that was statistically significant (-17.1% , $t(2972) = -9.82$, $p < 0.001$). We identified several drivers for this, such as the added complexity of smart features (*"Adding [smart] functions risks making them even more susceptible to problems."* PID564), software updates, or potential incompatibility, but also some more complex dependencies were taken into account, like *"The company selling this machine will go bankrupt, and we won't be able to install the application on updated OS versions."* (PID21).

As can also be derived from Table 3, devices' *Usage* and *Device type* were generally among the most common factors considered by participants when estimating lifespans across all devices. While static device qualities such as the type of device (*"Washing machines last a long time"*) can be seen as more straightforward heuristic for the lifespan, usage (*"How often the washing machine runs"*) is less deterministic, as this depends on wear and tear of components, how frequently and intensively the user decides to use the device, and if it is used as intended or not.

4.2.2 Individual differences

Lifetime expectations were also strongly affected by respondent-level factors besides device-related aspects. The regression model fit coefficients provided in Table 2 suggest that when accounting for respondent-level variation, the model fit (Conditional R^2 : 46.40%) increased substantially in contrast to only considering the device, country, or own experience with the device (Marginal R^2 : 16.60%). This highlights the substantial impact of individual differences and the subjective nature of lifespan expectations for products. Some respondents consistently expected longer lifespans across devices, while others had a tendency to expect shorter lifespans, indicating systematic variation in personal perceptions.

Also personal experience with the smart device affected expectations - Respondents who used the same device type themselves as described in the vignette at hand expected longer lifespans on average than participants who did not (8.0% longer, $p < 0.01$), possibly due to familiarity with the device or increased optimism due to personal investment in it. However, we found no effect of experience with smart devices in general (i.e., the number of smart device types the participant was using), implying that the user's experience with the same device category was a stronger predictor for expected lifetimes.

We also found significant differences between countries in how long respondents expected devices to last. Taking Spain as the reference, respondents in Poland generally expected devices to last significantly shorter (14.1% less, $p < 0.001$), while participants in The Netherlands and Germany had more optimistic expectations (9.2% and 8.6% longer, respectively). However, an interaction between country and the smartness of the product indicated that in these two countries, respondents expected smart devices to last significantly shorter than conventional devices compared to Poland (Germany: 8.5% shorter, The Netherlands: 12.2% shorter). Thus, participants in Germany and The Netherlands were comparatively more skeptical about the lifespan of smart devices. Age and Gender had no effect on expected lifetime.

4.3 Perceptions of software updates and security over devices' lifetime

As the previous analyses focus on smart devices' use times and expected lifetimes to measure what constitutes a reasonable lifetime, we now focus specifically on the role of software updates and security aspects over devices' lifespan to answer RQ: (iii) *How do consumers perceive security and software update support over smart devices' lifespans?*

4.3.1 Update expectations and experiences

In contrast to the static nature of most conventional, non-smart devices, smart devices can be under continuous modification due to software updates. We were thus interested in understanding how consumers perceived update-induced changes to devices over their lifespan and how their subsequent end would affect the user's experience with the product.

More than half of respondents ($n = 533$, 54%,) expected the software update support to correspond with the device's full lifespan, as they provided the same value for both (Q5.1.1 and Q8). When directly asked for their expectations on how the end of update support would impact smart devices' use, no new features ($n = 853$, 86% of participants) and incompatibility with other devices and services ($n = 752$, 76%) were the most commonly expected changes, while almost no participant expected no changes (Figure 4). Interestingly, both security-related

answer options (no more fixes to vulnerabilities and no more risk monitoring for the device) were also commonly expected ($n = 714$ and $n = 705$, respectively), despite the survey not mentioning security or privacy up to this point and answer order randomization. Thus, approximately 70% of the respondents were indeed aware of the security implications that the end of update support brings with it.

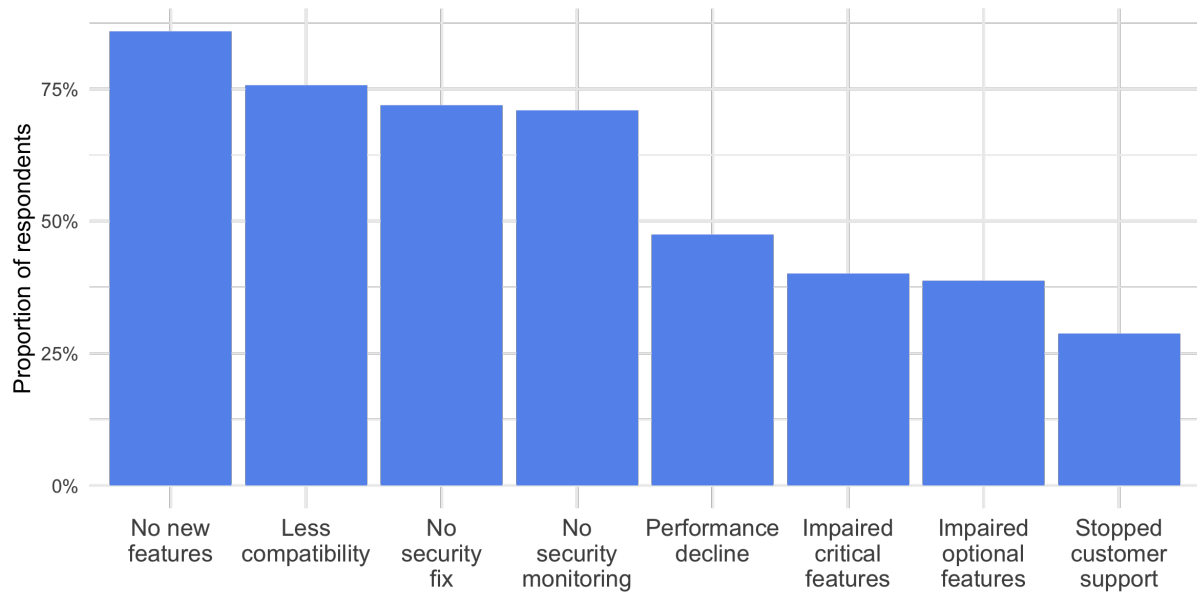


Figure 4: Changes to smart devices after software support ends as expected by respondents (in %). The order of the options was randomized. Multiple choices were possible. The responses “I don’t expect any changes”, “Not sure”, and “Other” were below 1% and omitted from this plot.

To check respondents’ own experiences with end-of-support-induced changes, we also asked if they had experienced their previously provided expected changes with their own devices. Figure 5 shows that no new features, a declining device performance, and less compatibility with other devices and services had the highest proportion of respondents experiencing this. We also saw the potential role of ended support for product obsolescence: Among the participants who expected critical features to stop working at this point, around half actually experienced this, so their devices’ functionality was essentially made obsolete after not receiving updates.

While such functional impacts on the device were thus quite apparent, security-related changes were more subtle and imperceptible for users. Both security-related answer options (no more fixes to vulnerabilities and No more risk monitoring for the device) had the highest rates of respondents indicating not experiencing them or not being sure, while they both were frequently expected as a common change after the end of support (see Figure 4), highlighting how opaque security (and its absence) can be for smart device users.

Related to this imperceptibility of updates, Figure 6 shows substantial differences in the current update support status across the smart devices used by respondents. For smartphones, the vast majority indicated the device to still be receiving updates, while for many other smart devices a substantial proportion of participants reported not knowing if it still was. For instance, for smart sensors and lighting products, at least half of respondents indicated they did not

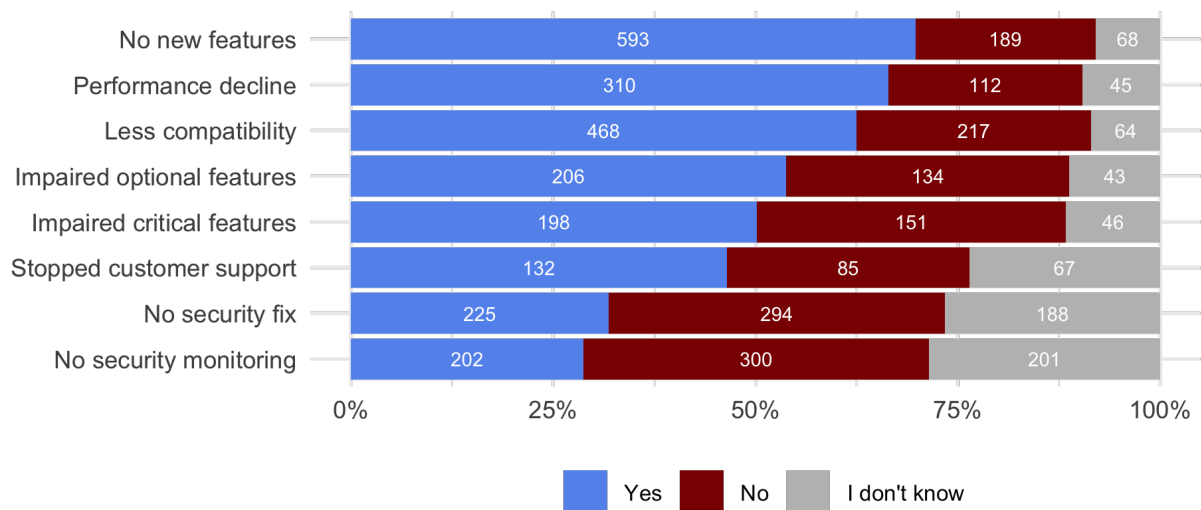


Figure 5: Respondents’ own experiences with changes to their devices after the end of update support. They were asked: “Did you experience any of these changes with your devices yourself?”

know if the device still received updates. Indeed, this uncertainty of the device’s update status was much more prevalent than unsupported devices still being used (with robot vacuum cleaners having the highest proportion of unsupported devices). Thus, while the majority of respondents’ smart devices were reported to still be supported, it also illustrates the challenge for users to actually *know* whether their smart devices still receive updates, especially for devices with limited user interfaces like sensors, lighting, doorbells, or routers.

4.3.2 Security and Privacy perceptions and behaviors

As a majority of respondents were aware of the security implications of the end of support, although often imperceptible, we now focus on their security and privacy-related perceptions towards smart devices.

Figure 1 suggests that when prompted for security-related concerns about their own smart devices, respondents mostly indicated to be concerned about their personal data (“My personal data being accessed by unauthorized individuals” = 57% of respondents, “More personal data collected from the device than I expect” = 56%, “My personal data being shared with third parties by the manufacturer without my consent.” = 52%). Two of these were actually privacy-related concerns, with the device’s vendor as the “perpetrator”. The device being directly attacked and leveraged maliciously was also a common concern (50%), while the device being damaged by an attack (30%) or insufficient customer support in case of an attack (23%) were expected less often. Not being concerned was the least selected response (15%).

To address such concerns, respondents indicated to apply varying mitigation actions, as depicted in Figure 2. The importance of updates became evident, as installing the latest software update was the most prominent mitigation behavior and reported by 56% of respondents ($n = 552$). Stopping to use the device altogether after software support ends was the least common behavior ($n = 121$), yet still selected by approximately 12% respondents.

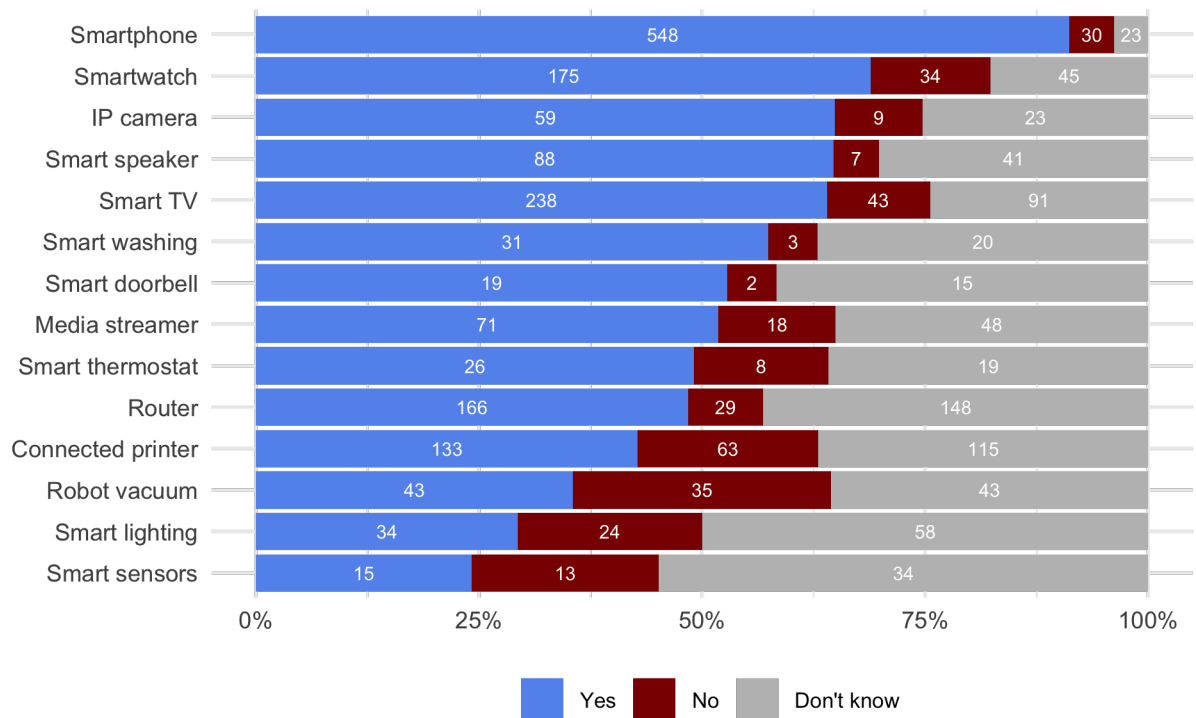


Figure 6: Responses to the question: “Does the particular device you are currently using still receive software updates, as far as you know?” Devices with less than 20 observations were not included.

This was in line with our previous finding that the end of software support or concerns about privacy or security were not prominent reasons to stop using a device.

When asked if respondents would use their smart devices for longer if they continued to receive *security* updates (Q9.3), the vast majority strongly agreed or agreed (78%). This seemed to be a contradiction at first, as the end of update support was not a common reason for respondents to stop using their devices nor a trigger to stop using the device to address security concerns. We interpret this finding such that as longer patching support will give reassurance to users that they can safely *continue* using their devices if they want to, its end was not a strong enough trigger for users to *quit* using them. We also note the importance of the device’s brand and its associated trustworthiness for respondents to avoid security risks (53%, $n = 528$).

We also found significant country differences in how participants reported to address their concerns ($X^2(24) = 38.03, p < 0.05$). Installing the latest updates was reported the most common mitigation in the Netherlands (24%) and Germany (23%), but less so in Poland (19%), where, as well as in Spain, being cautious about how using the device and choosing trustworthy brands were more popular.

5 Discussion

In this survey study ($n = 993$), we empirically explored consumers’ usage and expectations of smart devices and their lifespans in the EU, to address the uncertainty around the abstract

legal concept of reasonable user expectations. The Cyber Resilience Act [50] aims at converging security support duration with smart device lifetimes, and requires manufacturers to consider reasonable user expectations when defining this period – a policy with global ramifications for the smart device market. For instance, practically all brands of respondents’ smart devices were from large, globally active manufacturers, who will have to comply and could thus also uphold support in other markets.

5.1 Device lifetimes

We found that all smart devices included in this survey (except smartwatches) were on average expected to last longer than the CRA’s minimum support period of five years, despite many participants considering factors artificially reducing product lifetime, such as a premature replacement for newer alternatives or planned obsolescence. Smart products were also commonly used by respondents for a period longer than this, with use times well above 10 years common for some devices. Surprisingly, a majority (54%) of participants actually expected the update support period to correspond to the smart device’s full lifetime, which contrasts with current practices in the smart device market [18, 43, 40], but highlights the importance of aligning support periods to be closer to device lifetime to meet expectations.

Previous work found that device re-use is a common practice, with the first owners often gifting or selling their devices onwards [30, 26]. We found this was present but not substantial in our sample. 9% of respondents’ own devices were second-hand, and selling or gifting a previously used device was by far not as common as retiring it at home without using it. Still, second-hand use or repair [51, 10] are conceivable practices, perhaps due to economic reasons (e.g., for low-income users [28]) or sustainability considerations, increasing device use times. It is unclear to what degree second-hand use and repairability will be factored in when manufacturers, market surveillance authorities, or courts determine expected use time and support period.

5.2 Software Updates and Security over devices’ lifespan

“Smart” factors such as software updates, incompatibility, or added complexity led to smart devices being expected to have shorter lifetimes than conventional products (Section 4.2.1). However, the central role of software updates for security was often seen. In contrast to a commonly reported unawareness or uncertainty of updates among users in previous research [25, 22, 17, 11], we found that respondents generally exhibited awareness of updates’ security implications. 70% expected no more security reassurances after update support ended, and installing the latest updates was reported as the most common mitigation to address security concerns. As there are some differences in our study’s demographics in contrast to this previous work, with participants in [25, 22] being US-based smart home users with limited security experience, [17] studying young users of widely used software, and [11] practitioners at UK router vendors indirectly describing their users, it raises the question if this effect was due to differences in samples and or if this awareness might actually be increasing over time.

However, while an association between end of update support and security implications was arguably observable in our study, security concerns were weak triggers for respondents to stop using a device. More attractive alternatives or declining functional performance were the prevalent drivers. This was likely amplified by the imperceptibility of updates and security measures. For many of their own devices, respondents did not know if the device was still supported, or did not experience or know about security support stopping.

Thus, a key challenge with prolonged support duration is ensuring visibility to users. Currently, indicators of software versioning and update status are often unclear or inconsistent across smart devices (as observed in our work and in, e.g., [22, 25, 24]), which often lack a user interface. It is challenging for users to verify if a manufacturer is maintaining security updates as promised, potentially leading to a form of learned helplessness akin to delegation of security responsibilities [14], where users must rely on manufacturers' assurances without a straightforward means of verification for themselves. While the CRA sets requirements on update delivery and notifications (to be automatic by default, with notification channels to users available, e.g., to opt-out), it remains an open question through which mechanisms - if any - users can actively engage and hold manufacturers accountable for ongoing security support, comparable to other regulatory frameworks such as GDPR [48], where subject access requests can be submitted to obtain data about themselves.

As the CRA is still in a nascent stage, guidance about support periods will be crucial in the coming years before the market converges on expected support times for "products with digital elements" in all their forms. Guidance will reduce uncertainty and avoid courts having to eventually make the case for what constitutes a reasonable use time and which elements of a product determine this. Our work contributes to this ongoing conversation by empirically assessing device use times and expected lifetimes for a range of different smart product categories and what factors consumers take into account, as information valuable for manufacturers, market authorities, and the EU administrative cooperation group (ADCO), who will publish guidance on support times in the coming years.

5.3 Recommendations

Here we discuss initial recommendations emerging from our work.

Manufacturers: For manufacturers, users' expectations take center stage in product conformity with the CRA; manufacturers will now need to document how they consider these expectations when determining support periods.

Going beyond device-internal usage data. Our work demonstrates that for a meaningful understanding of users' expectations, getting in contact with them is essential, as relying exclusively on internal device usage data (i.e., device logs how long it is used) might be insufficient to account for expectations, as other contributing factors emerged from our data. For instance, respondents differentiated between smart and non-smart products and considered factors such as the device's price, perceived quality, or environmental factors of usage. Also, the duration how long device data can be collected is arguably determined by the manufacturer, not by expectations. We thus recommend that manufacturers leverage sales channels as well as market and user research capabilities to learn about and document their customers' lifetime expectations for the respective product categories. As our data exhibited substantial individual and country differences, we advise applying a sampling strategy that considers countries, user demographics, and sufficient sample sizes.

Reducing user uncertainty. Furthermore, our results suggest that ongoing security support for smart devices is often indistinct to users, as evidenced by high proportions of users not being sure about the update status of their own devices (Figure 6) and experiencing uncertainty with respect to the end of update support (Figure 5). Thus, tangible factors demonstrating competence to provide support should be made salient by manufacturers at the time of device

adoption and over the device's lifetime, possibly woven into marketing, product disclosure, and easy-to-access support status indications of the product (e.g., via a companion app). As we also found that choosing trusted brands was a major way for respondents to navigate security concerns (Figure 2) and a clear preference for longer support periods (as also suggested by previous work [15, 34, 36]), a stance of active security support has marketing and brand-building potential.

Policymakers and market surveillance: Approaching consumer expectations. Market surveillance authorities in EU member states should note that expected lifetimes and actual use times of consumer smart devices were commonly found to be higher than the CRA's baseline of five years (Figure 1, 2 and 3). The EU administrative authorities (ADCO) can publish guidance on reasonable support durations for different product categories, or, if "data suggests inadequate support periods for specific categories of products" (Article 52(16) & Recital 62) issue recommendations to market surveillance authorities to focus on those products or to the EU Commission to delegate acts and define minimum support durations. Our data should thus be considered as a first indication that several smart product categories considered in this study require delineation from the baseline of five years as suggested in the CRA. Additionally, they should be aware of a potentially self-defeating dynamic for consumers regarding expected smart device lifetimes: Smart versions of a product category were expected to last shorter on average than conventional counterparts, and participants considered factors they are accustomed to from the current smart device market; quick replacement, emerging incompatibility with other products, or planned obsolescence. As these are factors artificially reducing use times and thus not justifying a product's definite end of life (and smart devices being repaired, resold, and reused, as we also found in our study), policymakers and market authorities should be cautious to consider such dynamics when user expectations are measured or defined.

Providing assurances to users. The CRA's support duration provisions will likely lead to longer support with security updates to smart devices, exposing them to continuous modification. We found that participants experienced phenomena with their devices over their use time that may or may not relate to (the end of) security updates, like declining performance, less compatibility, impaired features, or simply being unsure (Figure 5). Thus, policymakers and market authorities should consider defining assurances for users over the devices' lifetime that manufacturers should provide. This could include explicitly calling out potential "side effects" how the update could affect the device's behavior via notifications accompanying updates. As the CRA also requires security updates to be published separately from functionality updates where technically feasible (Annex I, Part II (2)), we recommend market authorities to explicitly consider this legal instrument to reduce such in-transparency for users.

5.4 Limitations

A survey relies on self-reporting, and for some responses, such as whether longer security support leads to prolonged device use, it remains uncertain if this translates to actual behavior. Additionally, the survey topic and some questions were complex. For example, recalling the year a device was first used or whether it still receives updates could be difficult for respondents. We did not filter for smart device ownership, and while most respondents used at least one device, concepts like smartness, updates, and security could be challenging. To

mitigate this, we used simple language, refined the survey through iterations, conducted a pilot study, and provided definitions and “I don’t know” options.

Sampling and generalizability are further limitations. Our sample is not representative of the general EU population or the included countries, and we only studied a subset of product categories falling under the CRA. As a common limitation in such online surveys, participants on Prolific tend to be younger and more technologically knowledgeable than the general population [45], leading to an underrepresentation in our study of those over the age of 55, despite aiming for a balance across age groups and genders. However, even with a sample of participants with an arguably higher technological literacy, we observed high levels of uncertainty towards participants’ awareness of their devices’ support (e.g., Figure 6). Resource constraints also limited our survey delivery to a subset of five member states (with Section 3 explaining our rationale). We thus invite future work to extend our methodology to other countries and products with digital elements, as the CRA will apply to a plethora of products, not just consumer smart devices.

Lastly, many factors can influence a device’s expected lifespan, including usage, environment, quality, and price. Our vignettes focused only on device type, exploring additional factors through qualitative responses. Future work could adopt more complex vignette designs incorporating variables such as brand, price, and usage.

6 Conclusion

The upcoming Cyber Resilience Act will increase the responsibilities of manufacturers of smart consumer devices and market surveillance authorities in the EU to determine and uphold the update support periods of smart products. In contrast to other legislation, where disclosure on support periods via product labels is prominent [1, 47], the CRA will require manufacturers to actually uphold a certain support period. In contrast to the previous status quo, this will involve considering users, as reasonable user expectations regarding the product’s lifetime will have to be considered when determining the support period.

In this work, we empirically assess user expectations and behaviors regarding smart devices’ lifetimes, support durations, and security considerations to provide insights into this abstract legal notion. We find that expectations vary for different (smart) device categories, with smart devices generally being expected to last shorter than their conventional counterparts. We also find that a prolonged support duration harmonizes with users’ expectations.

Ethical Considerations

This research adheres to the principles of "*Beneficence*", "*Respect for Persons*", "*Justice*", and "*Respect for Law and Public Interest*" as in the Menlo report [27].

Beneficence: To appropriately balance probable harm and the likelihood of enhanced welfare resulting from our research, we carefully considered the related EU legal system and how our research could have an effect on the rights of consumers of smart devices. We see the possibility for societal benefits in our work, as our empirical analysis provides users a voice in ongoing and future discussions on support durations, and could also be considered by market authorities and manufacturers to define *longer* security support, as we also directly consider second-hand use and repairability. For this reason, we state that our results pose a conservative estimate, which could be increased.

Respect for persons: As our research involved human subjects, we deployed several safeguards to respect their rights. Before conducting the survey, we obtained approval from our Institutional Review Board (IRB), which also required a data management plan to detail how data was collected, stored, and used. The application to the IRB also included a comprehensive checklist for human subject research, where possible harms and risks had to be explicitly identified and mitigated. These documents for the IRB application were reviewed and approved by a data protection steward and the IRB.

To ensure informed consent, participants had to read and accept the IRB-approved consent form before starting the survey. This outlined survey purpose, estimated duration, data usage and storage, voluntary participation with the option to withdraw (resulting in data exclusion), and the collection of non-identifiable demographic information (e.g., age ranges, as optional responses). Data was stored on an encrypted institutional network, accessible only to the research team. Researcher contact details were provided for any inquiries.

We only used mild deception, as we did not immediately disclose to participants that the survey was also about security aspects of smart devices. This was so as not to bias their responses, and we gave a full disclosure at the end of the survey, to serve as a debrief. This is the typical extent of deception for human-subjects studies.

To protect respondents' right to privacy, we did not collect any PII in the survey explicitly. However, despite our best efforts, open-text responses can constitute indirect identifiers in combination with other data, for instance specific device models or store names. We then erred toward privacy preservation and do not share raw data. To translate open-text survey responses (to Q5.1.2 and Q8.1) with DeepL, we used an advanced membership, which included using TLS encrypted connection during storage and transfer to servers based in the EU and immediate deletion of any text after translation. DeepL is a Germany-based company adhering to GDPR and is ISO 27001 certified. Furthermore, as open-text responses were translated in isolation (i.e., not in combination with any other survey responses), an identification of any participant's identity would not be possible.

To pay respondents fairly for their time and effort, we paid them an hourly rate according to the minimum wage in the research institution's country. In the pilot study, we paid for 25 minutes; in the final survey, for 18 minutes; and in the short follow-up survey with updated Q2 – Q2.8, for 4 minutes. We took generous estimates on completion time. The median of the final survey was 11 minutes (3rd quartile: 16 minutes) instead of 18. Thus, we effectively paid the vast majority of participants more than minimum wage.

Justice: We aimed at fairly distributing risks and benefits across stakeholders by including recommendations for both manufacturers and policymakers, as well as including consumers as participants to give them an active voice in the ongoing and future conversations around support periods.

Respect for Law and Public Interest: In public interest, we did not want our results to give an argument to reduce device lifetimes artificially to comply with the CRA. For instance, as we found smartwatches were expected to have short lifetimes (shaped by current and unsustainable market practices), we did not want to provide an argument for vendors to reduce smartwatches' lifetime or keep them low. To address this, we reiterate that we only provide a starting point for manufacturers and market surveillance authorities on how to conceptualize user expectations via empirical insights for consideration when determining the support period. Only the courts can interpret the CRA and determine what constitutes a reasonable support period for a given product. We also explicitly stress that factors such as fast replacement or planned obsolescence are not valid factors to consider when determining the support period, and that most participants considered the device type and its usage instead, as also defined in the CRA as critical criteria. Further, we emphasize the preference of users for longer support times and the heightened transparency via the CRA and other labeling policies, thus highlighting the "costs" for manufacturers' reputations when keeping support times short.

Open Science

For other researchers to replicate or build on our work, we explain our methodology in Section 3, provide the survey instrument and vignettes in A, and the resulting codes from open-text responses in 4. We will share survey results in aggregated form across categories and dimensions such as device types, countries, or multiple choice responses, (thereby also including the source data for most of the plots). As explained in respecting respondents' privacy, based on our data protection steward's advice, we opted to take a more conservative stance to preserve privacy due to open text responses and potential indirect identifiers in them when applying for IRB approval.

Acknowledgments

This work has been partially supported by the INTERSCT project, Grant No. NWA.1160.18.301, funded by Netherlands Organisation for Scientific Research (NWO). The findings reported herein are solely responsibility of the authors.

References

- [1] Federal Communications Commission (FCC). *U.S. Cyber Trust Mark*. 2024. URL: <https://www.fcc.gov/CyberTrustMark#:~:text=The%20program%20applies%20to%20consumer,door%20openers%2C%20and%20baby%20monitors..>
- [2] Noura Abdi et al. "Privacy norms for smart home personal assistants". In: *Proceedings of the 2021 CHI conference on human factors in computing systems*. 2021, pp. 1–14.
- [3] Noah Apthorpe et al. "Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity". en. In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2.2 (2018), pp. 1–23. ISSN: 2474-9567. DOI: 10.1145/3214262.
- [4] Katrin Auspurg and Thomas Hinz. *Factorial survey experiments*. Vol. 175. Sage Publications, 2014. ISBN: 1-4833-1289-5.
- [5] Paritosh Bahirat et al. "Overlooking Context: How do Defaults and Framing Reduce Deliberation in Smart Home Privacy Decision-Making?" en. In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, 2021, pp. 1–18. ISBN: 978-1-4503-8096-6. DOI: 10.1145/3411764.3445672.
- [6] Jeff Bennett and Vic Adamowicz. "Some fundamentals of environmental choice modelling". In: *The choice modelling approach to environmental valuation* (2001), pp. 37–69.
- [7] Anu Bradford. *The Brussels Effect: How the European Union Rules the World*. Oxford University Press, 2020.
- [8] Conner Bradley and David Barrera. "Escaping Vendor Mortality: A New Paradigm for Extending IoT Device Longevity". In: *Proceedings of the 2023 New Security Paradigms Workshop*. NSPW '23. New York, NY, USA: Association for Computing Machinery, Dec. 2023, pp. 1–16. ISBN: 9798400716201. DOI: 10.1145/3633500.3633501. URL: <https://dl.acm.org/doi/10.1145/3633500.3633501> (visited on 09/12/2024).
- [9] Virginia Braun and Victoria Clarke. "One size fits all? What counts as quality practice in (reflexive) thematic analysis?" In: *Qualitative research in psychology* 18.3 (2021), pp. 328–352.
- [10] Jason Ceci, Jonah Stegman, and Hassan Khan. "No privacy in the electronics repair industry". In: *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2023, pp. 3347–3364.
- [11] G. Chalhoub and A. Martin. "But is it exploitable? Exploring how Router Vendors Manage and Patch Security Vulnerabilities in Consumer-Grade Routers". English. In: *European Symposium on Usable Security (EuroUSEC 2023)* (2023), pp. 277–295.
- [12] Jayne Cox et al. "Consumer understanding of product lifetimes". In: *Resources, Conservation and Recycling* 79 (2013), pp. 21–29.
- [13] *DeepL translator*. URL: <https://www.deepl.com/en/translator>.
- [14] Paul Dourish et al. "Security in the wild: user strategies for managing security as an everyday, practical problem". In: *Personal and Ubiquitous Computing* 8 (2004), pp. 391–401.

- [15] Pardis Emami-Naeini et al. "Exploring How Privacy and Security Factor into IoT Device Purchase Behavior". en. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 2019, pp. 1–12. ISBN: 978-1-4503-5970-2. DOI: 10.1145/3290605.3300764.
- [16] Pardis Emami-Naeini et al. "Ask the Experts: What Should Be on an IoT Privacy and Security Label?" In: *2020 IEEE Symposium on Security and Privacy (SP)*. 2020, pp. 447–464. DOI: 10.1109/SP40000.2020.00043.
- [17] Michael Fagan, Mohammad Maifi Hasan Khan, and Ross Buck. "A study of users' experiences and beliefs about software update messages". In: *Computers in Human Behavior* 51 (Oct. 2015), pp. 504–519. ISSN: 0747-5632. DOI: 10.1016/j.chb.2015.04.075. URL: <https://www.sciencedirect.com/science/article/pii/S0747563215003854> (visited on 01/21/2025).
- [18] Federal Trade Commission. *Smart Device Makers' Failure to Provide Updates May Leave You Smarting*. 2024. URL: <https://www.ftc.gov/reports/smart-device-makers-failure-provide-updates-may-leave-you-smarting>.
- [19] Alex Gnanapragasam et al. "Consumer expectations of product lifetimes around the world: a review of global research findings and methods". In: *PLATE: Product Lifetimes And The Environment* (2017), pp. 464–469.
- [20] Alex Gnanapragasam et al. "Consumer perspectives on longevity and reliability: a national study of purchasing factors across eighteen product categories". In: *Procedia Cirp* 69 (2018), pp. 910–915.
- [21] Julie Haney, Yasemin Acar, and Susanne Furman. "'It's the Company, the Government, You and I': User Perceptions of Responsibility for Smart Home Privacy and Security". In: *30th USENIX Security Symposium (USENIX Security 21)*. 2021, pp. 411–428.
- [22] Julie Haney and Susanne Furman. "User Perceptions and Experiences with Smart Home Updates". English. In: IEEE Computer Society, Dec. 2022, pp. 782–799. ISBN: 978-1-66549-336-9. DOI: 10.1109/SP46215.2023.00045. URL: <https://www.computer.org/csdl/proceedings-sp/2023/933600a782/1Js0Dlv3Xpe> (visited on 01/12/2023).
- [23] Julie M Haney and Susanne M Furman. "Work in progress: Towards usable updates for smart home devices". In: *International Workshop on Socio-Technical Aspects in Security and Trust*. Springer. 2020, pp. 107–117.
- [24] Julie M. Haney and Susanne M. Furman. "Work in Progress: Towards Usable Updates for Smart Home Devices". en. In: *Socio-Technical Aspects in Security and Trust*. Ed. by Thomas Groß and Luca Viganò. Cham: Springer International Publishing, 2021, pp. 107–117. ISBN: 978-3-030-79318-0. DOI: 10.1007/978-3-030-79318-0_6.
- [25] Julie M. Haney and Susanne M. Furman. "Smart Home Device Loss of Support: Consumer Perspectives and Preferences". In: *HCI for Cybersecurity, Privacy and Trust: 5th International Conference, HCI-CPT 2023, Held as Part of the 25th HCI International Conference, HCII 2023, Copenhagen, Denmark, July 23–28, 2023, Proceedings*. Berlin, Heidelberg: Springer-Verlag, July 2023, pp. 492–510. ISBN: 978-3-031-35821-0. DOI: 10.1007/978-3-031-35822-7_32. URL: https://doi.org/10.1007/978-3-031-35822-7_32 (visited on 10/31/2023).

- [26] harris interactive. *Consumer Internet of Things Security Labelling Survey Research Findings*. 2019. URL: https://assets.publishing.service.gov.uk/media/5ff713bfe90e0763a31280a1/Harris_Interactive_Consumer_IoT_Security_Labelling_Survey_Report_V2.pdf.
- [27] Erin Kenneally and David Dittrich. *The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research*. en. SSRN Scholarly Paper. Rochester, NY, Aug. 2012. DOI: 10.2139/ssrn.2445102. URL: <https://papers.ssrn.com/abstract=2445102> (visited on 01/22/2025).
- [28] Anastassija Kostan et al. "Exploring digital security and privacy in relative poverty in Germany through qualitative interviews". In: *33rd USENIX Security Symposium (USENIX Security 24)*. 2024, pp. 2029–2046.
- [29] Lorenz Kustosch et al. "Measuring Up to (Reasonable) Consumer Expectations: Providing an Empirical Basis for Holding IoT Manufacturers Legally Responsible". In: *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, CA: USENIX Association, Aug. 2023, pp. 1487–1504. ISBN: 978-1-939133-37-3. URL: <https://www.usenix.org/conference/usenixsecurity23/presentation/kustosch>.
- [30] Peiyu Liu et al. "How IoT Re-using Threatens Your Sensitive Data: Exploring the User-Data Disposal in Used IoT Devices". In: *2023 IEEE Symposium on Security and Privacy (SP)*. ISSN: 2375-1207. May 2023, pp. 3365–3381. DOI: 10.1109/SP46215.2023.10179294. URL: https://ieeexplore.ieee.org/abstract/document/10179294?casa_token=T6tqj4aLNdgAAAAA:gNWxmBMwzQVvsrwrp7eGnVvFRvWNjCCFe68kBXHxtRq-2j2bYnyKwDYKlJPovvmIKu_lsZ4 (visited on 04/05/2024).
- [31] René Mahieu et al. "Measuring the Brussels Effect through Access Requests: Has the European General Data Protection Regulation Influenced the Data Protection Rights of Canadian Citizens?" In: *Journal of Information Policy* 11 (Dec. 2021), pp. 301–349. ISSN: 2381-5892. DOI: 10.5325/jinfopoli.11.2021.0301. URL: <https://doi.org/10.5325/jinfopoli.11.2021.0301>.
- [32] Megan Crouse. *WUS to Launch Cyber Trust Mark to Label Secure Smart Devices*. 2025. URL: <https://www.techrepublic.com/article/us-cyber-trust-mark-iot-security/>.
- [33] Sharan B. Merriam and Elizabeth J. Tisdell. *Qualitative Research: A Guide to Design and Implementation*. en. Google-Books-ID: JFN_BwAAQBAJ. John Wiley & Sons, Aug. 2015. ISBN: 978-1-119-00361-8.
- [34] Philipp Morgner et al. "Security Update Labels: Establishing Economic Incentives for Security Patching of IoT Consumer Products". In: *2020 IEEE Symposium on Security and Privacy (SP)*. 2020, pp. 429–446. DOI: 10.1109/SP40000.2020.00021.
- [35] Pardis Emami Naeini et al. "Privacy expectations and preferences in an IoT world". In: *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. 2017, pp. 399–412.
- [36] Majid Nasirinejad and Srinivas Sampalli. "Evaluating Consumer Behavior, Decision Making, Risks, and Challenges for Buying an IoT Product". In: *IoT 4.2* (2023), pp. 78–94.

- [37] Daisuke Nishijima and Masahiro Oguchi. "Measuring product lifetime extension potential by increasing the expected product lifetime: Methodology and case study". In: *Business Strategy and the Environment* 32.4 (2023), pp. 1218–1231.
- [38] Dawn Carla Nunziato. "The Digital Services Act and the Brussels Effect on Platform Content Moderation". In: *Chi. J. Int'l L.* 24 (2023), p. 115. URL: <https://cjl.uchicago.edu/print-archive/digital-services-act-and-brussels-effect-platform-content-moderation>.
- [39] Masahiro Oguchi et al. "Consumers' expectations for product lifetimes of consumer durables". In: *2016 Electronics Goes Green 2016+(EGG)*. IEEE. 2016, pp. 1–6.
- [40] Privacy International. *We looked into the software support practices for 5 of the most popular smart devices (and the results may disappoint you)*. 2022. URL: <https://privacyinternational.org/report/4965/we-looked-software-support-practices-5-most-popular-smart-devices-and-results-may>.
- [41] Prolific. en. URL: <https://www.prolific.co/> (visited on 09/21/2022).
- [42] Qualtrics. *Qualtrics translate survey*. URL: <https://www.qualtrics.com/support/survey-platform/survey-module/survey-tools/translate-survey/>.
- [43] Dan Robinson. *Nice smart device – how long does it get software updates?* 2023. URL: https://www.theregister.com/2023/01/16/smart_device_software_support/.
- [44] Norbert Schwarz et al. "Response scales: Effects of category range on reported behavior and comparative judgments". In: *Public opinion quarterly* 49.3 (1985), pp. 388–395.
- [45] Jenny Tang, Eleanor Birrell, and Ada Lerner. "Replication: How Well Do My Results Generalize Now? The External Validity of Online Privacy and Security Surveys". In: *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 2022, pp. 367–385.
- [46] Roger Tourangeau, Lance J. Rips, and Kenneth Rasinski. *The Psychology of Survey Response*. en. Google-Books-ID: bjVYdyXXT3oC. Cambridge University Press, Mar. 2000. ISBN: 978-0-521-57629-1.
- [47] UK National Cyber Security Center. *Smart devices: new law helps citizens to choose secure products*. 2024. URL: <https://www.ncsc.gov.uk/blog-post/smart-devices-law>.
- [48] European Union. "General Data Protection Regulation". In: (2016). URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.
- [49] European Union. "Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC (Text with EEA relevance.)" In: *Official Journal of the European Union* (2019). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019L0771>.
- [50] European Union. "Proposal for a Regulation on cybersecurity requirements for products with digital elements - Cyber resilience Act". In: (2022). URL: <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act>.

- [51] Tanvi Vats, Neelima Sailaja, and Fabiana Anselmo Polido Lopes. "Exploration of User Perspectives around Software and Data-Related Challenges Associated with IoT Repair and Maintenance against Obsolescence: User Study on Software and Data Interactions and Considerations for IoT Repair and Maintenance against Obsolescence". In: *Proceedings of the 13th Nordic Conference on Human-Computer Interaction*. 2024, pp. 1–17.
- [52] Harald Wieser, Nina Tröger, and Renate Hübner. "The consumers' desired and expected product lifetimes". In: *Product Lifetimes And The Environment* (2015).

7.

The Vulnerability of Consumers under the Cyber Resilience Act

This article was submitted to JIPITEC on 31 March 2026. There have been no significant developments since the submission of the article.

Abstract

Human vulnerability is receiving increasing attention from scholars across disciplines, especially within the digital context. Initially, researchers often viewed specific individuals as 'vulnerable', due to fixed characteristics (e.g., age). However, modern analyses highlight how everyone can be vulnerable, for instance through the power imbalances within modern digital platforms.

EU legislation also addresses human vulnerability. The recently enacted Cyber Resilience Act (CRA) also shortly refers to the 'vulnerable consumer', without any further conceptualisation of that consumer. This notion warrants more attention, given ongoing discussions on the (legal) meaning of human vulnerability, especially in the nascent area of cybersecurity law.

This paper questions how the CRA's reference to protecting vulnerable consumers fits within ongoing calls for protecting vulnerable individuals in the digital realm. The paper holds that the CRA's structure as product safety law offers a beneficial approach to vulnerable consumers, but its provisions only offer a glimpse of this potential.

1 Introduction

Virtually everyone interacts with digital systems on a daily basis, even—or especially—during their most vulnerable moments. For example, individuals with health problems may more easily find social interaction through online platforms, being more accessible than offline options. At the same time, many children partake in online activities, such as through social media platforms, where they may encounter content unsuitable for their age. Digital systems and human vulnerability are thus becoming more interconnected.

The academic conceptualization of ‘vulnerability’ started in the 1980s, with scholars focusing on the vulnerability of people to natural disasters and other catastrophic events.¹ Today, vulnerability plays an ongoing role in interdisciplinary scholarship.² Modern notions hold that every individual may be or become vulnerable due to a number of reasons and causes.³ These reasons and causes often converge to such an extent that some scholars have stated that vulnerability is inherent in each person, a universal condition of being human.⁴

In the legal field, the exploration of what ‘vulnerability’ would mean was instigated mainly by human rights discussions and the Unfair Commercial Practices Directive (UCPD), but today the term appears in a plethora of EU legislation on digitalisation, such as the General Data Protection Regulation (GDPR) and, more recently, in the AI Act.⁵

Recently, the EU legislators also included the term ‘vulnerable consumer’ in the Cyber Resilience Act (CRA).⁶ The CRA enacts cybersecurity rules for virtually all software and hardware products on the market of the European Union.⁷ Recital 10 notes that the CRA will provide these rules also for products ‘intended for vulnerable consumers’. The CRA does not explicitly define a vulnerable consumer, raising unclarity about its meaning.

The need for a response to this question is amplified by cyberattacks which highlight the connection between cybersecurity and human vulnerability (e.g., health data breaches) and the ongoing legal debates surrounding the role of human vulnerability under EU law. Connecting both, the role of human vulnerability under EU cybersecurity law has not been addressed by

1 François Delor and Michel Hubert, ‘Revisiting the Concept of “Vulnerability”’ (2000) 50 *Social Science & Medicine* 1557, 1561; Sofia Ranchordas and Malou Beck, ‘Vulnerability’ in Mareile Kaufmann and Heidi Mork Lomell (eds), *De Gruyter Handbook of Digital Criminology* (De Gruyter 2025).

2 For an overview, see Ranchordas and Beck (n 1).

3 *ibid.*

4 Martha Albertson Fineman (ed), ‘The Vulnerable Subject: Anchoring Equality in the Human Condition’ (2010) 20 *Yale Journal of Law and Feminism* 1.

5 Duivenvoorde already discussed vulnerability in the UCPD in 2013, see Bram Duivenvoorde, ‘The Protection of Vulnerable Consumers under the Unfair Commercial Practices Directive’ [2013] *Journal of European Consumer and Market Law* 69; for an extensive overview of vulnerability in EU legislation, see Gianclaudio Malgieri, *Vulnerability and Data Protection Law* (1st edn, Oxford University Press 2023) ch 3; for the AI Act, see Federico Galli and Claudio Novelli, ‘The Many Meanings of Vulnerability in the AI Act and the One Missing’ [2024] *BioLaw Journal - Rivista di BioDiritto* 53.

6 Recital 10, Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

7 Art 1 CRA.

prior research. This mix of reasons reflects on the necessity of further exploration, even though the CRA only contains a minor reference to consumer vulnerability. The research question of this paper, therefore, is ‘Based on recent (legal) scholarship on human vulnerability, what does the ‘vulnerable consumer’ under the Cyber Resilience Act entail and to what extent does the Act mitigate the risks for such vulnerable consumers?’ Since the CRA speaks of the ‘vulnerable consumer’, most of the paper refers to either human or consumer vulnerability. However, most of the analysis provided in this paper addresses vulnerable individuals generally, thus including non-consumers as well.

The analysis proceeds as follows. Section 2 focuses on the academic conceptualisation of ‘human vulnerability’, specifically with regards to cybersecurity. Section 3 proceeds with a legal focus on human vulnerability, by analysing its role in the Unfair Commercial Practices Directive and, more recently, in legislation concerning digitalisation, such as the General Data Protection Regulation and AI Act. In Section 4, the analysis shift towards the Cyber Resilience Act, indicating its approach to human vulnerability and whether this approach fits with modern interdisciplinary scholarship on vulnerability. Section 5 rounds up the analysis by questioning the role of the Cyber Resilience Act—as product safety law—for mitigating human vulnerability. Section 6 concludes.

2 Human vulnerability under interdisciplinary scholarship

Speaking of a ‘vulnerability’ is commonplace in cybersecurity circles. Most often, cybersecurity professionals focus on vulnerabilities of systems and processes.⁸ Attackers exploit such vulnerabilities to infiltrate systems. Weak password encryption, for instance, forms such a vulnerability: without strong passwords, attackers can easily gain unauthorized access to user accounts. Such unauthorized access then gives rise to cybercrime that also affects the user: when an attacker holds the system hostage after they gain unauthorized access, the user is affected and must decide if they want to pay to regain access to—possibly critical—data. This effect on the user is where human vulnerability comes to the fore: instead of the notion of vulnerability of a system or process, human vulnerability focuses on factors which render (groups of) individuals (more) vulnerable. Here, I focus on how interdisciplinary scholarship came to understand those factors over recent years—and how they relate to cybersecurity.

In early conceptualisations, researchers often assigned vulnerability to certain populations due to fixed characteristics.⁹ Under this notion, individuals are vulnerable simply because they belong to a specific sub-population. Scholars soon challenged this early notion, since it does not distinguish between individuals within a sub-group and also assumes that vulnerability

8 The UK Cybersecurity Council defines a vulnerability as ‘an aspect of a computer system or network that is susceptible to intrusion due to a flaw in design or programming’ and the NIST speaks of a ‘weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.’ See <<https://www.ukcybersecuritycouncil.org.uk/glossary/>> and <<https://csrc.nist.gov/glossary/term/vulnerability>> respectively.

9 Florencia Luna, ‘Elucidating the Concept of Vulnerability: Layers Not Labels’ (2009) 2 IJFAB: International Journal of Feminist Approaches to Bioethics 121, 124.

is an infinite state, while, in reality, vulnerable can be transient (e.g., financial status).¹⁰ Some elderly people may be defined as 'vulnerable' in a digital context, but it is certainly false to state that all elderly people are vulnerable;¹¹ certain older individuals will have more than adequate knowledge about the digital environment in which they operate (e.g., someone who worked in the ICT sector).¹²

In contrast, Fineman held that vulnerability is a perpetual state, one part of being human.¹³ Under this notion, vulnerability is not a particular attribute, but a universal one. For instance, all humans, through our bodies, are vulnerable to biological problems, such as illness.¹⁴ Such universal vulnerability exists in the cybersecurity context too. In the cybersecurity context, one of the main drivers of vulnerability is the information and power asymmetry between the product manufacturer and the consumer.¹⁵ Virtually every person is vulnerable, because they do not have the capacity to fully understand the technical characteristics of devices and services that they engage with.¹⁶ In this context, researchers also speak of 'digital vulnerability', a type of vulnerability established by the 'state of powerlessness present in the digital environment'.¹⁷ Even the most senior cybersecurity expert will not consider all the security aspects of each device or service that they use, simply due to time constraints. Additionally, the manufacturer often carries the sole ability to adopt cybersecurity measures (e.g., encrypted data exchange).¹⁸ In general, the (well-informed) user only holds economic influence over these measures: they can simply refrain from purchasing or using the product. The consumer is thus inherently limited in their engagement with cybersecurity, causing an inherent state of vulnerability.

Fineman's concept of universal vulnerability, however, does not necessarily concern individual differences.¹⁹ Vulnerabilities are not one-dimensional, but layered.²⁰ A child may, for instance, have a learning disability. Both attributes (younger age and a learning disability) form vulnerability layers, which distinguish between individuals within a traditionally considered vulnerable sub-group.²¹ For cybersecurity, these layers matter too. The effects of cybercriminal activities can increase when someone carries multiple layers of vulnerability: a person with limited digital knowledge *and* a learning disability may be more prone to online scams or phishing e-mails. If this person is a child, they are perhaps even more prone to falling victim

10 Alyson Cole, 'All of Us Are Vulnerable, But Some Are More Vulnerable than Others: The Political Ambiguity of Vulnerability Studies, an Ambivalent Critique' (2016) 17 *Critical Horizons* 260.

11 Duivenvoorde (n 5) 73–77.

12 Dawn Branley-Bell and others, 'Exploring Age and Gender Differences in ICT Cybersecurity Behaviour' (2022) 2022 *Human Behavior and Emerging Technologies* 1.

13 Fineman (n 4).

14 *ibid* 9.

15 Federico Ferretti, 'The Consumer Image under EU Law: Average, Rationally Bounded and Dispositionally Vulnerable. What Are the Prospects for Protection in Digital Markets?' (2025) 62 *Common Market Law Review* 121, 138–141; See also Malgieri (n 5) 51 stating 'The identifying criterion of the consumer–supplier relationship is power asymmetry.'

16 Steven Furnell and Kerry-Lynn Thomson, 'Recognising and Addressing "Security Fatigue"' (2009) 2009 *Computer Fraud & Security* 7; see also in Ranchordas and Beck (n 1) 511.

17 Ferretti (n 15) 136; see also N Helberger and others, 'Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability' (2022) 45 *Journal of Consumer Policy* 175.

18 Rebrean and Malgieri also speak of 'asymmetrical dependency': Maria-Lucia Rebrean and Gianclaudio Malgieri, 'Vulnerability in the EU AI Act: Building an Interpretation', *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency* (ACM 2025) 1945.

19 Although Fineman does acknowledge the existence of individual differences: Fineman (n 4) 10.

20 Luna (n 9).

21 *ibid* 128–129.

to a cyberattack. Additionally, the *effects* of a cyberattack can increase depending on a person's layered vulnerabilities. Those effects could even render a person more vulnerable, for example through mental harms. The theory of layered vulnerabilities thus allows for an understanding of how different vulnerability factors can combine and thus impact diverse individuals in diverse ways.

The layered vulnerability theory also connects to cybersecurity's traditional technical vulnerabilities. A malicious actor who retrieves a system's administrators account details through phishing techniques should not immediately gain access to other systems, given sufficient access control mechanisms that prevent further escalation when the administrator's account is compromised. In this context, the administrator is also rendered vulnerable by how the systems they engage with are designed—a 'systemic' vulnerability.²² In the cybersecurity context, an insufficiently secured system forms such a systemic vulnerability for the system's users. This systematic vulnerability builds on the power asymmetry between the manufacturer and the consumer: it is the manufacturer who implements cybersecurity measures, but the end user who may carry shame, guilt, or even damages if their vulnerable state is exploited.²³ A systemic vulnerability thus forms an additional layer of human vulnerability in a cybersecurity context, one manifested by a lack of adequate cybersecurity measures in digital products.

Human vulnerability differs from the more common notion of vulnerability of systems in cybersecurity. In essence, all humans are vulnerable, as evident from the information asymmetry shaped by modern manufacturer-consumer relations. However, additional layers of vulnerability may exist, for instance when a child has a learning disability or through systemic vulnerabilities in modern digital products. Human vulnerability is thus a context-dependent and dynamic concept.

3 Human vulnerability under recent EU law

The multi-faceted nature of human vulnerability is also evident in EU legislation. In consumer law, the Unfair Commercial Practices Directive has contained the notion for two decades, while the General Data Protection Regulation and the AI Act have brought the concept to digital policy.²⁴ In this Section, I discuss the meaning of vulnerability under this legislation, to provide a holistic review of consumer vulnerability under the Cyber Resilience Act in Section 4. In particular, I focus on the existence of vulnerability as both universal and layered in these pieces of legislation.

22 Ferretti (n 15) 137.

23 Karen Renaud, Rosalind Searle and Marc Dupuis, 'Shame in Cyber Security: Effective Behavior Modification Tool or Counterproductive Foil?', *New Security Paradigms Workshop* (ACM 2021).

24 Vulnerability is also found in other legislation, including the Digital Services Act and Product Safety Regulation. This paper does not intend to provide a full scope overview of human vulnerability in EU legislation and thus Section 3 focuses on several (more) prominent examples.

3.1 The Unfair Commercial Practices Directive

The EU enacted the Unfair Commercial Practices Directive (UCPD) in 2005.²⁵ Since its inception, the UCPD contained a definition for the ‘vulnerable consumer’—the same term which now appears in the Cyber Resilience Act.²⁶ The UCPD enacted the term as an exception to the general rule of the ‘average consumer’, a benchmark which the Court of Justice of the European Union (CJEU) developed to understand how certain commercial practices affect a general consumer.²⁷

In *Gut Springenheide* (1998), the Court summarised earlier case law on product labelling to hold that the average consumer is a ‘reasonably well informed and reasonably observant and circumspect’ person.²⁸ In 2000, the Court added a further condition in *Lauder*.²⁹ The Court held that the average consumer must be conceptualised using several additional considerations, such as ‘social, cultural or linguistic factors’.³⁰

In 2005, the Unfair Commercial Practices Directive codified the average consumer benchmark and included the *Lauder* test. The Directive takes as a benchmark the ‘average consumer, who is reasonably well-informed and reasonably observant and circumspect, taking into account social, cultural and linguistic factors, as interpreted by the Court of Justice.’³¹ The UCPD prohibits a commercial practice when it ‘materially distorts or is likely to materially distort the economic behaviour’ of the average consumer (e.g., falsely stating that a product can be sold legally).³²

However, the UCPD concept of an average consumer is rather archaic.³³ The CJEU established the average consumer benchmark before the incursion of online consumerism, which occurs in an environment where data-driven practices (e.g., personalised advertisements) constantly aim to influence a consumer’s decision-making.³⁴ Modern consumers must thus process all kinds of (false) information, which shifts the benchmark for a reasonably well-informed consumer.³⁵ In other words, faced with immense data-driven power imbalances, the average consumer

25 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (‘Unfair Commercial Practices Directive’) [2005] OJ L149/22.

26 Art 5(3) UCPD.

27 *Malgieri* (n 5) 29.

28 Case C-210/96 *Gut Springenheide GmbH and Others v Oberkreisdirektor des Kreises Steinfurt Ä Amt für Lebensmittelüberwachung* ECLI:EU:C:1998:369, [1998] ECR I-4681 at 31.

29 Case C-220/98 *Estée Lauder Cosmetics GmbH & Co. OHG v Lancaster Group GmbH* ECLI:EU:C:2000:8, [2000] ECR I-135.

30 Case C-220/98 *Estée Lauder Cosmetics v Lancaster Group* (n 59) at 29.

31 Unfair Commercial Practices Directive, Recital 18.

32 Art 5(2)(b) UCPD. For this specific example, see its outright ban in art Annex I(9) UCPD.

33 *Malgieri* (n 5) 30–32.

34 Michelle Liu, ‘Digital Vulnerability: Rethinking Power Imbalances in the Digital Age’ (2024) 32 *European Review of Private Law* 827.

35 Emilia Mišćenić, ‘Information, Transparency and Fairness for Consumers in the Digital Environment’ in Camilla Crea and Alberto De Franceschi (eds), *The New Shapes of Digital Vulnerability in European Private Law* (Nomos Verlagsgesellschaft mbH & Co KG 2024); see also Christine Riefa, ‘Protecting Vulnerable Consumers in the Digital Single Market’ (2022) 33 *European Business Law Review* 607, 618.

can no longer regain a balanced relationship with the trader by becoming ‘reasonably well-informed’.³⁶

Next to the average consumer benchmark, the UCPD offers an alternative benchmark for vulnerable consumers. Under the UCPD, vulnerable consumers are a member of a ‘clearly identifiable group of consumers who are particularly vulnerable to the practice or the underlying product because of their mental or physical infirmity, age or credulity in a way which the trader could reasonably be expected to foresee.’³⁷ The same provision mentions how to assess the fairness of a commercial practice for vulnerable consumers. This assessment questions whether a commercial practice is likely to distort the economic behaviour ‘only of a clearly identifiable group’ of vulnerable consumers.³⁸ In other words, a practice may be fair for the average consumer, but unfair from the perspective of an average member of a group of vulnerable consumers.³⁹

The UCPD’s vulnerable consumer benchmark, however, does not coincide with more modern conceptualisations of vulnerability. Helberger et al. point out that the UCPD’s approach contains elements of what Cole calls a ‘victim approach’ to vulnerability: ‘the concept is used to draw attention to the inherent weakness of particular groups, or their inability to fend for their own interests.’⁴⁰ Indeed, the UCPD builds on a binary approach that delineates between those consumers who are vulnerable and those who are not: the vulnerable group is a stark demarcation from the average consumer and thus requires specific protection.

This victimized approach to vulnerability does not align with the universal approach to vulnerability proposed by Fineman.⁴¹ As mentioned in Section 2, Fineman holds that vulnerability is an inherent universal state. The UCPD, in contrast, views vulnerability as a permanent attribute of particular groups of consumers.⁴²

Next to this universal state of vulnerability, the UCPD does also not consider how vulnerability can come in layers.⁴³ The Directive specifies which criteria determine an individual’s vulnerability. While these criteria are non-exhaustive,⁴⁴ they appear as mutually exclusive. The theory of layered vulnerability points to the different sources of vulnerability which may exist simultaneously. In this sense, it is not, as the UCPD notes ‘mental *or* physical infirmity’, but mental *and* physical infirmity which may render an individual (more) vulnerable.⁴⁵

More recently, the European Commission seems to have picked up on a more universal and layered concept of vulnerability, as a recent report states that ‘consumer vulnerability is situational, meaning that a consumer can be vulnerable in one situation but not in others,

36 Helberger and others (n 17); Ferretti (n 15).

37 Art 5(3) UCPD.

38 Art 5(3) UCPD.

39 Helberger and others (n 17) 178–179 who also point out that this is the only role for the vulnerable consumer benchmark in the UCPD.

40 *ibid* 179; Cole (n 10).

41 Fineman (n 4).

42 On so-called ‘particularism’, see Gianclaudio Malgieri and Jędrzej Niklas, ‘Vulnerable Data Subjects’ (2020) 37 Computer Law & Security Review 105415.

43 Luna (n 9).

44 Duivenvoorde (n 5) 71; on the affirmation of non-exhaustiveness in more recent guidelines, see Riefa (n 35) 614.

45 See on the infirmity conditions, Duivenvoorde (n 5) 77–78.

and that some consumers may be more vulnerable than others.⁴⁶ In addition, the CJEU recently acknowledged that cognitive biases can influence an individual's decision-making—thus offering a (limited) addition to the current interpretation of the average consumer benchmark.⁴⁷ Both developments may point to a legislative evolution, where modern concepts of vulnerability shape the average or vulnerable consumer benchmark.

3.2 General Data Protection Regulation

The General Data Protection Regulation (GDPR) forms the key legislative act for data protection law in the European Union.⁴⁸ The GDPR is one of the first pieces of legislation which points to human vulnerability in the context of digital technology.

The GDPR centers around rules for entities which process (e.g., collecting) personal data of 'data subjects' (i.e., users of digital systems).⁴⁹ The data subject notion contains many elements of the average consumer under the UCPD. Malgieri finds a general interpretation of the data subject as a person who 'reads the information policy and makes free rational and conscious decisions'.⁵⁰ Building on this similarity, the GDPR places the vulnerable data subject in the context of data protection risk management.⁵¹ Recital 75 holds that entities must assess data processing risks when 'personal data of vulnerable natural persons, in particular of children, are processed.' Hence, the GDPR indicates that children are one example of 'vulnerable natural persons', leaving room for further interpretations.⁵²

Malgieri recognises two categories of vulnerability in these data processing relations: one occurs *during* data processing and the other is based on the *outcome* of data processing.⁵³ During data processing, the data subject might not know how to exercise the rights afforded to them by the GDPR, such as the right to access their personal data. The outcome of data processing may also affect the data subject, for example when an Amazon driver is reprimanded when AI data processing systems determine that they drink coffee while driving their delivery van.⁵⁴ These two categories aptly describe the type of human vulnerability that occurs in the cybersecurity domain as well: vulnerability may arise due to the use of a product—through asymmetric power relations—but also due to the outcome of a cyberattack, such as through mental harms.

46 European Commission, 'Understanding Consumer Vulnerability in the EU's Key Markets' (2016) <https://commission.europa.eu/system/files/2018-04/consumer-vulnerability-factsheet_en.pdf> accessed 7 February 2025.

47 Case C-646/22 *Compass Banca SpA v Autorità Garante della Concorrenza e del Mercato (AGCM)* ECLI:EU:C:2024:957, [2024]. See on the limits of this case: M Namysłowska, 'The Silent Death of EU Consumer Law and Its Resilient Revival: Reinventing Consumer Protection Against Unfair Digital Commercial Practices' [2025] *Journal of Consumer Policy*, 10.

48 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

49 Art 2 GDPR.

50 Malgieri (n 5) 40.

51 Malgieri and Niklas (n 42).

52 Malgieri (n 5) 87.

53 *ibid* 89.

54 Orianna Rosa Royle, 'Amazon Driver Breaks down the AI System Watching Them for Safety Violations like Drinking Coffee While Driving' (*Fortune*) <<https://fortune.com/2023/02/27/amazon-delivery-driver-breaks-down-ai-surveillance-in-vans/>> accessed 25 March 2025.

The GDPR has a risk-based approach to data protection.⁵⁵ Hence, the GDPR mentions the vulnerable data subject in the context of a Data Processing Impact Agreement (DPIA), ‘an assessment of the impact of the envisaged processing operations on the protection of personal data’ when the activity ‘is likely to result in a high risk to the rights and freedoms of natural persons.’⁵⁶ This risk-based approach aligns with the theory of layered vulnerability.⁵⁷ For instance, if a software developer builds a website for autistic children, there are layered risks which require stricter data protection measures. In this line, data protection risks are one element of a wider cybersecurity-minded risk assessment:⁵⁸ a data breach may affect vulnerable individuals more than others.

At the same time, the GDPR’s framework also highlights the conceptual complexity of human vulnerability. Since the GDPR does not itself define the vulnerable data subject, much interpretation is left to practice and data protection supervision authorities.⁵⁹ This approach, so far, led to a fragmented and unclear meaning of the ‘vulnerable data subject’ under the GDPR.⁶⁰

3.3 AI Act

In 2024, the European legislators enacted the AI Act.⁶¹ The AI Act regulates the use of artificial intelligence systems through a risk-based approach.⁶² The Act is part of the ‘New Legislative Framework’—together with, inter alia, the Cyber Resilience Act—which introduces harmonised product safety requirements for the European market.⁶³

AI systems pose unique risks to vulnerable (groups of) individuals. Teo exemplifies these risks through machine learning models which can identify individuals with low impulse control, by using rather trivial data, such as the spoken language or eye movement.⁶⁴ This means that the data vector ‘age’, which often identifies (more) vulnerable people, is not necessary to identify individuals with low impulse control. AI systems therefore challenge traditional notions of data related to vulnerability (e.g., health data).

The AI Act works with different risk levels for AI systems; some systems are prohibited, where others have strict requirements depending on their risk level.⁶⁵ The AI Act references

55 Raphaël Gellert, *The Risk-Based Approach to Data Protection* (1st edn, Oxford University Press 2020).

56 Art 35(1) & Recital 75 GDPR.

57 Malgieri and Niklas (n 42) 11–12.

58 See also art 32 GDPR, which requires ‘appropriate’ security measures for data processing.

59 Stanislaw Piasecki, ‘Expert Perspectives on GDPR Compliance in the Context of Smart Homes and Vulnerable Persons’ (2023) 32 *Information & Communications Technology Law* 385, 392.

60 Malgieri (n 5) ch 1.

61 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L2024/1689.

62 Art 1 AI Act.

63 European Commission, ‘New Legislative Framework’, <https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en>.

64 Sue Anne Teo, ‘Artificial Intelligence, Human Vulnerability and Multi-Level Resilience’ (2025) 57 *Computer Law & Security Review* 106134, 7.

65 See Raphaël Gellert, ‘The Role of the Risk-Based Approach in the General Data Protection Regulation and in the European Commission’s Proposed Artificial Intelligence Act: Business as Usual?’ (2021) 3 *Journal of Ethics and Legal Technologies* 16.

vulnerability in multiple ways. However, in line with the GDPR, the AI Act does not offer a single definition for vulnerability.⁶⁶

Most prominently, AI systems which ‘exploit an individual’s vulnerabilities’ are prohibited.⁶⁷ This concept of vulnerability seems closely related to the vulnerable consumer benchmark of the UCPD: it is the *misuse* of someone’s vulnerability that the legislation aims to tackle. However, authorities will face difficulties in gauging when exploitation occurs, especially since certain AI systems continuously adapt to new vectors, thus leaving considerable leeway for future—unforeseen—impact.⁶⁸

A second notion of vulnerability considers how an AI system may exploit vulnerabilities not directly, but as a side-effect of processing.⁶⁹ For ‘high-risk’ AI systems, the AI provider must perform a risk assessment, which must also consider whether the system ‘is likely to have an *adverse impact* on persons under the age of 18 [...] and other vulnerable groups.’⁷⁰ Vulnerability also has a role in the risk management provisions for market surveillance authorities and the AI Act’s own authority, the AI Office.⁷¹ As mentioned for the GDPR, placing vulnerability inside a risk assessment aligns with layered concepts of vulnerability. The AI Act thus continues the framework set in place by the GDPR, by assessing human vulnerability as part of a broader risk management framework.⁷²

Finally, the AI Act also considers vulnerability stemming from power asymmetries. The Commission may adapt the list of high-risk AI systems.⁷³ In their assessment, the Commission must consider ‘the extent to which there is an *imbalance of power*, or the persons [who the systems affects] are in a *vulnerable position* in relation to the deployer of an AI system, in particular due to *status, authority, knowledge, economic or social circumstances, or age*.’⁷⁴ The relation between age and vulnerability is thus present throughout the AI Act (e.g., in the risk management framework for high-risk systems),⁷⁵ while concepts such as ‘status’, ‘authority’ and ‘knowledge’ remain undefined.⁷⁶ How the Commission will assess these power relations thus remains unclear, but the AI Act does confirm that power relations shape human vulnerability.

The AI Act and Cyber Resilience Act are part of the same New Legislative Framework for product requirements. The position of human vulnerability in the AI Act thus indicates how

66 Galli and Novelli (n 5); Rebrean and Malgieri (n 18).

67 Art 5(1)(b) AI Act.

68 Teo (n 64).

69 Galli and Novelli (n 5) 61.

70 Art 9(9) AI Act. Emphasis mine.

71 Art 79(2) & 95 AI Act.

72 Galli and Novelli (n 5) 56 stating ‘in this risk-based regulatory architecture, vulnerability constitutes a key component of AI Risk.’

73 Art 7 AI Act.

74 Art 7(2)(h) AI Act. Emphasis mine.

75 Art 9(9) AI Act.

76 Galli and Novelli (n 5) 63.

product safety requirements and mitigating human vulnerability can come together.⁷⁷ It is clear that vulnerability is now a key element of risk assessment procedures.

3.4 The legal landscape for human vulnerability

The UCPD, GDPR, and AI Act highlight the current role for human vulnerability under EU law.

The UCPD places vulnerability in a clear consumer protection framework: vulnerability only arises during a commercial practice and is an act where the *trader* exploits the *consumer*. The definition of a vulnerable consumer under the UCPD shows a bygone notion of vulnerability as an attribute of specific populations.

The GDPR and AI Act highlight how human vulnerability is approached legally in a digital context. They show that human vulnerability is now mainly an element of risk assessment procedures. This approach allows for a more modern notion of human vulnerability, through considerations of layered vulnerability. In other words, if a system is designed for use by children with learning disabilities, the developers must adopt stricter risk management measures than if they designed the system for the general public. The GDPR shows that this approach also concerns cybersecurity. In the following, I build on these equivalences and analyse to which extent the Cyber Resilience Act meets the modern concepts of universal and layered vulnerability.

4 Vulnerable consumers under the Cyber Resilience Act

The Cyber Resilience Act (CRA) notes that ‘vulnerable consumers’ require protection against cybersecurity risks propagated by modern digital products.⁷⁸ As with the General Data Protection Regulation, the Act only contains this short reference in the Recitals, with further operationalisation left to its provisions. The Recitals do not have legal power; they, however, help judges and authorities in interpreting the legal provisions.⁷⁹ Given the relation between cybersecurity and human vulnerability, a better understanding of this reference is required. Unfortunately, the ‘vulnerable consumer’ definition in the Unfair Commercial Practices Directive does not offer a proper conceptualisation, given its archaic interpretation of human vulnerability. Moreover, the CRA is not a piece of consumer protection legislation.⁸⁰ Rather, the CRA aims to set horizontal rules for ‘products with digital elements’.⁸¹

The analysis therefore first addresses the scope and primary objectives of the CRA. Second, it focuses on how the CRA aims to mitigate universal human vulnerability, i.e. the asymmetric

⁷⁷ See also the risk assessment in the Product Safety Regulation: Art 6(1)(e) Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC.

⁷⁸ Recital 10 CRA.

⁷⁹ Case C-162/97 *Nilsson and others* ECLI:EU:C:1998:554, [1998] ECR I-7477, para 54.

⁸⁰ See Recital 4 CRA, stating ‘The Union regulatory landscape should be harmonised by introducing horizontal cybersecurity requirements for products with digital elements.’

⁸¹ Pier Giorgio Chiara, ‘Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise?’ [2025] *European Journal of Risk Regulation* 1.

power relation between manufacturer and consumer. Third, the analysis focuses on how the CRA's risk-based approach may address layered vulnerability, in line with the GDPR and AI Act.⁸²

4.1 The basis of the Cyber Resilience Act

The CRA prescribes cybersecurity requirements for 'products with digital elements', i.e. virtually all software and hardware products, that manufacturers wish to place on the EU market.⁸³ This product safety approach aligns with the CRA's position in the New Legislative Framework, together with, *inter alia*, the AI Act. The CRA aims to provide an 'objective-oriented and technology neutral' horizontal approach.⁸⁴ All products must adhere to similar requirements, except for two categories of 'important' and 'critical' products which pose a more substantial cybersecurity risk.⁸⁵ I discuss the meaning of this categorisation more extensively in Section 4.3.

Manufacturers must comply with a diverse set of requirements under the CRA. There are two main sets: 1) cybersecurity-related requirements and 2) product information requirements. In the first category, the CRA's Annex lists requirements such as providing sufficient data integrity and swift remediation of technical vulnerabilities through updates.⁸⁶ In the second category, the CRA requires manufacturers to provide information with the product so that consumers can make informed decisions before and after purchasing a product.⁸⁷ For example, the CRA requires manufacturers to share how long they provide security updates for each specific product.⁸⁸

As product safety regulation, the CRA follows a product labeling approach. As proof of compliance, manufacturers can affix a CE mark to their product.⁸⁹

Recital 10 manifests the role of human vulnerability in the CRA. The Recital states that the CRA intends to enhance the cybersecurity of products, which 'also includes requirements for placing on the market consumer *products [...] intended for vulnerable consumers*'.⁹⁰ This terminology aligns with the CRA as product safety law: the emphasis is on the products—what consumers are they intended for—rather than specifying consumer vulnerability. As further proof of this focus, the Recital refers to 'toys and baby monitoring systems' as examples of 'products intended for vulnerable consumers'. The CRA thus only offers a glimpse of which consumers are 'vulnerable' through defining specific products, in this case children.

Outside Recital 10, the CRA mainly relies on a technical concept of vulnerability. The CRA defines a vulnerability as 'a weakness, susceptibility or flaw of a [product] that can be exploited by a cyber threat'.⁹¹ Such a vulnerability—for instance unencrypted data storage—makes the

82 Éloïse Gennet, Roberto Andorno and Bernice Elger, 'Does the New EU Regulation on Clinical Trials Adequately Protect Vulnerable Research Participants?' (2015) 119 *Health Policy* 925; Malgieri and Niklas (n 42).

83 Art 1 CRA.

84 Chiara (n 81) 4.

85 Art 7 & 8 CRA.

86 Annex I CRA.

87 Art 13 CRA.

88 Art 13(8) & 13(19) CRA.

89 Art 30 CRA.

90 Emphasis mine.

91 Art 3(40) CRA.

system susceptible to attacks from external actors, such as hackers. A technical cybersecurity vulnerability, therefore, differs from human vulnerability. Of the three elements (weakness, susceptibility, flaw), only one aligns narrowly with human vulnerabilities: susceptibility. Vulnerable humans are indeed susceptible to exploitation of their vulnerabilities, which causes the need for mitigation strategies. In fact, a cybersecurity incident can cause such susceptibility for exploitation, for instance when a hacker gains access to a person's medical data. However, human vulnerability is not a weakness or flaw, i.e. something to be fixed.⁹²

In the following, I view the CRA's provisions through the lens of universal and layered vulnerability. The CRA does not contain explicit conceptual guidance, but its framework may still contribute to mitigating human vulnerabilities in the context of cybersecurity.

4.2 Universal vulnerability under the Cyber Resilience Act

A modern doorbell offers more than just a simple sound cue; the device often contains both a microphone and camera. With these doorbells, users can see who is at their door and remotely speak to them. A consumer purchasing this device, however, may become more vulnerable than a consumer who, years ago, bought a normal doorbell that simply just rang. The modern consumer relies on the manufacturer to keep their doorbell updated with the latest security fixes. If, instead, the product is not sufficiently secure, it is possible that other people gain access to the camera and thus valuable insights into the consumer's daily life (e.g., when they leave their house). The consumer depends on the manufacturer to protect them against these risks; by simply purchasing their new doorbell, the consumer becomes (more) vulnerable. This asymmetric power relation forms the cornerstone of the universal vulnerability present in the cybersecurity context.

The CRA prescribes a security-by-design approach for products with digital elements. Security-by-design is a relatively novel concept; a unified definition does not exist yet, even in the legal domain.⁹³ The Cyber Resilience Act conceptualises the term specifically as a requirement for devices, which 'shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks'.⁹⁴ In addition, manufacturers must assess cybersecurity risks associated with their product, the outcome of which they must take into account 'during the planning, design, development, production, delivery and maintenance phases of the product'.⁹⁵

Security-by-design closely relates to 'security-by-default', often encompassing the latter term.⁹⁶ Security-by-default means that developers configure systems with the most secure settings and architecture by default (e.g., unique default passwords). As an embodiment of this concept, the Cyber Resilience Act requires that a device has a 'secure by default' configuration when placed on the market.⁹⁷

92 Claudia Wiesemann, 'On the Interrelationship of Vulnerability and Trust' in Christine Straehle (ed), *Vulnerability, Autonomy, and Applied Ethics* (Routledge 2016).

93 Lee A Bygrave, 'Security by Design: Aspirations and Realities in a Regulatory Context' (2022) 8 *Oslo Law Review* 126; Cristina Del-Real, Els De Busser and Bibi Van Den Berg, 'Shielding Software Systems: A Comparison of Security by Design and Privacy by Design Based on a Systematic Literature Review' (2024) 52 *Computer Law & Security Review* 105933.

94 Annex I Part I(1) CRA.

95 Art 13(2) CRA.

96 Bygrave (n 93) 126.

97 Annex I(I)(2)(b) CRA.

Security-by-design and by-default are processes which mitigate systemic vulnerabilities.⁹⁸ As mentioned in Section 2, systemic vulnerabilities in digital products render users (more) vulnerable. With security-by-design and by-default, the overall level of cybersecurity of systems improves. For instance, the smart doorbell will have technical specifications which ensure that the camera is not accessible remotely, other than by the consumer. The manufacturer cannot just ship a product without caring for the default state of cybersecurity in their product. Consequently, the consumer's position vis-à-vis the manufacturer improves: the manufacturer no longer holds sole control over the cybersecurity in their product.

Recently, legal frameworks mainly aimed to improve the asymmetric relation between manufacturer and consumers by empowering the consumer. For example, the CRA obliges the manufacturer to inform the consumer about many aspects of the product.⁹⁹ Riefa et al. pointed to the fallacy of information obligations, which policy makers often propose to rebalance the consumer-supplier relation.¹⁰⁰ It is a regulatory illusion that such information provision mitigates consumer vulnerabilities.¹⁰¹ For example, the CRA requires manufacturers to inform users when they cease their operations.¹⁰² The manufacturer does not have to inform the consumer of any logical next steps. What if the consumer is dependent on the continued functioning of that product?¹⁰³ Rather than 'empowering' the consumer, mitigating vulnerability requires infrastructural improvements,¹⁰⁴ such as security-by-design.

A related issue to information provision is dependency. The CRA places obligations on the manufacturer, so that *third parties* cannot exploit the consumer. In this triangular relation, the CRA differs from the UCPD, GDPR, and AI Act, which protect a vulnerable user in their direct relation to the trader, data controller, or deployer respectively.¹⁰⁵ In other words, the CRA manufacturer fulfills an active caretaking role. This role confirms the asymmetrical relation between manufacturer and consumer, as the consumer depends on the manufacturer for their cybersecurity needs.¹⁰⁶

The CRA brings an important shift. The consumer was always dependent on the manufacturer to take cybersecurity measures. The incursion of the CRA means that there are now authorities which govern this dependency; supervisory authorities can enforce the CRA with fines, or, in certain cases, by taking offending products out of the market.¹⁰⁷ Therefore, strong enforcement and supervision of the CRA is vital to ensuring an effective rebalancing of the asymmetrical

98 See also the connection between vulnerable consumers, security by design, and privacy by design in the Product Safety Regulation, Recital 23: 'Therefore, when assessing the safety of digitally connected products likely to have an impact on [vulnerable consumers, including] children, manufacturers should ensure that the products they make available on the market meet the highest standards of safety, security and privacy by design, in the best interests of children.'

99 Art 13 CRA.

100 Riefa (n 35) 621–624.

101 On this illusion in EU consumer law, see Ferretti (n 15).

102 Art 23 CRA.

103 Mattis van 't Schip, 'The Internet of Forgotten Things: European Cybersecurity Regulation and the Cessation of Internet of Things Manufacturers' (2025) 57 Computer Law & Security Review 106152.

104 Riefa (n 35) 622.

105 With some small exceptions, such as the cybersecurity provisions in the General Data Protection Regulation and the AI Act.

106 See further on the relation between dependence and vulnerability, Susan Dodds, 'Dependence, Care, and Vulnerability' in Catriona Mackenzie, Wendy Rogers and Susan Dodds (eds), *Vulnerability* (Oxford University Press 2013).

107 Art 52-58 & 64 CRA.

relation between manufacturer and consumer. Such enforcement can now influence the power dynamics between manufacturer and consumer over the cybersecurity of modern products.

4.3 Layered vulnerability under the Cyber Resilience Act

Where the theory of universal vulnerability addresses a shared state of vulnerability, the theory of layered vulnerability instead addresses a more individual situation. As discussed for the GDPR, this individualised approach therefore often connects to risk management, where each additional layer increases the risks contained in a data processing activity. The risk-based approach can contribute to mitigating, avoiding, or minimising vulnerability layers.¹⁰⁸ Most of the CRA consists of product conformity and risk-based provisions. Such a risk-based approach, as discussed for the GDPR, aligns well with mitigations proposed within the layered vulnerabilities framework.

There are two levels to the risk-based approach in the CRA: the first requires manufacturers to perform a generic risk assessment before placing their product on the EU market, while the second relies on the Commission's categorisation of 'important' and 'critical' products.

The use of products by vulnerable consumers is not an element of the required risk assessment that manufacturers must perform before placing their products on the EU market. The manufacturers must merely take into account 'the cybersecurity risks associated with [their product]'.¹⁰⁹ The manufacturer must assess such risks to minimise the impact of cybersecurity incidents, 'including in relation to the health and safety of users'.¹¹⁰ This means that the manufacturer might need to consider how cybersecurity *incidents* might render a consumer (more) vulnerable, but the risk assessment does not directly concern a consumer's existing vulnerability.

However, manufacturers must assess the 'reasonably foreseeable use' of their product, which is 'not necessarily the intended purpose supplied by the manufacturer [...], but which is likely to result from reasonably foreseeable human behaviour',¹¹¹ as part of the general risk assessment.¹¹² Based on this assessment, the manufacturer must indicate which security requirements 'are applicable to the [product]'.¹¹³ Imagine, for instance, that a manufacturer develops an AI chat bot; a further reasonably foreseeable use could be that people with lower socioeconomic status use the chat bot when they require psychological support. In other words, multiple layers of vulnerability might become apparent in the reasonably foreseeable use of a product. The manufacturer must take those layers into account and adopt certain (stronger) cybersecurity requirements.

The CRA, finally, includes a list of products which the legislators deem to carry 'significant risks of adverse effects', regardless of the manufacturer's own assessment.¹¹⁴ In the list of important products, there is a connection between risks and vulnerable consumers. For example, the category of 'important' products includes 'personal wearable products that are intended *for*

¹⁰⁸ Luna (n 9) 131; see also as described in Malgieri (n 5) 51.

¹⁰⁹ Art 13(2) CRA.

¹¹⁰ Art 13(2) CRA.

¹¹¹ Article 3(24) CRA.

¹¹² Article 13(3) CRA.

¹¹³ Article 13(3) CRA.

¹¹⁴ Recital 10 CRA.

the use by and for children', 'internet connected toys', and 'baby monitoring systems'.¹¹⁵ These, however, are specific examples: the Annex does not state that all products intended for children—or for vulnerable consumers—are 'important'. The list of critical products does not clearly connect to any (groups of) vulnerable consumers.¹¹⁶ The important and critical product categories therefore only add a few explicit examples to the list of 'products intended for vulnerable consumers'.

The CRA exemplifies again how a risk-based approach connects to mitigating layered vulnerabilities. However, the CRA only shortly refers to 'vulnerable consumers' in the Recital and does not explicitly refer to these consumers as part of the required cybersecurity risk assessment for manufacturers. The CRA does indicate that children are a group of consumers who deserve specific protection, but only for specific products. The role for layered vulnerabilities within the risk-based system of the CRA is thus implicit at most.

5 The Cyber Resilience Act as a platform for mitigating vulnerability

Most scholarship on consumer vulnerability so far addressed EU consumer law or digital policy such as the GDPR and the AI Act; the role of consumer vulnerability in cybersecurity law has, thus far, escaped scholarly attention. The Cyber Resilience Act puts human vulnerability forward in the context of the 'vulnerable consumer', but the CRA is not a piece of consumer law. The CRA is part of the New Legislative Framework, which introduces a broad set of product safety legislation.¹¹⁷ In addition, the CRA is a piece of 'cybersecurity law' based on its substantive focus on cybersecurity problems, together with recent legislation such as the NIS2 Directive.¹¹⁸ The combination of product safety law and cybersecurity law might offer alternatives to current approaches.

The CRA emphasises an ex-ante product safety approach by placing obligations on manufacturers before products are placed on the EU market. The product must conform with the CRA's standards, such as security-by-design requirements, before the manufacturer can place it on the EU market. Manufacturers must thus consider vulnerable consumers before placing the product on the European market, not when harm occurs.

At the same time, there are problems arising out of enforcing such ex-ante provisions, either through ex-post private litigation or ex-post public enforcement. European consumer law already confirms some of the problems arising from a *private ex-post* enforcement system. Goanta et al. hold that individualised legal approaches based on consumer vulnerabilities would lack practical impact.¹¹⁹ They point, for instance, to the need for judicial interpretation to mitigate consumer-specific vulnerabilities under an ex-post approach, which would take a

¹¹⁵ Annex III Class 1(19) CRA. Emphasis mine.

¹¹⁶ Annex IV CRA.

¹¹⁷ Chiara (n 81).

¹¹⁸ See, for instance, on this EU cybersecurity law landscape before the incursion of the CRA: Pier Giorgio Chiara, 'The IoT and the New EU Cybersecurity Regulatory Landscape' [2022] *International Review of Law, Computers & Technology* 1.

¹¹⁹ Catalina Goanta, Giovanni De Gregorio and Jerry Spanakis, 'Consumer Protection and Digital Vulnerability: Common and Diverging Paths' in Camilla Crea and Alberto De Franceschi (eds), *The New Shapes of Digital Vulnerability in European Private Law* (Nomos Verlagsgesellschaft mbH & Co KG 2024).

long time to develop and ‘may open the door to an overwhelming amount of individually personalised parameters and combinations of parameters which may be very specific to the circumstances of individual consumers.’¹²⁰ They consider such an approach the ‘complete collapse of harmonisation as we know it.’¹²¹ A private ex-post enforcement methodology thus requires vulnerable consumers to undertake extensive and complex legal procedures, with the risk of providing only specific, individualised remediation.

Public authorities can also conduct ex-post enforcement.¹²² However, the GDPR practice proves that authorities have so far struggled to find a meaningful role—and thus enforcement procedure—for human vulnerability. Industry professionals mentioned in a recent interview study that ‘organisations do not take vulnerable adults into consideration unless the device is specifically developed for them.’¹²³ Furthermore, respondents stated that children, a population deemed vulnerable in a broad set of EU legislation,¹²⁴ are often not even taken into account during product security implementation.¹²⁵ These responses show that the GDPR has not incentivised product developers to consider vulnerable consumers. Following the barriers presented in this paper, it thus remains unclear whether the public enforcement mechanisms of the CRA can provide more practical relevance for mitigating consumer vulnerability.

Finally, the CRA’s caretaker approach might also impact the relevance of cybersecurity or product safety rules for mitigating consumer vulnerabilities. The legislation mentioned in this paper generally regulated the ‘harmer’: the trader under EU consumer law, the controller under the GDPR, and the provider under the AI Act. The harm, under these frameworks, originates from the regulated entity while, in the case of cybersecurity, the harm originates from a third party who exploits systemic product vulnerabilities in such a way that they can exploit human vulnerabilities (e.g., through holding a person’s data ransom). In other legislation, this type of protection against third-party risks is part of cybersecurity-related provisions (e.g., DPIA, data breaches),¹²⁶ but not the intention of the overall legal framework. This ‘caretaker approach’ is thus rather novel and might also shape the legal protection afforded to vulnerable individuals.

Roughly summarised, the CRA offers some promising legal approaches for mitigating human vulnerabilities. The practical relevance for addressing human vulnerability strongly depends on the strength of public enforcement—which so far has not reached its potential under EU digital policy—and the impact of the ex-ante product safety rules on manufacturing processes.

6 Conclusion

The Cyber Resilience Act (CRA) forms the cornerstone of EU cybersecurity policy, bringing cybersecurity requirements to virtually all software and hardware products. The Recitals of the CRA include a small reference to ‘vulnerable consumers’, without further attention to its meaning. Although only a short reference, the attention paid to human vulnerabilities fits

¹²⁰ *ibid* 47.

¹²¹ *ibid*.

¹²² See Chapter V CRA.

¹²³ Piasecki (n 59) 392.

¹²⁴ See the summarising table in Malgieri (n 5) 63.

¹²⁵ Piasecki (n 59) 392.

¹²⁶ See, for instance, in the AI Act Art 15(5): ‘High-risk AI systems shall be resilient against attempts by unauthorised third parties to alter their use, outputs or performance by exploiting system vulnerabilities.’

within a longer discussion in EU digital policy circles. This paper therefore addressed the following research question: Based on recent (legal) scholarship on human and consumer vulnerability, what might consumer vulnerability entail under the Cyber Resilience Act and to what extent does the Act mitigate such vulnerability?

This paper shows that vulnerability is a context-dependent and dynamic topic. Human vulnerability is, as scholars have argued in recent years, an inherent universal experience—to be human is to be vulnerable. Such universal vulnerability is most visible in the asymmetric power relations in modern digital environments. Vulnerability, however, is also layered: although everyone is vulnerable to a certain extent, some people may have multiple layered vulnerabilities, such as a child with a physical disability. As such, vulnerability highly depends on a personal situation at a given moment—it is not a fixed binary attribute.

In European law, human vulnerability initially came to the fore in the Unfair Commercial Practices Directive (UCPD). This Directive concerns the ‘average consumer’, a well-informed and reasonable person, who may become subject to unfair commercial practices. If certain (groups of) individuals are particularly vulnerable—which the UCPD presents as a binary state—it is the average consumer of that vulnerable group who becomes the benchmark. This binary approach thus does not align with more recent scholarly advancements on human vulnerability.

More recently, human vulnerability came to the fore in the General Data Protection Regulation and the AI Act. In these legislative acts, the term is placed predominantly within a risk management framework: if certain vulnerable individuals may become subject to the data processing activities or AI systems, these activities and systems pose a higher risk.

The Cyber Resilience Act does not define the vulnerable consumer. The CRA, however, does mitigate human vulnerabilities when analysed from the perspective of universal and layered vulnerabilities. First, from the perspective of universal vulnerabilities, the CRA introduces product requirements such as security-by-design, which ensure that a product is secure regardless of consumer actions (e.g., unique default password). These measures raise the cybersecurity level of the product, thus reducing the vulnerable position of the consumer vis-à-vis the manufacturer. Second, from the perspective of layered vulnerabilities, the CRA highlights once more the emphasis on a risk-based approach. The CRA categorises specific products as higher risk when they are, for instance, used by children. In addition, the CRA requires some risks to be considered from which the manufacturer can infer that consumer vulnerabilities might play a role. This latter approach therefore remains rather limited.

Finally, this paper questions whether product safety law, such as the CRA and the AI Act, could help to mitigate human vulnerabilities. Product safety law often builds on the idea of protecting vulnerable consumers, so that products are safe according to specific contexts (e.g., rules for toys). These rules put forward an ex-ante approach in which manufacturers must immediately consider their product’s (unforeseen) effects. Furthermore, the emphasis on public enforcement means that the consumer is not (solely) responsible for ex-post litigation or enforcement of the CRA. Product safety law, such as the CRA, might thus offer practical relevance for vulnerable consumers. The effectiveness of such an approach, however, relies strongly on the efficacy of public enforcement and on further, more explicit references to human vulnerability in product safety risk management processes.

References

- Branley-Bell D and others, 'Exploring Age and Gender Differences in ICT Cybersecurity Behaviour' (2022) 2022 Human Behavior and Emerging Technologies 1
- Bygrave LA, 'Security by Design: Aspirations and Realities in a Regulatory Context' (2022) 8 Oslo Law Review 126
- Chiara PG, 'The IoT and the New EU Cybersecurity Regulatory Landscape' [2022] International Review of Law, Computers & Technology 1
- , 'Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise?' [2025] European Journal of Risk Regulation 1
- Cole A, 'All of Us Are Vulnerable, But Some Are More Vulnerable than Others: The Political Ambiguity of Vulnerability Studies, an Ambivalent Critique' (2016) 17 Critical Horizons 260
- Delor F and Hubert M, 'Revisiting the Concept of "Vulnerability"' (2000) 50 Social Science & Medicine 1557
- Del-Real C, De Busser E and Van Den Berg B, 'Shielding Software Systems: A Comparison of Security by Design and Privacy by Design Based on a Systematic Literature Review' (2024) 52 Computer Law & Security Review 105933
- Dodds S, 'Dependence, Care, and Vulnerability' in Catriona Mackenzie, Wendy Rogers and Susan Dodds (eds), *Vulnerability* (Oxford University Press 2013)
- Duivenvoorde B, 'The Protection of Vulnerable Consumers under the Unfair Commercial Practices Directive' [2013] Journal of European Consumer and Market Law 69
- European Commission, 'Understanding Consumer Vulnerability in the EU's Key Markets' (2016) <https://commission.europa.eu/system/files/2018-04/consumer-vulnerability-factsheet_en.pdf> accessed 7 February 2025
- Ferretti F, 'The Consumer Image under EU Law: Average, Rationally Bounded and Dispositionally Vulnerable. What Are the Prospects for Protection in Digital Markets?' (2025) 62 Common Market Law Review 121
- Fineman MA (ed), 'The Vulnerable Subject: Anchoring Equality in the Human Condition' (2010) 20 Yale Journal of Law and Feminism 1
- Furnell S and Thomson K-L, 'Recognising and Addressing "Security Fatigue"' (2009) 2009 Computer Fraud & Security 7
- Galli F and Novelli C, 'The Many Meanings of Vulnerability in the AI Act and the One Missing' [2024] BioLaw Journal - Rivista di BioDiritto 53
- Gellert R, *The Risk-Based Approach to Data Protection* (1st edn, Oxford University Press 2020)
- , 'The Role of the Risk-Based Approach in the General Data Protection Regulation and in the European Commission's Proposed Artificial Intelligence Act: Business as Usual?' (2021) 3 Journal of Ethics and Legal Technologies 16
- Gennet É, Andorno R and Elger B, 'Does the New EU Regulation on Clinical Trials Adequately Protect Vulnerable Research Participants?' (2015) 119 Health Policy 925

- Goanta C, Gregorio GD and Spanakis J, 'Consumer Protection and Digital Vulnerability: Common and Diverging Paths' in Camilla Crea and Alberto De Franceschi (eds), *The New Shapes of Digital Vulnerability in European Private Law* (Nomos Verlagsgesellschaft mbH & Co KG 2024)
- Helberger N and others, 'Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability' (2022) 45 *Journal of Consumer Policy* 175
- Liu M, 'Digital Vulnerability: Rethinking Power Imbalances in the Digital Age' (2024) 32 *European Review of Private Law* 827
- Luna F, 'Elucidating the Concept of Vulnerability: Layers Not Labels' (2009) 2 *IJFAB: International Journal of Feminist Approaches to Bioethics* 121
- Malgieri G, *Vulnerability and Data Protection Law* (1st edn, Oxford University Press 2023)
- Malgieri G and Niklas J, 'Vulnerable Data Subjects' (2020) 37 *Computer Law & Security Review* 105415
- Mišćenić E, 'Information, Transparency and Fairness for Consumers in the Digital Environment' in Camilla Crea and Alberto De Franceschi (eds), *The New Shapes of Digital Vulnerability in European Private Law* (Nomos Verlagsgesellschaft mbH & Co KG 2024)
- Piasecki S, 'Expert Perspectives on GDPR Compliance in the Context of Smart Homes and Vulnerable Persons' (2023) 32 *Information & Communications Technology Law* 385
- Ranchordas S and Beck M, 'Vulnerability' in Mareile Kaufmann and Heidi Mork Lomell (eds), *De Gruyter Handbook of Digital Criminology* (De Gruyter 2025)
- Rebrean M-L and Malgieri G, 'Vulnerability in the EU AI Act: Building an Interpretation' *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency* (ACM 2025)
- Renaud K, Searle R and Dupuis M, 'Shame in Cyber Security: Effective Behavior Modification Tool or Counterproductive Foil?' *New Security Paradigms Workshop* (ACM 2021)
- Riefa C, 'Protecting Vulnerable Consumers in the Digital Single Market' (2022) 33 *European Business Law Review* 607
- Royle OR, 'Amazon Driver Breaks down the AI System Watching Them for Safety Violations like Drinking Coffee While Driving' (*Fortune*) <<https://fortune.com/2023/02/27/amazon-delivery-driver-breaks-down-ai-surveillance-in-vans/>> accessed 25 March 2025
- Teo SA, 'Artificial Intelligence, Human Vulnerability and Multi-Level Resilience' (2025) 57 *Computer Law & Security Review* 106134
- van 't Schip M, 'The Internet of Forgotten Things: European Cybersecurity Regulation and the Cessation of Internet of Things Manufacturers' (2025) 57 *Computer Law & Security Review* 106152
- Wiesemann C, 'On the Interrelationship of Vulnerability and Trust' in Christine Straehle (ed), *Vulnerability, Autonomy, and Applied Ethics* (Routledge 2016)

8.

Conclusion

In the autumn of 2025, a conflict emblematic of this dissertation took place just a few kilometres from my office. The scene of this conflict: Nexperia, a Chinese manufacturer headquartered in the Dutch city of Nijmegen. Nexperia is a semiconductor manufacturer; the company mainly produces basic chips for the car industry. In September 2025, the Dutch government seized control over Nexperia due to fears that Europe would be locked out of chip supply ‘in an emergency’.¹ A day later, the Dutch commercial court confirmed the seizure. For the seizure, the Dutch relied on a Cold War-era legal provision—one never used before. In response, the Chinese offices of Nexperia swiftly halted production, leading to panic among global carmakers: without Nexperia’s chips, modern cars cannot function.² The Nexperia case illustrates how interdependencies of digital products are emerging as a key battleground at the nexus of geopolitics, diplomacy, and economic security.

This dissertation analyses the EU legal framework concerning the cybersecurity risks of digital product interdependencies. It answers the following research question: ‘To what extent does, and how could, EU cybersecurity law address the cybersecurity challenges raised by the increasing interdependencies in digital products, as exemplified by Internet of Things devices?’ The six articles in this dissertation all approach this research question from a different perspective, but share a common conclusion: digital product interdependencies present complex and multi-faceted challenges. European cybersecurity law does not meet those challenges yet.

In this conclusion, I summarise the findings of the dissertation and answer the central research question. I summarise the articles along shared themes, instead of individually. Based on the main findings, I recommend several policy directions. Finally, I offer some perspectives for the future of this research topic.

1 Interdependence

This dissertation examines digital product interdependencies, their associated cybersecurity risks, and how European cybersecurity law addresses those risks. The below summary of the research findings therefore starts with the interdependence of digital products, followed

-
- 1 Lisa O’Carroll, ‘Netherlands Suspends State Seizure of Chinese Chipmaker Nexperia’ The Guardian (19 November 2025) <<https://www.theguardian.com/business/2025/nov/19/netherlands-suspends-seizure-china-chipmaker-nexperia>> accessed 24 November 2025.
 - 2 Lisa O’Carroll, ‘EU Carmakers “Days Away” from Halting Work as Chip War with China Escalates’ The Guardian (29 October 2025) <<https://www.theguardian.com/business/2025/oct/29/europe-carmakers-china-computer-chip>> accessed 24 November 2025.

by associated cybersecurity risks.³ In section 2, I discuss the extent to which European cybersecurity law addresses those risks.

1.1 Heterogeneity

Together, the preceding chapters illustrate that digital product interdependencies form a heterogeneous landscape, which ranges from open-source software to bankrupt IoT manufacturers. The digital product is, as illustrated in Figure 1 of chapter 1, merely the tip of the iceberg. This iceberg consists of a software (or data-driven) side and a hardware side—the articles mainly addressed cybersecurity risks arising out of the former.

Chapter 4 points to the heterogeneity of a component like ‘software’. Modern software ranges from entire operating systems to simple websites. Most commercial software is known as proprietary software, as the developer maintains sole access to and control over the source code. On the other hand, there is a wide range of software known as ‘open-source software’, which means that the software code is openly accessible, downloadable, and reproducible.⁴

The difference in these software development styles means that regulating software as a singular object is futile. Even within open-source software, important differences exist. Open-source software developers can work voluntarily on a passion project, but much software also stems from academic research, or even commercial funding. Open-source software can be a standalone product, or one intended for integration into other software packages. These differences show that the term ‘open-source software’ captures a varied landscape. If policy makers would regulate software as a homogeneous artefact, they would overlook the diverse palette that software is.

Manufacturers are equally heterogeneous entities, as Chapter 5 presents. A conventional hardware supplier differs significantly from an Internet of Things manufacturer; the latter holds much more control over the end product, even after delivery to the end user. An IoT device, for instance, often communicates with the manufacturer—or external cloud service under their control—to analyse or store data. In turn, if the IoT manufacturer ceases to exist, the device can no longer access that data. In many cases, this leads to the device becoming defunct. This is a problem for the IoT end user, but not for the end user of a conventional counterpart. These novel problems demonstrate the heterogeneity of manufacturers.

Consumers have a crucial role in the interdependencies of digital products, as Chapters 3, 6, and 7 confirm. In line with software and manufacturers, the consumer is not a singular entity, the simple end point of the product’s supply chain. Consumers use the product, rely on cloud services, and may return it to the production line when they require repairs. Chapters 3 and 6 highlight the diverse expectations that consumers may have regarding the privacy and security of their product. Interviewed consumers generally expect manufacturers to address security problems, such as by patching or recalling the product (Chapter 3). Moreover, consumers envision different product lifecycles depending on the product type—expectations differ significantly between a smart washing machine and a smartphone (Chapter 6). Both chapters show that consumers look towards the manufacturer for cybersecurity measures, particularly with regards to software patches. A number of variables shape these expectations, such as the

3 I do not cover each article—or discuss them in order—for each section below. I only summarise them when their findings cover that particular element.

4 Relying on the definition of open-source software established and maintained by the Open Source Initiative: <<https://opensource.org/osd>>

product type. The social-empirical analyses of Chapter 3 and 6 confirm that IoT consumers vary significantly. Moreover, when cybersecurity incidents occur, they remain dependent on the manufacturer.

Chapter 7 further builds on these consumer perspectives. The law often speaks of an ‘average consumer’. However, modern digital environments challenge this traditional benchmark, as they render certain individuals (more) vulnerable, for instance through personalised advertisement campaigns or addictive design. As interdisciplinary literature shows, human vulnerability can differ significantly between individuals, for instance due to socioeconomic status or digital literacy. The question is to which extent the average consumer benchmark remains apt—a question raised by the heterogeneity of consumers.

Digital products are the tip of the iceberg, veiling a heterogeneous landscape of interdependent actors and processes. This heterogeneity gives rise to various cybersecurity risks.

1.2 Cybersecurity risks

In Chapter 1 of this dissertation, I hold that the problems of digital product interdependencies centre around three key properties: complexity, control, and opaqueness. Throughout the articles of this dissertation, it becomes clear that the cybersecurity risks of digital product interdependencies centre around these same three properties.

Chapter 2 identifies cybersecurity risks from the perspective of supply chain cybersecurity. Modern cyber attacks focus on the weakest member in a supply chain, cascading from this initial access point to further (key) actors in the chain, or even the consumer. Supply chain cybersecurity forms the strategic response to such attacks—for instance by setting out standardised, collective cybersecurity measures for the entire chain.

Supply chain cybersecurity strategies demand visibility and transparency of the supply chain, so that experts can take targeted measures. This endeavour is stifled by the opaqueness of digital product interdependencies: experts struggle to identify interdependencies, which are often hidden in layered structures and unknown even to participating entities. In addition, supply chain cybersecurity strategies touch upon questions of control around key choke points, which are often managed by large technology companies. These choke points are the most critical elements of a supply chain and the most attractive points of attack for malicious actors. Finally, supply chain cybersecurity emerges as a strategic endeavour precisely because of the complexity of interdependencies: without clear strategic guidance, establishing a cybersecure supply chain is simply impossible. In sum, supply chain cybersecurity raises critical questions centred around the complexity, control, and opaqueness of digital product interdependencies.

The open-source software problems identified in Chapter 4 illustrate the opaqueness of digital product interdependencies. Open-source software holds a key function in the software ecosystem, but its integration into layers of other, possibly closed-source software packages veils its importance.

A vulnerability in an open-source software package can cascade to numerous commercial counterparts. This is not just a hypothetical issue, but one raised by existing cases, such as XZ Utils and Log4j. Indeed, open-source software is a common target of supply chain attacks because of its accessibility and criticality.⁵ At the same time, those attacks are often more easily

5 Marc Ohm and others, ‘Backstabber’s Knife Collection: A Review of Open Source Software Supply Chain Attacks’ in Clémentine Maurice and others (eds), *Detection of Intrusions and Malware*,

addressed due to the transparency of open-source software: the XZ Utils attack was prevented because a software developer started digging through the code to find out why it was suddenly using more computing power.

Open-source software therefore exemplifies the complex puzzle of digital product interdependencies. On the one hand, the software is more transparent than proprietary software about its inner workings, providing cybersecurity guarantees. On the other hand, developers are regularly unaware of their reliance on open-source software packages. There is also no incentive to lessen their reliance: adding a few extra packages bears no additional (financial) cost. But precisely because of this integration, cybersecurity problems become not only opaque, but also more critical.

Chapter 5 concerns the cybersecurity problems that may arise if a manufacturer ceases operations. It is common, especially in the IoT space, that the manufacturer ceases their operations; they may go bankrupt or disappear without clear reason.⁶

Indeed, the discontinuation of the manufacturer leads to the collapse of the interdependent ecosystem which they manage. For instance, the cloud service on which the manufacturer stores the end user's data can become inaccessible. The manufacturer's cessation therefore leads to cybersecurity risks for end users: they may lose their data, or their device may no longer be updated, rendering it vulnerable to cyber attacks. This is a novel concern stemming from modern product design, in which the end user depends on the manufacturer even after purchasing the product.

Cybersecurity problems are inherent in digital products. In essence, digital products are ecosystems: diverse entities are interdependent because of the production and functioning of a single digital product. But merely viewing these interdependencies as an ecosystem neglects individual, contextual concerns. This is demonstrated by components such as open-source software, or manufacturers that cease their operations. The question remains whether European cybersecurity law adequately addresses the risks both for the general digital product ecosystem and the individual, contextual components.

2 The limits of European cybersecurity law in the context of interdependencies

It is clear that the cybersecurity problems of digital product interdependencies are varied and complex. My description of this problematic landscape served as groundwork for the legal-doctrinal analysis, which focused on the extent to which European cybersecurity law addresses these problems. I examined this question across various legislative acts, mainly the NIS2 Directive and the Cyber Resilience Act.

Chapter 2 starts with a more general analysis, concerning the rules for supply chain cybersecurity in the NIS2 Directive. NIS2 applies to entities in critical sectors, such as hospitals; these entities must assess the cybersecurity risks for their organisation. As part of

and Vulnerability Assessment, vol 12223 (Springer International Publishing 2020); Piergiorgio Ladisa and others, 'SoK: Taxonomy of Attacks on Open-Source Software Supply Chains' 2023 IEEE Symposium on Security and Privacy (SP) (2023).

6 Respondents of the study in Chapter 6 actually noted their awareness of this dynamic, believing that IoT products may have a shorter lifespan because manufacturers can simply disappear.

this assessment, the entities must consider the supply chain security of their network and information systems.

The legislators chose to place supply chain security among a list of other requirements, which neglects the complexity of supply chain security. This complexity is rooted in the fact that academic and policy documents offer conflicting definitions of supply chain security. It is therefore unclear what the NIS2 Directive demands. Although the Commission elucidated some requirements in the Implementing Regulation,⁷ certain practical questions remain. For instance, given the opaqueness of digital product interdependencies, how should organisations identify entities in their multi-layered network?

Furthermore, as Chapter 2 argues, the NIS2 Directive has the wrong focus for tackling supply chain security, as its rules only apply to entities in critical sectors. In other words, NIS2 requires that entities, such as hospitals, take supply chain security measures for each ICT system they use: a complex task. The entity is simply the end user of a digital product; end users generally do not oversee the supply chain of their devices. Most likely, entities can merely add some contractual requirements when purchasing new systems. The obligation should thus lie with the product's manufacturers, instead of with entities in critical sectors.

Moving towards entity-specific questions, Chapter 4 analyses how the particularities of open-source software affected the regulatory framework of the Cyber Resilience Act. The initial Commission proposal for this Act regulated all software equally. This meant that all software developers had to comply with similar demands, including possible third-party audits.

Open-source software developers often have fewer financial and organisational means than commercial developers. This proposal therefore led to widespread concern among the open source community, as strict cybersecurity requirements would raise significant barriers to open-source software development.

In the end, the European Council and Parliament amended the proposal and subjected open-source software developers to a more relaxed regulatory regime. However, the chapter shows that such a hands-off approach could, in turn, overlook the impact of cybersecurity vulnerabilities in open-source software. This difficult regulatory balance reflects on the regulation of digital product interdependencies broadly: open-source software is just a single cog in the wheel of digital products; a single cog that already demands proper regulatory choices.

Chapter 5 shows that European cybersecurity law contains comprehensive rules for device manufacturers. At first sight, the rules seem sufficiently broad to cover all types of manufacturers. However, faced with unique problems, such as manufacturers ceasing their operations, cybersecurity law seems to lack sufficient flexibility. Update obligations—which hold the manufacturer responsible for continued device support—are no longer enforceable when the manufacturer ceases to exist. Under the Cyber Resilience Act, manufacturers must merely notify market authorities about their cessation. Other than this small obligation, the CRA lacks enforceable obligations for manufacturers ceasing their operations.

Regulatory creativity is necessary, given the responsibility vacuum presented by manufacturer cessation. Regulators must ensure that manufacturers act pre-emptively, so that they have procedures in place *if* they cease their operations. These measures must be manufacturer-independent, to prevent falling into the same responsibility fallacy as update obligations.

⁷ Released after the publication of the journal article of Chapter 2.

In this context, interoperability and open-source software are promising manufacturer-independent solutions. The inclusion of these solutions in policy would provide benefits beyond manufacturer cessation; interoperability and open-source software can support broader efforts to offer end users more control over and insight into the functioning of their digital product.

The same context-specific measures are required when we look at consumers. Chapter 3 and 6 analyse what consumers expect. Across various degrees, those chapters indicated that consumers depend on the manufacturer when security incidents occur. If a product does not provide the security that a consumer expects, the manufacturer is liable under the Product Liability Directive (Chapter 3). The Product Liability Directive is directly connected to the Cyber Resilience Act.⁸ Moreover, the Cyber Resilience Act mandates that manufacturers consider these consumer expectations when they determine the product's support period (Chapter 6). Therefore, the Cyber Resilience Act creates an interdependent dynamic: the consumer depends on the manufacturer for cybersecurity measures, but the manufacturer depends on the consumer in setting certain standards, such as product support periods. In the future, the expectations identified in Chapters 3 and 6 may shape the practical relevance of the Product Liability Directive and the Cyber Resilience Act respectively.

Chapter 7 analyses how the Cyber Resilience Act aims to protect vulnerable consumers. This aim is included in the CRA's preamble, but there is no further reference to it in the actual legal text. It is therefore unclear how the CRA relates to vulnerable consumers.

There are two dominant ontological approaches to human vulnerability: universal and layered. Universal vulnerability refers to the type of vulnerability that is present in being human. For instance, all humans share a vulnerability to diseases. Still, certain (groups of) individuals carry multiple layers of vulnerabilities, such as a child with a learning disability. These individual differences are captured in the layered theory, which emphasises the need for individual or contextual approaches.

Chapter 7 shows that the CRA moderately mitigates universal vulnerabilities. This is especially evident through the lens of the power imbalances between manufacturers and consumers. The CRA aims to mitigate such power imbalances in two ways: first, by raising the cybersecurity demands of products (e.g., security-by-design) and, second, by improving consumer knowledge of the device through information obligations. At the same time, 'empowering' the consumer with more information also burdens them with the idea of having to understand the information provided and acting accordingly, such as by changing default settings for more security.

The CRA barely adopts a layered view of consumer vulnerability. First, consumer vulnerability is not an element of the cybersecurity risk assessment. Manufacturers hence do not have to consider if their consumers may be rendered (more) vulnerable by their product. Second, the CRA classifies certain products specifically as high risk, but these classifications only focus on specific products with specific vulnerable consumers. As such, wearables for children are high-risk products, but products for children in general are not. Taken together, the Cyber Resilience Act again covers mostly the default notion—a general consumer—instead of allowing for a more contextual approach.

8 See Recital 31 CRA.

3 Answering the research question

In this dissertation, I answer the following research question:

To what extent does, and how could, EU cybersecurity law address the cybersecurity challenges raised by the increasing interdependencies in digital products, as exemplified by Internet of Things devices?

My answer to this central question is as follows.

Although EU cybersecurity law provides some rules in relation to cybersecurity risks of digital product interdependencies, it *does not* sufficiently address them. When faced with problems that stretch beyond the familiar, such as open-source software or vulnerable consumers, EU cybersecurity law is not sufficiently flexible.

At the same time, EU cybersecurity law *could*, in principle, adequately address challenges presented by digital product interdependencies. Digital product interdependencies are a complex, multi-headed problem. More visibility, control, and understanding over the multi-headed nature of these interdependencies is necessary. To achieve this aim, policy makers should develop a legal framework that encompasses the heterogeneity of this interdependent ecosystem. Moreover, interoperable and open-source components can help European cybersecurity law address some challenges of digital product interdependencies. Based on these options, I offer the following policy recommendations—extending to (EU) legislators, technical experts, and (supply chain) practitioners alike.

- Recommendation 1: The identification of digital product interdependencies is crucial for further policy work

This dissertation highlighted across various sectors how heterogeneous digital product interdependencies are: open vs. closed-source software; manufacturers that cease to exist; vulnerable consumers using the product—all have different risks, demands, and capabilities. But if these interdependencies remain hidden beneath the surface, in layered structures of which policy makers and practitioners remain unaware, addressing them is impossible. It is crucial that digital product interdependencies are brought to light.

Certain developments already support the identification of interdependencies. One of those developments is the incursion of the ‘Software Bill of Materials’ (SBOM). The SBOM is a technology for listing all the software dependencies of a single software package. This overview can, for instance, indicate which dependencies need to be updated. However, SBOMs currently suffer from low adoption rates among developers, which complicates relying on data from other software vendors: the lower the adoption rate, the lower the quality of the software data in the SBOM. In response to this low adoption rate, the Cyber Resilience Act and a recent US Executive Order mandate the adoption of the SBOM for a variety of software products.⁹ The SBOM may therefore be the first regulatory tool that brings light to the opaque world of interdependencies.

9 Annex I Part II(1) CRA: ‘Manufacturers of products with digital elements shall: [...] [draw] up a software bill of materials [...] covering at the very least the top-level dependencies of the products.’ US Executive Order 14028 ‘Improving the Nation’s Cybersecurity’, section 4(e)(vii) and section 10(j).

Policy makers cannot address cybersecurity risks if digital product interdependencies remain obscured. Upcoming developments like the SBOM can offer fruitful groundwork for more transparent dependencies, but more work is necessary. The identification of digital product interdependencies must serve further policy that tackles the cybersecurity dynamics of digital product interdependencies, bringing me to my second recommendation.

- Recommendation 2: EU cybersecurity law should focus on a combination of: i) a general rule addressing digital products as ecosystems and ii) concrete norms focused on critical components

Through the interconnection of diverse systems, actors, and processes, cybersecurity problems now ripple through entire product ecosystems. In order to tackle these ripple effects, policy makers must acknowledge that cybersecurity measures require an ecosystem approach—that is, a holistic set of measures aimed at addressing insecurity across digital product interdependencies.¹⁰ This ecosystem mindset diverges from the New Legislative Framework ethos, which focuses largely on the security of individual products. An ecosystem approach goes beyond stating that ‘all products on the European market must be secure’. Instead, regulators understand that digital products are mere parts of a whole: it is the ecosystem in which they operate that must be secure.

This is not to disregard the need for individual measures. To strengthen the overall ecosystem, certain individual products demand regulatory specificity: simply regulating all software or hardware as a singular product type, or all consumers as a unified concept, does not suffice. In environmental terms, we must protect both ecosystems and individual organisms.¹¹

A combination of overarching principles with individualised measures follows an established regulatory culture for law and technology. In 2006, Koops stated that ‘open-ended formulations and a mixed approach of abstract and concrete rules that are periodically evaluated’ can offer legal certainty for both current and future technologies.¹² Indeed, I recommend that the ecosystem approach forms the broader, open-ended formulation, while specific measures, for example for open-source software, offer more concrete rules. This balance will, as in 2006, require constant evaluation of digital product interdependencies.

There is already some groundwork for this regulatory approach in European cybersecurity law. The supply chain security rules in the NIS2 Directive contain some components of an ecosystem approach. If critical entities can only use products with a secure supply chain, manufacturers of such products are more likely to offer supply chain security as a product feature. Consequently, a ripple effect can emerge, where manufacturers impose minimum cybersecurity standards on all their suppliers, who then require the same standards from their own suppliers, and so forth.¹³ In principle, such a ripple effect would establish a more secure ecosystem of digital

10 On the ecosystem approach in environmental law, see also Froukje Maria Platjouw, *Environmental Law and the Ecosystem Approach* (Routledge 2016) ch 2.

11 See also *ibid* 25.

12 EJ Koops, ‘Should ICT Regulation Be Technology-Neutral?’ in BJ Koops and others (eds), *Starting Points for ICT Regulation* (TMC Asser Press 2006).

13 See also the recommendations made by ENISA, the European Union Agency for Cybersecurity, on this topic: European Union Agency for Cybersecurity, *Good Practices for Supply Chain Cybersecurity*. (Publications Office 2023) <<https://data.europa.eu/doi/10.2824/805268>> accessed 15 January 2024.

products. This approach, though, is only mentioned in the Recitals of NIS2, which do not have legal power themselves. Whether this effect of NIS2 will materialise remains to be seen.

The Cyber Resilience Act connects to the ecosystem approach by mandating that manufacturers must exercise ‘due diligence’ in the integration of third-party components.¹⁴ Unfortunately, once more, the practical impact of this requirement remains uncertain. Courts and supervisory authorities will have to flesh out the meaning of the abstract ‘due diligence’ norm. Regardless, it seems unlikely that manufacturers must fully consider their interdependencies under this diligence requirement. Moreover, this dissertation demonstrates that the Cyber Resilience Act has certain gaps, for instance regarding manufacturers that cease operations. Such legal uncertainty regarding the scope of the Cyber Resilience Act will only further dilute the due diligence obligation. A stricter principle regarding the ecosystem of the digital product is necessary.

Policy makers must re-evaluate the current focus on individual products in the New Legislative Framework. As mentioned above, instead of requiring products to comply with a set of cybersecurity requirements,¹⁵ the principle of European cybersecurity law should be that all products are part of a secure ecosystem. This principle could form a duty of care for manufacturers vis-à-vis consumers—just as states must protect their ecosystems to protect nature and, as a result, their citizens. If this regulatory shift is a step too far, there are more nuanced options available: the NIS2 Directive could be more specific with regards to supply chain security and the ecosystem of critical entities, while the CRA could move beyond a ‘due diligence’ rule towards strict requirements of ecosystem cybersecurity.

In sum, the future of European cybersecurity law lies somewhere between principle-based and rule-based norms—a recurring conclusion for EU digital policy. On a general level, it is necessary that policy makers introduce a new ethos, which focuses on the security of digital product ecosystems—not on digital products individually. Regulators should complement this novel general approach with concrete norms for components that warrant individual attention, for example because of specific cybersecurity concerns.

- Recommendation 3: Promote the development of interdependent software and hardware components that offer choice and control, through open-source and interoperable components

Finally, when viewing interdependencies, I believe that policy makers should give more attention to interoperable and open-source components. The reason is simple: open-source products and interoperability allow for more control and visibility of a product’s interdependencies.

Open-source components are inherently about visibility. The source code is in principle visible to the end user and to other developers, who can know what they are incorporating into their product. This is true for software, but also for hardware components, where product developers share their designs so others can freely re-create them. The XZ Utils case not only showed the cybersecurity risks of open-source components, but also their benefits: anyone can audit the code and make changes when desired. This transparency is what prevented the XZ Utils backdoor from materialising. Next to transparency, end users are in control when using open-source components, with licenses that allow for free use, modification, and sharing. Indeed,

14 Art 13(5) CRA.

15 See Art 6(a) CRA.

the EU is working on a strategy for ‘European open digital ecosystems’; the Commission recently stated that open-source software is vital to achieving these ecosystems, as it provides ‘user agency’, ‘control’, and the ‘resilience of our digital infrastructure’.¹⁶ The findings of this dissertation emphasise these statements and the need for a structural embedding of open-source components within cybersecurity policy work.

Additionally, interoperable components allow for more control over the digital product. End users, for instance, can easily swap out components when they desire and therefore identify which components fit their use case best. The Digital Markets Act already mandates such interoperability, for instance: if one messaging service does not provide desired privacy and cybersecurity standards, consumers can easily switch to another and retain their communication with individuals across other services.¹⁷ Policy makers must ensure that such ambitions persist—embedding interoperability in product design will offer a degree of control over digital products currently unattainable.

To address the cybersecurity risks arising out of digital product interdependencies, we must critically examine the individual components that together create this interdependent ecosystem. In this dissertation, it became clear that components exist that offer a degree of choice and control to end users: open-source and interoperable components. The only barrier to achieving a more open, interoperable digital ecosystem is stronger regulatory embedding.

4 Outlook for the future

During the writing of this dissertation, a deluge of supply chain attacks occurred. ENISA, the European Agency for Cybersecurity, considers supply chain attacks one of the key cybersecurity threats of the future.¹⁸ It seems inevitable that attention to the risks of digital product interdependencies will continue to rise on the academic and political agenda. In this dissertation, I could only cover a small selection of the many aspects of this topic. Therefore, on the basis of the limitations of this dissertation, I offer an outlook of future research directions.

4.1 Limitations

This dissertation focuses on EU cybersecurity law and therefore the analysis was limited to a specific jurisdiction and legal field. Certainly, there are also important approaches to the risks of digital product interdependencies outside this jurisdiction and outside cybersecurity law.

In terms of jurisdiction, the EU legislators are not alone in regulating cybersecurity. Most regulation outside the EU, however, still consists of soft law approaches, such as guidance

16 European Commission, ‘Call for Evidence – Towards European open digital ecosystems’, Ares (2026)69111.

17 Art 7 Digital Markets Act.

18 European Union Agency for Cybersecurity, Foresight Cybersecurity Threats for 2030 (Extended Report) (Publications Office 2024).

by cybersecurity authorities.¹⁹ Further development of cybersecurity law globally will—hopefully—accompany an equal rise in attention to topics related to interdependencies.

This dissertation barely discussed regulatory responses outside cybersecurity law. For example, as just shared in the recommendations, researchers could approach supply chain cybersecurity as a contractual issue: if organisations include a contractual clause that their suppliers must attain a certain level of cybersecurity, it is likely that this requirement cascades downstream.²⁰ In turn, the entire supply chain follows the organisation's standards. Investigating these and similar legal approaches, such as the role of cybersecurity in tenders, fell outside the scope of this dissertation but certainly warrant further research.

This dissertation misses some of the cybersecurity risks arising out of digital product interdependencies. This topic is simply too comprehensive for one dissertation. For instance, I did not discuss the use of IoT devices at manufacturing sites, the 'Industrial Internet of Things', which may present some unique cybersecurity risks (e.g., machinery overheating after an attack). I deliberately exempted some of these sectors and associated risks, but I must admit that there are most likely many that I remain unaware of.

Finally, the digital product ecosystem extends beyond what I presented here. This dissertation mostly concerned the software/data side of the digital product iceberg. Many significant components of a modern digital product lie outside that scope, such as undersea cables, lithium batteries, and chips/semiconductors. Even within the software/data side, I neglected some crucial components, such as 5G communication networks and domain name servers. One could write an entire dissertation about each of these respective components—which is why I could not cover them here.

4.2 The future is interdisciplinary

This dissertation is the labour of interdisciplinarity. Throughout this doctoral track, I had the pleasure and benefit of working at the 'Interdisciplinary Hub for Society and Digitalisation' (iHub) at Radboud University. Colleagues from various disciplines enlightened me with insights about this intricate topic and helped me foray into parts unknown. Of course, problems related to digital product interdependencies are the subject of a range of disciplines—the future of this research topic is, indeed, multi- and interdisciplinary.

Supply chain cybersecurity concerns, for example, largely originated in business management research. In the end, supply chains aim to produce economic goods and services. Recent incidents highlight the economic impact that cyber attacks have: they can halt entire production chains, leading to serious business problems.²¹ Furthermore, these attacks illustrate how

19 Japan and Singapore form an exception (although with limited scopes to their regulation), see Nicholas Seng, 'Cybersecurity Regulation—Types, Principles, and Country Deep Dives in Asia' (2024) 5 *International Cybersecurity Law Review* 387; On the USA, see Elaine Fahey, 'The Evolution of EU-US Cybersecurity Law and Policy: On Drivers of Convergence' (2024) 46 *Journal of European Integration* 1073; On the UK, see Betül Gokkaya, Konstantina Spanaki and Erisa Karafili, 'Strengthening the UK Regulatory Framework: Enhancing Cybersecurity in Supply Chains' (2025) 5 *International Journal of Information Management Data Insights* 100370.

20 See also Recital 85 NIS2 Directive: 'Essential and important entities should in particular be encouraged to incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers.'

21 Jasper Jolly and Dan Milmo, 'Inside the Jaguar Land Rover Hack: Stalled Smart Factories, Outsourced Cybersecurity and Supply Chain Woes' *The Guardian* (20 September

proper supply chain cybersecurity is a novel business management task. This dissertation, for instance, called for increased visibility of supply chains—a task that most likely falls to business managers. In sum, there is plenty of reason for further business management studies on digital product interdependencies.

Inherently, cybersecurity is a topic illuminated by information security researchers. The various cybersecurity problems highlighted in this dissertation all stem from such research. I relied on studies that empirically measured the rise of supply chain attacks on open-source software, studies that examined how to keep devices functional even without access to manufacturer's cloud servers, and studies detailing the impact of cybersecurity incidents for vulnerable individuals. This body of work already supported this dissertation and will only grow in importance in the future. Digital products are forever the subject of change. As new interdependent actors enter the stage, such as AI providers, information security research will remain crucial in understanding novel attack vectors and appropriate policy responses.

Digital product interdependencies are equally a political science topic, as evident by digital sovereignty policies. Moreover, many states exploit the interdependence of digital products to achieve political goals. The semiconductor industry, for instance, is one of the main defence mechanisms for Taiwan vis-à-vis China, as Taiwan hosts the largest global semiconductor manufacturer, TSMC. A Chinese invasion of Taiwan will inevitably impact the production capacity of TSMC, in turn impacting virtually every digital product globally.²² For other states, a Chinese invasion of Taiwan would therefore lead to the collapse of their digital infrastructure; a more than sufficient reason to protect Taiwan against Chinese aggression. Supply chains and their cybersecurity are therefore contested geopolitical landscapes. Political science studies elucidate the governance and power structures within these landscapes and how they shape digital product interdependencies.

Finally, digital product interdependencies are a subject of science and technology studies (STS). A supply chain, for instance, is itself a technological artefact, one defined by social, cultural, and historical contexts. The sociotechnical perspective of STS can help us understand the labour conditions across a supply chain, or how data centres influence local communities. STS can contribute to visualising the interdependencies themselves, but also their local, cultural, political, or social impact.

The need for interdisciplinary future work ranges across economic and business studies, information security studies, political science and STS—but there are other fields that bring novel and beneficial approaches to the topic of digital product interdependencies. Studies related to artificial intelligence may help contextualise the incessant rise of this technology in modern digital products, where philosophers can help build an ontology of interdependence that aligns with digital products. The study of digital product interdependencies is simply interdependent itself.

2025) <<https://www.theguardian.com/business/2025/sep/20/jaguar-land-rover-hack-factories-cybersecurity-jlr>> accessed 22 September 2025.

22 Chris Miller, *Chip War: The Fight for the World's Most Critical Technology* (Scribner 2022).

References

- European Union Agency for Cybersecurity, *Good Practices for Supply Chain Cybersecurity*. (Publications Office 2023) <<https://data.europa.eu/doi/10.2824/805268>> accessed 15 January 2024
- , *Foresight Cybersecurity Threats for 2030 (Extended Report)* (Publications Office 2024)
- Fahey E, ‘The Evolution of EU–US Cybersecurity Law and Policy: On Drivers of Convergence’ (2024) 46 *Journal of European Integration* 1073
- Gokkaya B, Spanaki K and Karafili E, ‘Strengthening the UK Regulatory Framework: Enhancing Cybersecurity in Supply Chains’ (2025) 5 *International Journal of Information Management Data Insights* 100370
- Jolly J and Milmo D, ‘Inside the Jaguar Land Rover Hack: Stalled Smart Factories, Outsourced Cybersecurity and Supply Chain Woes’ *The Guardian* (20 September 2025) <<https://www.theguardian.com/business/2025/sep/20/jaguar-land-rover-hack-factories-cybersecurity-jlr>> accessed 22 September 2025
- Koops EJ, ‘Should ICT Regulation Be Technology-Neutral?’ in BJ Koops and others (eds), *Starting Points for ICT Regulation* (TMC Asser Press 2006)
- Ladisa P and others, ‘SoK: Taxonomy of Attacks on Open-Source Software Supply Chains’ 2023 *IEEE Symposium on Security and Privacy (SP)* (2023)
- Miller C, *Chip War: The Fight for the World’s Most Critical Technology* (Scribner 2022)
- O’Carroll L, ‘EU Carmakers “Days Away” from Halting Work as Chip War with China Escalates’ *The Guardian* (29 October 2025) <<https://www.theguardian.com/business/2025/oct/29/europe-carmakers-china-computer-chip>> accessed 24 November 2025
- , ‘Netherlands Suspends State Seizure of Chinese Chipmaker Nexperia’ *The Guardian* (19 November 2025) <<https://www.theguardian.com/business/2025/nov/19/netherlands-suspends-seizure-china-chipmaker-nexperia>> accessed 24 November 2025
- Ohm M and others, ‘Backstabber’s Knife Collection: A Review of Open Source Software Supply Chain Attacks’ in Clémentine Maurice and others (eds), *Detection of Intrusions and Malware, and Vulnerability Assessment*, vol 12223 (Springer International Publishing 2020)
- Platjouw FM, *Environmental Law and the Ecosystem Approach* (Routledge 2016)
- Seng N, ‘Cybersecurity Regulation—Types, Principles, and Country Deep Dives in Asia’ (2024) 5 *International Cybersecurity Law Review* 387

A.

Appendix

Table 1: Regression models predicting 1) Appropriateness of manufacturer response, 2) Likelihood of manufacturer response, and 3) Suitableness of user response with the vignette factors; Device, Security / Privacy Event, Manufacturer response, and User response. Each model was run separately for security and for privacy. Scale of measurement: For Model 1, 2, 5, and 6: 7-point Likert scale with 1 = 'Strongly disagree' and 7 = 'Strongly agree' to the statement 'The manufacturer's response to the situation is appropriate considering the circumstances.' or 'Alex's response is a suitable way to move forward from this situation.'. For Model 3 and 4: 7-point Likert scale with 1 = 'Extremely unlikely' and 7 = 'Extremely likely' to the statement 'If you had to predict, how likely do you think a real manufacturer would respond this way considering the circumstances?'. For Model 1, there were slight regional differences, where participants from Central and South America rated manufacturer responses significantly more appropriate on average than participants from North America (Coefficient = 0.45, SE = 0.20, p<0.05). Other participant characteristics (Age, Gender, Count of used IT device) did not show an effect. We only present statistically significant interaction terms here for space considerations.

Regression tables		Appropriateness ratings		Likelihood ratings		User suitability ratings	
Coefficient	Model 1: Security Estimate Std. Error	Model 2: Privacy Estimate Std. Error	Model 3: Security Estimate Std. Error	Model 4: Privacy Estimate Std. Error	Model 5: Security Estimate Std. Error	Model 6: Privacy Estimate Std. Error	
Intercept	1.65 *** 0.14	2.61 *** 0.12	3.80 *** 0.14	4.52 *** 0.08	3.15 *** 0.15	4.63 *** 0.11	
Device:							
Connected car	0.30 0.17	-0.03 0.14	0.27 0.19	0.05 0.08	-0.35 0.18	-0.34 *** 0.08	
Smart speaker	0.05 0.16	-0.07 0.15	0.19 0.18	0.20 * 0.08	0.06 0.17	-0.12 0.08	
Smart washing machine	0.64 *** 0.17	-0.08 0.14	0.54 *** 0.19	0.12 0.08	-0.26 0.18	-0.03 0.08	
Smartphone	0.39 * 0.17	-0.07 0.15	0.15 * 0.19	0.21 ** 0.08	0.07 0.18	-0.22 ** 0.08	
Smartwatch	0.32 0.16	-0.04 0.15	0.28 0.18	0.13 0.08	0.36 * 0.18	-0.06 0.08	
Security camera (reference)							
Security/ Privacy Event:							
IoT ransomware	-0.10 0.06		-0.02 0.07		0.16 ** 0.06		
Unauthorized data access	-0.01 0.06		0.05 0.07		0.08 0.06		
DDoS (reference)							
Forced data collection		0.19 0.15		0.16 * 0.06		0.47 *** 0.14	
Third party sharing		0.44 ** 0.15		0.15 ** 0.06		-0.04 0.13	
No consent (reference)							
Manufacturer response:							
(Sec) Inform users	2.37 *** 0.19		1.02 *** 0.19		0.30 0.18		
(Sec) Recall	4.21 *** 0.19		1.14 *** 0.19		-0.17 0.17		
(Sec) Patch	3.54 *** 0.19		1.89 *** 0.18		0.45 * 0.18		
(Sec) No response (reference)							
(Priv) Inform via privacy policy		2.14 *** 0.06		0.56 *** 0.06		0.34 *** 0.07	
(Priv) Privacy S-W update		2.12 *** 0.06		0.47 *** 0.05		0.18 ** 0.06	
(Priv) No response (reference)							
User response:							
Advice online forums					2.01 *** 0.09	0.58 *** 0.13	
Return device					2.65 *** 0.09	0.87 *** 0.12	
Tech. mitigation					1.73 *** 0.09	0.58 *** 0.13	
Turn off					1.95 *** 0.09	0.77 *** 0.13	
Keep using (reference)							
Interaction Effects:				None found			
ManuResp*Device:							
Inform*Car (-0.75 **)		Car*Forced (0.43 **)		Recall*WashMachi (-0.89 ***)	ManuResp*Device:	Event*UserResp:	
WashMachi (-0.51 *)		WashMachi*Forced (0.78 ***)		Patch*WashMachi (-0.69 *)	Inform*Smartwatch (-0.81 **)	Forced*Return (-0.82 ***)	
Smartphone (-0.65 **)		Smartphone*Forced (0.57 **)			Recall*Car (0.54 *)	Forced*TurnOff (-0.98 ***)	
Recall*WashMachi(-0.63 **)		Smartwatch*Forced (0.65 **)			Patch* Smartphone (-0.98 ***)		
Smartphone (-0.87 **)							
Conditional R ² :	0.602	0.464	0.217	0.248	0.306	0.172	
ICC:	0.15	0.18	0.09	0.22	0.05	0.11	

* p<0.05 ** p<0.01 *** p<0.001

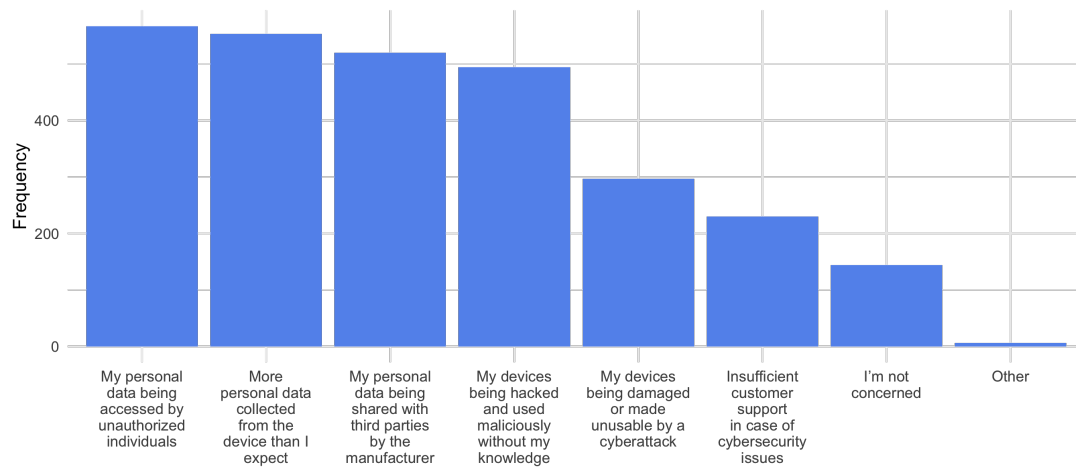


Figure 1: Respondents' concerns relating to security and privacy risks with their smart devices. The order of the options was randomized. Multiple choices were possible.

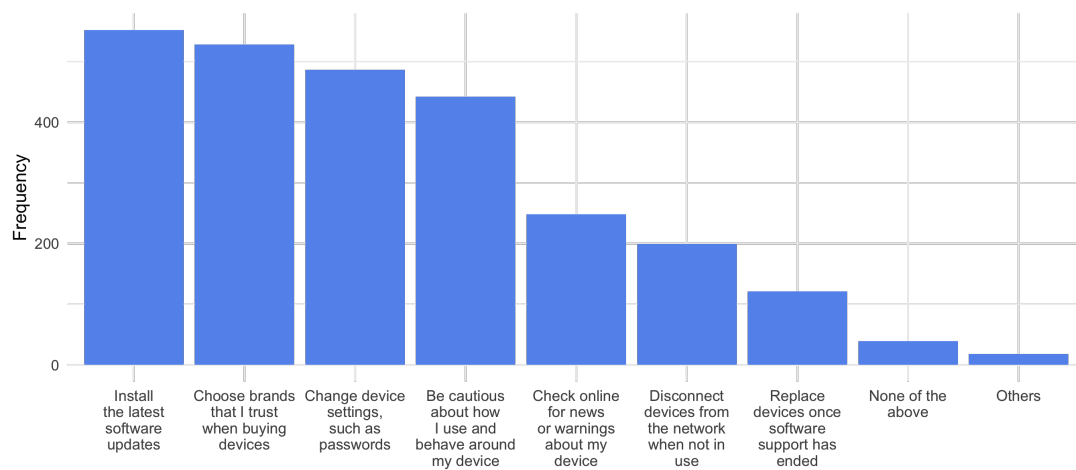


Figure 2: Respondents' mitigation behaviors relating to their security and privacy concerns with their smart devices. The order of the options was randomized. Multiple choices were possible.

Survey Instrument

Survey description as advertised on Prolific:

In this survey, we would like to learn about how you use smart devices and your general thoughts about such products. It will take approximately 18 minutes to complete. We will ask you some questions about any smart devices you are currently using and show you several descriptions of different smart devices to learn about your thoughts about them. These questions will not test your performance in any way, as we are only interested in your perspective. The survey will also ask for basic demographic information like age, gender, occupation, and country of residence.

Q1: Introduction In this survey, we want to learn your opinions on smart devices. There will be no right or wrong answers - we are only interested in your experiences and your opinion of these products. But what exactly are smart devices? A growing number of physical things around us are being equipped with electronic capabilities and connected to the internet and apps. Examples of such devices are smart speakers with voice assistants, smart security cameras, smart thermostats, or smartwatches. These devices have several features in common: They have sensors that collect information around them, like microphones, video cameras, a thermometer, or GPS. They can be connected to the internet, for example, via WiFi or cellular networks. Thus, they can communicate with other devices, mobile apps, or services. They provide features that would not be possible if they were not connected.

Q2: Device usage Which of the following types of smart devices do you own and use? Please select from the list below.

Smartphone, Smartwatch and/ or fitness tracker, Smart TV, Smart speaker with voice assistant (e.g., Amazon Echo or Google Nest), Media streaming device (e.g., Chromecast or music streamer), Smart lighting (smart light bulbs, light switches), Smart hub, Robot vacuum cleaner, Smart washing machine, Smart fridge, Smart baby monitor,

Internet connected security camera (indoor and / or outdoor), Smart video doorbell, Smart door-lock, Smart sensor (e.g., smoke detector, motion detector, air quality sensor), Smart thermostat, Wi-Fi solar inverter, Printer with internet / WiFi connection, Internet router, Other(s);,None of the above

Q2.1: Device model/brand We selected some of the smart device types you previously indicated to own. For each of them, please indicate the specific device's brand and/or model you are currently using. If you are using multiple devices of the same type (e.g., several different cameras), please pick one and focus your answers on that device.

Brand and/or model name, I don't know (For a list of three randomly chosen devices from Q2)

Q2.2: Start usage When answering the following questions, please focus on these specific smart device models you just described (e.g., the exact smartphone you are currently using), rather than the general device type (e.g., smartphones in general).

For the particular device you are currently using, when did you start using it, as far as you can recall? Please select the year.

2024, 2023, 2022, 2021, 2020, 2019, 2018, 2017, 2016, 2015, 2014 or earlier, I don't know (For the list of the previous devices)

Q2.3: Condition For the particular device you are currently using, was it new or previously owned (second-hand) when you started using it? *New, Previously owned, I don't know* (For the list of the previous devices)

Q2.4: Purchase channel Where was the device you are currently using purchased from?

Online store, Physical store, I don't know, It wasn't purchased (For the list of the previous devices)

Q2.5: Shop What is the name of the store where the device was purchased?

Shop name, I don't know (For the list of the previous devices)

Q2.6: Future use Looking ahead, for approximately how many more years do you plan to keep using the particular device you are currently using?

Less than a year, 1 year, 2 years, 3 years, 4 years, 5 years, 6 - 10 years, More than 10 years, I don't know (For the list of the previous devices)

Q2.7: Motivation for planned end of use

You indicated that you are planning to not use some of the devices for much longer. Why do you plan to stop using them soon? Please select the choices that best describe your reasons.

Experiencing issues and flaws with it, Desire for a newer device, Dissatisfied with brand or manufacturer, Concerns about my data, Concerns about cybersecurity, Software update support ended, Incompatible with other devices and/or services, I don't know, Other reasons (For the previous devices planned to be used for less than a year)

Q2.8. Update status Does the particular device you are currently using still receive software updates, as far as you know? (This refers to updates to the device itself, not any companion app or third-party apps running on the device.)

Yes, it still receives software updates, No, it no longer receives software updates, I don't know if it still receives software updates (For the list of the previous devices)

Q3: Attention check Please select 'Agree' for both Smart Washing Machine and Smart-watch. This is an attention check.

Q4: Recently stopped devices Now we would like to learn about any smart devices that you have recently stopped using, for instance to replace them.

Q4.1: Devices Have you recently stopped using any smart devices? Please select the type of the smart device you stopped using. If you haven't, just select "None of the above".

Smartphone, Smartwatch and/ or fitness tracker, Smart TV, Smart speaker with voice assistant (e.g., Amazon Echo or Google Nest), Media streaming device (e.g., Chromecast or music streamer), Smart lighting (smart light bulbs, light switches), Smart hub, Robot vacuum cleaner, Smart washing machine, Smart fridge, Smart baby monitor, Internet connected security camera (indoor and / or outdoor), Smart video doorbell, Smart door-lock,

Smart sensor (e.g., smoke detector, motion detector, air quality sensor), Smart thermostat, Wi-Fi solar inverter, Printer with internet / WiFi connection, Internet router, Other(s);, None of the above

Q4.2: Past use duration For approximately how many years did you use the device in total? If you stopped using more than one device of the same type (e.g., several different cameras), please pick one and focus your answers on that device.

Less than a year, 1 year, 2 years, 3 years, 4 years, 5 years, 6 - 10 years, More than 10 years, I don't know (For the list of three randomly chosen devices from Q4.1)

Q4.3: Action with old device What did you do with the device once you stopped using it? Please select the option that best describes your action.

Sold it, Returned it, Discarded it, Traded it in, Gifted it, Still have it but not in use, I don't know, Something else (For the list of the previous devices)

Q4.4: Motivation Why did you stop using the device? Please select the choice(s) that best describe your reasons. Multiple answers are possible.

It stopped working, Experiencing issues and flaws with it, Desire for a newer device, Dissatisfied with brand or manufacturer, Concerns about my data, Concerns about cybersecurity, Software update support ended, Incompatible with other devices and/or services, I don't know, Other reasons (For the list of the previous devices)

Q5: Device vignettes In the following, you will read short descriptions of three different conventional and smart devices. For each one, we will ask you how long you expect such a device to last. When answering, please imagine you are buying such a device today. Realistically, for how many years would you expect it to last under normal intensity of use until it cannot be used for its intended purpose anymore?

Q5.1: Vignette conventional device

A washing machine. It has different washing

programs for different textiles that the user can select on the machine's buttons

Q5.1.1: Expected lifetime If you had to predict, for how many years do you expect such a device to last? Please write your answer as a number in the field below.

(Open text field for integer text input)

Q5.1.2: Factors considered What aspects did you take into account when estimating the number of years? *(Open text field)*

The other devices vignettes:

A home printer. It can print documents in different formats and colors and can be connected to a computer with a cable to receive print jobs.

A vacuum cleaner. It can be used to clean the home's floor and has different suction strengths for different surfaces, which can be selected on the machine's buttons.

A thermostat. It is installed in the home's heating system and can be used to adjust the home's temperature on the thermostat's controls to set the desired temperature.

A smoke detector. It can continuously monitor the home's air for smoke and potential fire hazards and alert occupants with an audible alarm.

A solar inverter. It is connected to a home's solar panels and converts the energy from the solar panels into electricity for the home.

A smart washing machine. It has different washing programs for different textiles that the user can select on the machine's buttons. It can be connected to the internet via the home Wi-Fi, so the user can check the status of their laundry and control the machine remotely through a companion app on their mobile phone

An internet-connected home printer. It can print documents in different formats and colors and can be connected to a computer with a cable or wirelessly to receive print jobs. It can be connected to the internet via the

home Wi-Fi, so the user can send documents to print and check the printer's status remotely.

A robot vacuum cleaner. It can map and clean the home's floor on its own. It is connected to the internet via the home Wi-Fi, so the user can monitor its cleaning progress, set schedules, and control it remotely through a companion app on their mobile phone.

A smart thermostat. It is installed in the home's heating system and can be used to adjust the home's temperature on the thermostat's controls to set the desired temperature. It can be connected to the internet via the home Wi-Fi, so the user can check and control the temperature settings remotely through a companion app on their mobile phone.

A smart smoke detector. It can continuously monitor the home's air for smoke and potential fire hazards and alert occupants with an audible alarm. It can be connected to the internet via the home Wi-Fi, so the user can receive alerts and check its status remotely through a companion app on their mobile phone.

A Wi-Fi solar inverter. It is connected to a home's solar panels and converts the energy from the solar panels into electricity for the home. It can be connected to the internet via the home Wi-Fi, so the user can track energy production and monitor system performance remotely through a companion app on their mobile phone.

A home router. It keeps up and manages the home Wi-Fi and connects the devices in the home to the internet via a broadband connection. The user can manage connected devices, monitor the activity in the Wi-Fi network, and adjust settings through a web portal.

A smart security camera. It can continuously collect video recordings of the home or its surroundings. It is connected to the internet via the home Wi-Fi, so the user can check the video feed remotely through a companion app on their mobile phone.

A smart door lock. It is installed at the home's entrance door to lock and unlock it. It can be connected to the internet via the home Wi-Fi, so the user can remotely lock or unlock the door, monitor entry logs, or grant or revoke access to guests through a companion app on their mobile phone.

A smartwatch. It can continually track various health metrics of the user, be used for navigation, receiving messages, and can have various apps installed on it. It can be connected to the internet via a cellular network, so the user can use such features directly on the watch or through a companion app on their mobile phone.

A smart speaker. It can continually listen for voice commands to perform features like streaming music, setting reminders, getting weather updates, or controlling other connected devices in the home. It is connected to the internet via the home Wi-Fi, so the user can use these features via the smart speaker or manage the speaker via a companion app on their mobile phone.

Q6: Attention check We would like to learn what your favorite device is. Please select Voice assistant from the list below. This is an attention check.

Based on the text you read above, what device have you been asked to enter? *Smartphone, Washing machine –Laptop, Voice assistant, Smart Watch*

Q7: End of update support expectations Many smart devices receive software updates for a limited time after purchase. Once a device no longer receives software updates, how do you expect this will impact its use? Please select all that apply.

Device's performance declines, Some critical features stop working, affecting important functionality, Some non-essential features stop working, affecting 'nice-to-have' aspects, New features are no longer added, Less compatibility with other devices or services, Customer support services are no longer available, Cybersecurity weaknesses in the device are no longer fixed,

Potential cybersecurity risks to the device are no longer tracked (new threats may go unnoticed), Other, namely:, I don't expect any changes, I'm not sure

Q7.1: Own experience Have you experienced any of these changes with your own smart devices after software update support ended? *Yes, No, I don't know* (For the selected answers in Q7)

Q8: Update support duration Coming back to the two smart devices you have previously been presented with. For how many years do you expect such a smart device to receive software updates after purchase, if at all? Please write your answer as a number in the left-most column, or select one of the other options.

Number of years: (), I don't know, I don't expect it to receive updates (For the two smart devices seen in the vignettes.)

Q8.1: End of update support expectations You indicated that software updates for the smart device(s) will likely stop before the device's actual end of life. In what ways, if any, do you expect the device to work differently after software updates stop and it is still used? *(Open text field)* (Only shown if response to Q5.1.1 (expected lifetime) was lower than Q8 (expected update support))

Q9: Security considerations Since smart devices can be connected to the internet, they can be exposed to cybersecurity risks. Cybersecurity for smart devices focuses on protecting the devices, users, and their data from potential attacks through online connectivity.

Q9.1: Concerns Do you have any cybersecurity concerns regarding the use of your own smart devices? Please select all that apply, if any.

My personal data being accessed by unauthorized individuals., My devices being hacked and used maliciously without my knowledge., My devices being damaged or made unusable by a cyberattack., Insufficient customer support in case of cybersecurity issues., My personal data being shared

with third parties by the manufacturer without my consent., More personal data collected from the device than I expect., Other:, I'm not concerned., I'm not sure.

Q9.2: Mitigation actions Do you take any actions to address your cybersecurity concerns with your smart devices? Please select all that apply, if any.

Ensure the latest software updates are installed., Replace devices once software update support has ended., Disconnect devices from the network when not in use., Change device settings, such as passwords., Check online for news or warnings about my device., Be cautious about how I use and behave around my device., Choose brands that I trust when buying devices., Others;, None of the above.

Q9.3: Prolonged use Please rate your agreement with the following statement: I would use my smart devices for longer if they continued to receive software updates that fix cybersecurity weaknesses.

Strongly agree, Agree, Neither agree nor disagree, Disagree, Strongly disagree

Q10: Demographics Please answer some final questions about yourself to complete the survey.

Q10.1: Age How old are you?

Under 18, 18-24 years old, 25-34 years old, 35-44 years old, 45-54 years old, 55-64 years old, 65+ years old, Prefer not to say

Q10.2: Gender Which gender do you identify with?

Male, Female, Non-binary / third gender, Prefer not to say

Q10.3: Country In which country do you currently reside?

(List)

Q10.4: Employment Which option best describes your current status?

Employed / self-employed, Unemployed, Student, Retired, Other

Q10.5: Employment field Which option best describes the field you are currently working in?

Business or sales, Administrative support, Research, Hospitality service – Education, Computer engineer or IT, Engineer in other fields, Medical, Legal, Homemaker, Skilled labor, Art or writing, Government, Other, Prefer not to say

Q11: Debriefing Thank you for your responses! This study was about your expectations of smart device's lifetime and the role that security and privacy play. We did not disclose this explicitly at the beginning of the survey to not influence your responses in any way. Security and privacy is a sensitive topic which becomes increasingly important as the number of different smart devices in our environment grows rapidly. At the same time, regulations increasingly demand a longer time for these devices to receive software updates to protect them from attacks. In this survey, we wanted to measure your expectations about how long such devices will last, as this could affect how long manufacturers will provide such security updates. By reading and responding to the different descriptions of smart devices, you helped us a lot to research this topic.

Table 2: Regression model predicting expected device lifetime in the vignettes with Device Type, Country, respondents' Experience with the Device Category, and an Interaction between Country and the device's Smartness. "Ref" = Reference level. The outcome variable was log-transformed, and coefficients were exponentiated to denote an average increase or decrease in expected device lifetime, holding all other factors constant. Standard errors are not exponentiated.

	Coefficient	Standard error
Intercept	6.431***	0.054
Device Type (Ref: Smart speaker)		
Conventional printer	0.072	0.052
Conventional smoke detector	0.211***	0.053
Conventional solar inverter	0.569***	0.053
Conventional thermostat	0.527***	0.053
Conventional vacuum cleaner	0.054	0.053
Conventional washing machine	0.301***	0.052
Smart security camera	0.061	0.043
Robot vacuum cleaner	−0.126**	0.043
Home router	0.072	0.043
Smart door lock	0.116*	0.043
Connected printer	0.091*	0.043
Smart smoke detector	0.244***	0.043
Smart thermostat	0.434***	0.043
Smart washing machine	0.232***	0.043
Smartwatch	−0.221***	0.043
WiFi solar inverter	0.469***	0.043
Country (Ref: Spain)		
CountryFrance	−0.041	0.046
CountryGermany	0.092	0.046
CountryNetherlands	0.086	0.046
CountryPoland	−0.141***	0.046
Device Experience		
Device category experience	0.080**	0.024
Country:Smartness (Ref: Poland)		
Spain:Smartness	−0.049	0.045
France:Smartness	−0.071	0.045
Germany:Smartness	−0.085*	0.045
Netherlands:Smartness	−0.122**	0.045
AIC	3477.401	
BIC	3645.336	
Num. observations	2974	
Num. groups: Participant	993	
Conditional R^2	0.464	
Marginal R^2	0.166	

*** $p < 0.001$; ** $p < 0.01$; * $p < 0.05$

Table 3: Factors taken into account by respondents when estimating devices' lifetimes. Factors were derived by coding open-text responses to the question: "What aspects did you take into account when estimating the number of years?". Only the five most prevalent factors per device are listed.

Device	Factor	Count	Proportion
Washing Machine (Conventional)	Device type	47	19.03%
	Usage	43	17.41%
	Own experience	38	15.38%
	Components	22	8.91%
	Device quality	16	6.48%
Printer (Conventional)	Usage	63	25.82%
	Own experience	55	22.54%
	Device type	26	10.66%
	Components	23	9.43%
	Device quality	14	5.74%
Vacuum cleaner (Conventional)	Usage	53	24.65%
	Own experience	33	15.35%
	Device type	27	12.56%
	Components	20	9.30%
	Device quality	17	7.91%
Thermostat (Conventional)	Usage	58	24.79%
	Device type	41	17.52%
	Complexity	19	8.12%
	Own experience	17	7.26%
	Components	15	6.41%
Smoke detector (Conventional)	Usage	60	26.32%
	Complexity	38	16.67%
	Device type	23	10.09%
	Components	20	8.77%
	Safety	18	7.89%
Solar inverter (Conventional)	Device type	33	13.98%
	Price	32	13.56%
	Usage	29	12.29%
	Other / similar device	28	11.86%
	Estimate	17	7.20%
Smart washing machine (Smart)	Device type	70	26.32%
	Usage	33	12.41%
	Own experience	27	10.15%
	Smart complexity	22	8.27%
	Better alternative	14	5.26%
Connected printer (Smart)	Usage	56	21.71%
	Own experience	41	15.89%
	Device type	39	15.12%
	Updates	19	7.36%
	Components	18	6.98%

(Continued on next page.)

(Continued from previous page.)

Device	Factor	Count	Proportion
Robot vacuum (Smart)	Usage	68	25.66%
	Device type	30	11.32%
	Environment	22	8.30%
	Components	20	7.55%
	Own experience	19	7.17%
Smart thermostat (Smart)	Usage	48	19.59%
	Device type	33	13.47%
	Updates	29	11.84%
	Complexity	20	8.16%
	Estimate	15	6.12%
Smart smoke detector (Smart)	Usage	42	17.87%
	Device type	39	16.60%
	Complexity	19	8.09%
	Safety	19	8.09%
	Smart complexity	15	6.38%
WiFi Solar inverter (Smart)	Estimate	31	12.60%
	Device type	28	11.38%
	Usage	28	11.38%
	Price	22	8.94%
	Other / similar device	20	8.13%
Home router (Smart)	Own experience	49	19.92%
	Usage	40	16.26%
	Better alternative	38	15.45%
	(In-)compatibility	29	11.79%
	Device type	23	9.35%
Smart security camera (Smart)	Usage	37	14.12%
	Environment	32	12.21%
	Updates	27	10.31%
	Better alternative	25	9.54%
	Device quality	23	8.78%
Smart doorlock (Smart)	Usage	39	16.05%
	Device type	33	13.58%
	Estimate	18	7.41%
	Updates	18	7.41%
	Better alternative	15	6.17%
Smartwatch (Smart)	Usage	51	18.02%
	Better alternative	41	14.49%
	Updates	38	13.43%
	Components	29	10.25%
	Obsolescence	21	7.42%
Smart speaker (Smart)	Usage	38	15.51%
	Device type	34	13.88%
	Updates	32	13.06%
	Better alternative	27	11.02%
	Obsolescence	19	7.76%

Table 4: Final codebook of analysis of open text responses to the question: “What aspects did you take into account when estimating the number of years?”

Theme	Code	Code description
Static device quality	Device Type	The general sort of device was considered (e.g., "Washing machines last long")
	Conventional / Smart Device type	Lifetime estimate was explicitly based on the conventional counterpart of the smart device (e.g., "A normal vacuum cleaner lasts that long.").
	Device Quality	The device build quality would be taken into account.
	Components	Components of the device and their respective longevity were mentioned (e.g., "The battery will degrade quickly.").
	Manufacturer disclosure	What is disclosed about the device via marketing, the packaging, manuals, or the website.
	Brand	The device's brand would be considered.
	Similar / Other Device	A similar device was taken as an heuristic (e.g., solar panels as an heuristic for solar inverters, or smartphones for smart watches).
	Security	Security factors were considered (e.g., new encryption protocols or vulnerabilities).
	Safety	The safety relevance of the device was highlighted, requiring it to be reliable (e.g., reliance on a smoke detector)
	Modern	Modern technology in general was considered (e.g., "Modern devices break earlier" or "Modern devices are more reliable").
Dynamic device quality	Price	The device's purchase price was taken into account.
	Country	The device's country of manufacture was considered.
	Complexity	A general perception of the devices build-up complexity (e.g., "It is a complex device, so there are more parts that can break.").
	Smart complexity	It is highlighted explicitly that the added smartness (complexity) has an effect on the device's lifespan.
	Obsolescence	Planned obsolescence was mentioned as a consideration.
	Updates	Updates were explicitly mentioned as a factor.
	Innovation: Better alternatives	Newer, more attractive products available on the market, so that fast innovation drives faster replacement.
	(In-)compatibility	(In-)compatibility with other devices or services that are necessary to run the device.
	Spare parts / Component availability	For how long important components or spare parts are available.
	Upkeep costs	Costs of running the device were considered, like electricity costs or printer ink.
Device use	Usage	The frequency and intensity the device is used by its owners was considered.
Subjective factors	Environment	Environmental factors affecting device lifespan, like dog hairs for a vacuum cleaner of outdoor conditions.
	Maintenance / Installation	Device maintenance and duty of care were considered, or how the device is installed.
	Own experience	Respondents' own experiences with this device.
	Estimate	Respondents emphasized that they estimated the device's lifespan, e.g., because they were not completely sure.
Support structure	Preference	Respondents explicitly mentioned that they considered their normative preference for the lifetime (e.g., "wishful thinking").
	Warranty	The warranty period of the device type was mentioned.
	Regulations	Local regulations were taken into account (e.g., Laws on regular smoke detector replacement).

References

Literature

Abaquita D and others, 'Privacy Norms within the Internet of Things Using Contextual Integrity' *Companion of the 2020 ACM International Conference on Supporting Group Work* (2020)

Abdi N and others, 'Privacy Norms for Smart Home Personal Assistants' *Proceedings of the 2021 CHI conference on human factors in computing systems* (2021)

Abdi N, Ramokapane KM and Such JM, 'More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants' *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)* (2019)

Abrams L, 'QNAP Force-Installs Update after DeadBolt Ransomware Hits 3,600 Devices' <<https://www.bleepingcomputer.com/news/security/qnap-force-installs-update-after-deadbolt-ransomware-hits-3-600-devices/>>

Adee S, 'The Hunt For The Kill Switch' (2008) 45 IEEE Spectrum 34

Aertsen M, 'Open-Source Software vs. the Proposed Cyber Resilience Act' <<https://blog.nlnetlabs.nl/open-source-software-vs-the-cyber-resilience-act/>>

Ajmera P, 'Cybersecurity in the Internet of Things: Trends and Challenges in a Nascent Field' (2025) 59 Computer Law & Security Review 106204

Al-Masri E and others, 'Investigating Messaging Protocols for the Internet of Things (IoT)' (2020) 8 IEEE Access 94880

Amadeo R, 'Google's Iron Grip on Android: Controlling Open Source by Any Means Necessary' <<https://arstechnica.com/gadgets/2018/07/googles-iron-grip-on-android-controlling-open-source-by-any-means-necessary/>>

Amini S and Kanich C, 'Characterizing the Impact of Malware Infections and Remediation Attempts through Support Forum Analysis' *2017 APWG Symposium on Electronic Crime Research (eCrime)* (2017)

Anderson R, 'Why Information Security Is Hard - an Economic Perspective' *Seventeenth Annual Computer Security Applications Conference* (IEEE Comput Soc 2001)

—, 'Open and Closed Systems Are Equivalent (That Is, in an Ideal World)' in Joseph Feller and others (eds), *Perspectives on free and open source software* (MIT Press 2005)

Apthorpe N and others, 'Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity' (2018) 2 Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 1

Arnbak AM, 'Securing Private Communications: Protecting Private Communications Security in EU Law: Fundamental Rights, Functional Value Chains and Market Incentives' (PhD thesis, Universiteit van Amsterdam 2015)

Associated Press, ‘Recently Uncovered Software Flaw “Most Critical Vulnerability of the Last Decade”’ [2021] *The Guardian* <<https://www.theguardian.com/technology/2021/dec/10/software-flaw-most-critical-vulnerability-log-4-shell>>

Auspurg K and Hinz T, *Factorial Survey Experiments*, vol 175 (Sage Publications 2014)

Baeyens A and Goffin T, ‘Boston Scientific Medizintechnik GmbH v. AOK Sachsen-Anhalt’ (2015) 22 *European Journal of Health Law* 301

Bahirat P and others, ‘Overlooking Context: How Do Defaults and Framing Reduce Deliberation in Smart Home Privacy Decision-Making?’ *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (ACM 2021)

Barbosa NM, Zhang Z and Wang Y, ‘Do Privacy and Security Matter to Everyone? Quantifying and Clustering User-Centric Considerations About Smart Home Device Adoption’ *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)* (2020)

Barcomb A and others, ‘Managing Episodic Volunteers in Free/Libre/Open Source Software Communities’ (2022) 48 *IEEE Transactions on Software Engineering* 260

Barth A and others, ‘Privacy and Contextual Integrity: Framework and Applications’ *2006 IEEE Symposium on Security and Privacy (S&P’06)* (2006)

Bartolini C and others, ‘Cloud Providers Viability: How to Address It from an IT and Legal Perspective?’ in Jorn Altmann, Gheorghe Cosmin Silaghi and Omer F Rana (eds), *Economics of Grids, Clouds, Systems, and Services*, vol 9512 (Springer International Publishing 2016)

Basarir-Ozel B, Turker HB and Nasir VA, ‘Identifying the Key Drivers and Barriers of Smart Home Adoption: A Thematic Analysis from the Business Perspective’ (2022) 14 *Sustainability* 9053

BBC, ‘German Parents Told to Destroy Cayla Dolls over Hacking Fears’ *BBC News* (17 February 2017) <<https://www.bbc.com/news/world-europe-39002142>> accessed 28 October 2024

—, ‘Google Seeks Permission for Staff to Listen to Assistant Recordings’ [2019] *BBC News* <<https://www.bbc.com/news/technology-49796207>> accessed 27 September 2022

Beautement A and others, ‘Productive Security: A Scalable Methodology for Analysing Employee Security Behaviours’ *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)* (2016)

Becker I, Parkin S and Sasse MA, ‘Measuring the Success of Context-Aware Security Behaviour Surveys’ *The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER 2017)* (2017)

Behavioural Economics Team of the Australian Government (BETA), ‘Stay Smart: Helping Consumers Choose Cyber Secure Smart Devices’ <<https://behaviouraleconomics.pmc.gov.au/sites/default/files/projects/beta-report-cyber-security-labels.pdf>>

Bellanova R, Carrapico H and Duez D, ‘Digital/Sovereignty and European Security Integration: An Introduction’ (2022) 31 *European Security* 337

Bennett J and Adamowicz V, ‘Some Fundamentals of Environmental Choice Modelling’ [2001] *The choice modelling approach to environmental valuation* 37

- Berg R, 'Ex-Israeli Agents Reveal How Hezbollah Pager Attacks Were Carried Out' (23 December 2024) <<https://www.bbc.com/news/articles/cwy3l02wxqdo>> accessed 5 February 2026
- BEUC, 'Taming Temu' <<https://www.beuc.eu/enforcement/taming-temu>> accessed 27 November 2025
- Biasin E and Kamenjašević E, 'Cybersecurity of Medical Devices: New Challenges Arising from the AI Act and NIS 2 Directive Proposals' (2022) 3 *International Cybersecurity Law Review* 163
- Birkinbine BJ, *Incorporating the Digital Commons: Corporate Involvement in Free and Open Source Software* (University of Westminster Press 2020)
- Bitzer Jurgen, Schrettl W and Schröder PJH, 'Intrinsic Motivation in Open Source Software Development' (2007) 35 *Journal of Comparative Economics* 160
- Björck F and others, 'Cyber Resilience – Fundamentals for a Definition' in Alvaro Rocha and others (eds), *New Contributions in Information Systems and Technologies*, vol 353 (Springer International Publishing 2015)
- Blume P, 'An Alternative Model for Data Protection Law: Changing the Roles of Controller and Processor' (2015) 5 *International Data Privacy Law* 292
- Blythe JM, Coventry L and Little L, 'Unpacking Security Policy Compliance: The Motivators and Barriers of Employees' Security Behaviors' *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security* (USENIX Association 2015)
- Boniface C, Urquhart L and Terras M, 'Towards a Right to Repair for the Internet of Things: A Review of Legal and Policy Aspects' (2024) 52 *Computer Law & Security Review* 105934
- Bouwmeester B and others, '“The Thing Doesn't Have a Name”: Learning from Emergent Real-World Interventions in Smart Home Security' *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)* (2021)
- Boyes H, 'Cybersecurity and Cyber-Resilient Supply Chains' [2015] *Technology Innovation Management Review* 7
- Boyson S, 'Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical IT Systems' (2014) 34 *Technovation* 342
- Boyson S, Corsi TM and Paraskevas J-P, 'Defending Digital Supply Chains: Evidence from a Decade-Long Research Program' (2022) 118 *Technovation* 102380
- Bradford A, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020)
- Bradley C and Barrera D, 'Escaping Vendor Mortality: A New Paradigm for Extending IoT Device Longevity' *New Security Paradigms Workshop* (ACM 2023)
- Branley-Bell D and others, 'Exploring Age and Gender Differences in ICT Cybersecurity Behaviour' (2022) 2022 *Human Behavior and Emerging Technologies* 1 Bratton BH, *The Stack: On Software and Sovereignty* (MIT Press 2015)
- Braun V and Clarke V, 'One Size Fits All? What Counts as Quality Practice in (Reflexive) Thematic Analysis?' (2021) 18 *Qualitative research in psychology* 328

Brown I, 'Interoperability as a Tool for Competition Regulation' (LawArXiv 2020) preprint <<https://osf.io/fbvxd>>

Brown M, 'Ring Announces 6 New Products, along with Measures to Quiet Criticism of Its Privacy Practices' <<https://www.techhive.com/article/584254/ring-announces-6-new-products-along-with-measures-to-quiet-criticism-of-its-privacy-practices.html>>

Bundy J and others, 'Crises and Crisis Management: Integration, Interpretation, and Research Development' (2017) 43 *Journal of Management* 1661

Bundy J and Pfarrer MD, 'A Burden of Responsibility: The Role of Social Approval at the Onset of a Crisis' (2015) 40 *Academy of Management Review* 345

Burt J, 'Typosquat Supply Chain Attack Targets Go Developers' (*DevOps.com*, 5 February 2025) <<https://devops.com/typosquat-supply-chain-attack-targets-go-developers/>> accessed 18 September 2025

Bygrave LA, 'Cyber Resilience versus Cybersecurity as Legal Aspiration' 2022 *14th International Conference on Cyber Conflict: Keep Moving! (CyCon)* (2022)

——, 'Security by Design: Aspirations and Realities in a Regulatory Context' (2022) 8 *Oslo Law Review* 126

——, 'The Emergence of EU Cybersecurity Law: A Tale of Lemons, Angst, Turf, Surf and Grey Boxes' (2025) 56 *Computer Law & Security Review* 106071

Carman A, 'They Welcomed a Robot into Their Family, Now They're Mourning Its Death' <<https://www.theverge.com/2019/6/19/18682780/jibo-death-server-update-social-robot-mourning>>

——, 'Jibo, the Social Robot That Was Supposed to Die, Is Getting a Second Life' <<https://www.theverge.com/2020/7/23/21325644/jibo-social-robot-ntt-disruptionfunding>>

Carnovale S and Yenyurt S (eds), *Cyber Security and Supply Chain Management: Risks, Challenges and Solutions* (World Scientific 2021)

Castleman A and others, 'Vulnerable SDK Components Lead to Supply Chain Risks in IoT and OT Environments' <<https://www.microsoft.com/en-us/security/blog/2022/11/22/vulnerable-sdk-components-lead-to-supply-chain-risks-in-iot-and-ot-environments/>>

Çetin O and others, 'Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai.' *NDSS* (2019)

——, '“It Did Not Give Me an Option to Decline”: A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products' *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (ACM 2021)

Chalhoub G and Martin A, 'But Is It Exploitable? Exploring How Router Vendors Manage and Patch Security Vulnerabilities in Consumer-Grade Routers' [2023] *European Symposium on Usable Security (EuroUSEC 2023)* 277

Chan J, *Dying for an Iphone: Apple, Foxconn, and the Lives of China's Workers* (Haymarket Books 2020)

Chee FY, 'EU Plan to Phase-out High-Risk Tech Draws Fire from China's Huawei' *Reuters* (21 January 2026) <<https://www.reuters.com/business/media-telecom/eu-phase-out-high-risk-tech-targets-huawei-chinese-companies-2026-01-20/>> accessed 2 February 2026

Chen J and others, 'Who Is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption' (2020) 10 *International Data Privacy Law* 15

Chen J and Urquhart L, '“They're All about Pushing the Products and Shiny Things Rather than Fundamental Security”: Mapping Socio-Technical Challenges in Securing the Smart Home' (2022) 31 *Information & Communications Technology Law* 99

Cheruvu S and others, *Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment* (Apress 2020)

Chiara PG, 'The Cyber Resilience Act: The EU Commission's Proposal for a Horizontal Regulation on Cybersecurity for Products with Digital Elements: An Introduction' [2022] *International Cybersecurity Law Review*

——, 'The IoT and the New EU Cybersecurity Regulatory Landscape' [2022] *International Review of Law, Computers & Technology* 1

——, 'Towards a Right to Cybersecurity in EU Law? The Challenges Ahead' (2024) 53 *Computer Law & Security Review* 105961

——, 'Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise?' [2025] *European Journal of Risk Regulation* 1

Cimpanu C, 'Hackers Are Hijacking Smart Building Access Systems to Launch DDoS Attacks' <<https://www.zdnet.com/article/hackers-are-hijacking-smart-building-access-systems-to-launch-ddos-attacks/>>

Clark J, 'Google Swaps out MySQL, Moves to MariaDB' [2013] *The Register* <https://www.theregister.com/2013/09/12/google_mariadb_mysql_migration/>

Cobbe J, 'Governance and Interdependence in Data-Driven Supply Chains' *Global Governance by Data: Infrastructures of Algorithmic Rule* (2026)

Cobbe J, Norval C and Singh J, 'What Lies beneath: Transparency in Online Service Supply Chains' (2020) 5 *Journal of Cyber Policy* 65

Cobbe J, Veale M and Singh J, 'Understanding Accountability in Algorithmic Supply Chains' *2023 ACM Conference on Fairness Accountability and Transparency* (ACM 2023)

Cole A, 'All of Us Are Vulnerable, But Some Are More Vulnerable than Others: The Political Ambiguity of Vulnerability Studies, an Ambivalent Critique' (2016) 17 *Critical Horizons* 260

Colicchia C, Creazza A and Menachof DA, 'Managing Cyber and Information Risks in Supply Chains: Insights from an Exploratory Analysis' (2019) 24 *Supply Chain Management: An International Journal* 215

Colonna L, 'The End of Open Source? Regulating Open Source under the Cyber Resilience Act and the New Product Liability Directive' (2025) 56 *Computer Law & Security Review* 106105

Council of the European Union, 'Council Conclusions on ICT Supply Chain Security' (2022) 13664/22

Cox J and others, 'Consumer Understanding of Product Lifetimes' (2013) 79 Resources, Conservation and Recycling 21

Creazza A and others, 'Who Cares? Supply Chain Managers' Perceptions Regarding Cyber Supply Chain Risk Management in the Digital Transformation Era' (2022) 27 Supply Chain Management: An International Journal 30

Daigle K and GitHub Staff, 'Octoverse: The State of Open Source and Rise of AI in 2023' <<https://github.blog/news-insights/research/the-state-of-open-source-and-ai/>>

Das S and others, 'Breaking! A Typology of Security and Privacy News and How It's Shared' *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (2018)

Das S, Dabbish LA and Hong JI, 'A Typology of Perceived Triggers for End-User Security and Privacy Behaviors' *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)* (2019)

Davis A, 'Building Cyber-Resilience into Supply Chains' [2015] Technology Innovation Management Review 9

Davis W, 'Vizio Hit With Privacy Lawsuit Over Connected TVs' <<https://www.mediapost.com/publications/article/262835/vizio-hit-with-privacy-lawsuit-over-connected-tvs.html>>

Day M, Turner G and Drozdiak N, 'Thousands of Amazon Workers Listen to Alexa Users' Conversations' <<https://time.com/5568815/amazon-workers-listen-to-alexa/>>

De Hert P and others, 'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services' (2018) 34 Computer Law & Security Review 193

Dean B, 'An Exploration of Strict Products Liability and the Internet of Things' (Center for Democracy and Technology 2018) <<https://cdt.org/wp-content/uploads/2018/04/2018-04-16-IoT-Strict-Products-Liability-FNL.pdf>> accessed 28 September 2022

Deane JK and others, 'Managing Supply Chain Risk and Disruption from IT Security Incidents' (2009) 2 Operations Management Research 4 Deb S, 'Smart Beds Helped Them Sleep on a Cloud. Then the Cloud Crashed.' *The New York Times* (24 October 2025) <<https://www.nytimes.com/2025/10/24/business/amazon-aws-outage-eight-sleep-mattress.html>> accessed 31 October 2025

Delor F and Hubert M, 'Revisiting the Concept of "Vulnerability"' (2000) 50 Social Science & Medicine 1557

Del-Real C, De Busser E and Van Den Berg B, 'Shielding Software Systems: A Comparison of Security by Design and Privacy by Design Based on a Systematic Literature Review' (2024) 52 Computer Law & Security Review 105933

Department for Digital, Culture, Media and Sport (UK Government), 'Code of Practice for Consumer IoT Security' <<https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security>>

Dodds S, 'Dependence, Care, and Vulnerability' in Catriona Mackenzie, Wendy Rogers and Susan Dodds (eds), *Vulnerability* (Oxford University Press 2013)

Dourish P and others, 'Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem' (2004) 8 Personal and Ubiquitous Computing 391

Duivenvoorde B, 'The Protection of Vulnerable Consumers under the Unfair Commercial Practices Directive' [2013] *Journal of European Consumer and Market Law* 69

EDPB, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR'

Emami-Naeini P and others, 'Exploring How Privacy and Security Factor into IoT Device Purchase Behavior' *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (ACM 2019)

——, 'Ask the Experts: What Should Be on an IoT Privacy and Security Label?' *2020 IEEE Symposium on Security and Privacy (SP)* (2020)

——, 'Which Privacy and Security Attributes Most Impact Consumers' Risk Perception and Willingness to Purchase IoT Devices?' *2021 IEEE Symposium on Security and Privacy (SP)* (2021)

European Commission, 'Understanding Consumer Vulnerability in the EU's Key Markets' (2016) <https://commission.europa.eu/system/files/2018-04/consumer-vulnerability-factsheet_en.pdf>

——, 'Impact Assessment Report Accompanying the Document Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity across the Union, Repealing Directive (EU) 2016/1148' SWD (2020) 345 final

——, 'Staff Working Document Impact Assessment Report Accompanying the Document Proposal for a Regulation on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020' SWD (2022) 282 final

——, 'Commission and National Authorities Urge SHEIN to Respect EU Consumer Protection Laws' <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1331> accessed 27 November 2025

——, '2025 State of the Union Address by the President' <https://ec.europa.eu/-commission/presscorner/detail/ov/SPEECH_25_2053> accessed 10 October 2025

European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 'The EU's Cybersecurity Strategy for the Digital Decade' (2020) JOIN(2020) 18

European Union, 'Questions and Answers: Strengthening Cybersecurity of Wireless Devices and Products' <https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_5635>

European Union Agency for Cybersecurity, *Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures* (European Network and Information Security Agency 2017)

——, *Good Practices for Security of IoT: Secure Software Development Lifecycle* (European Network and Information Security Agency 2019)

——, *Guidelines for Securing the Internet of Things – Secure Supply Chain for IoT* (European Network and Information Security Agency 2020)

——, *ENISA Threat Landscape for Supply Chain Attacks* (A Malatras and others eds, European Network and Information Security Agency 2021) —, *ENISA Threat Landscape 2021 – April 2020 to Mid-July 2021* (M Theocharidou and others eds, European Network and Information Security Agency 2021)

——, *Good Practices for Supply Chain Cybersecurity* (European Network and Information Security Agency 2023)

——, '59% of EU Individuals Using Social Networks in 2023' (19 March 2024) <<https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20240319-1>> accessed 6 November 2025

——, 'Internet-Connected Devices Are Widely Used in the EU' (28 August 2025) <<https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20250828-2>> accessed 6 November 2025

——, 'Foundational Cybersecurity Activities for IoT Device Manufacturers' (National Institute of Standards and Technology 2020) NIST Internal or Interagency Report (NISTIR) 8259 <<https://csrc.nist.gov/publications/detail/nistir/8259/final>> accessed 4 August 2022

Fagan M, Khan MMH and Buck R, 'A Study of Users' Experiences and Beliefs about Software Update Messages' (2015) 51 *Computers in Human Behavior* 504

Fahey E, 'The Evolution of EU–US Cybersecurity Law and Policy: On Drivers of Convergence' (2024) 46 *Journal of European Integration* 1073 Favero N and Kim M, 'Everything Is Relative: How Citizens Form and Use Expectations in Evaluating Services' (2021) 31 *Journal of Public Administration Research and Theory* 561

Farrand B, Carrapico H and Turobov A, 'The New Geopolitics of EU Cybersecurity: Security, Economy and Sovereignty' (2024) 100 *International Affairs* 2379

Federal Communications Commission, 'U.S. Cyber Trust Mark' <<https://www.fcc.gov/CyberTrustMark>>

Federal Trade Commission, 'Smart Device Makers' Failure to Provide Updates May Leave You Smarting' <<https://www.ftc.gov/reports/smart-device-makers-failure-provide-updates-may-leave-you-smarting>>

Ferretti F, 'The Consumer Image under EU Law: Average, Rationally Bounded and Dispositionally Vulnerable. What Are the Prospects for Protection in Digital Markets?' (2025) 62 *Common Market Law Review* 121

Fineman MA (ed), 'The Vulnerable Subject: Anchoring Equality in the Human Condition' (2010) 20 *Yale Journal of Law and Feminism* 1

Frenkel S, Bergman R and Saad H, 'How Israel Built a Modern-Day Trojan Horse: Exploding Pagers' *The New York Times* (18 September 2024) <<https://www.nytimes.com/2024/09/18/world/middleeast/israel-exploding-pagers-hezbollah.html>> accessed 20 January 2025

Frik A and others, 'Privacy and Security Threat Models and Mitigation Strategies of Older Adults' *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)* (2019)

Friis K and Lysne O, 'Huawei, 5G and Security: Technological Limitations and Political Responses' (2021) 52 *Development and Change* 1174

Frostenson M and Prenkert F, 'Sustainable Supply Chain Management When Focal Firms Are Complex: A Network Perspective' (2015) 107 *Journal of Cleaner Production* 85

Furnell S and Thomson K-L, 'Recognising and Addressing "Security Fatigue"' (2009) 2009 Computer Fraud & Security 7

Gabriele S and Chiasson S, 'Understanding Fitness Tracker Users' Security and Privacy Knowledge, Attitudes and Behaviours' *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (ACM 2020)

Galli F and Novelli C, 'The Many Meanings of Vulnerability in the AI Act and the One Missing' [2024] BioLaw Journal - Rivista di BioDiritto 53

Garvey MD, Samuel J and Kretinin A, 'An Ontology of Supply Chain Cybersecurity' in Steven Carnovale and Sengun Yeniyurt (eds), *Cyber security and supply chain management: risks, challenges and solutions* (World Scientific 2021)

Gellert R el, *The Risk-Based Approach to Data Protection* (1st edn, Oxford University Press 2020)

—, 'The Role of the Risk-Based Approach in the General Data Protection Regulation and in the European Commission's Proposed Artificial Intelligence Act: Business as Usual?' (2021) 3 Journal of Ethics and Legal Technologies 16

Gennet Éloïse, Andorno R and Elger B, 'Does the New EU Regulation on Clinical Trials Adequately Protect Vulnerable Research Participants?' (2015) 119 Health Policy 925

Gerner-Beuerle C and Schuster E-P, 'The Evolving Structure of Directors' Duties in Europe' (2014) 15 European Business Organization Law Review 191

Ghadge A and others, 'Managing Cyber Risk in Supply Chains: A Review and Research Agenda' (2019) 25 Supply Chain Management: An International Journal 223

Ghiglieri M, Volkamer M and Renaud K, 'Exploring Consumers' Attitudes of Smart TV Related Privacy Risks' in Theo Tryfonas (ed), *Human Aspects of Information Security, Privacy and Trust*, vol 10292 (Springer International Publishing 2017)

Gigaset, 'Gigaset Smart Home/Care Wurde Eingestellt' <<https://www.gigaset.com/châÅÜde/cms/smart-home-uebersicht.html>>

—, 'Gigaset Smart Home/Care Staakt Zijn Diensten Vanaf 29 Maart 2024' <<https://www.gigaset.com/nlâÅÜnl/cms/smart-home-overzicht.html>>

Gokkaya B, Spanaki K and Karafili E, 'Strengthening the UK Regulatory Framework: Enhancing Cybersecurity in Supply Chains' (2025) 5 International Journal of Information Management Data Insights 100370

Gnanapragasam A and others, 'Consumer Expectations of Product Lifetimes around the World: A Review of Global Research Findings and Methods' [2017] PLATE: Product Lifetimes And The Environment 464

—, 'Consumer Perspectives on Longevity and Reliability: A National Study of Purchasing Factors across Eighteen Product Categories' (2018) 69 Procedia Cirp 910

Goanta C, Gregorio GD and Spanakis J, 'Consumer Protection and Digital Vulnerability: Common and Diverging Paths' in Camilla Crea and Alberto De Franceschi (eds), *The New Shapes of Digital Vulnerability in European Private Law* (Nomos Verlagsgesellschaft mbH & Co KG 2024)

Goodin D, 'As Log4Shell Wreaks Havoc, Payroll Service Reports Ransomware Attack' <<https://arstechnica.com/information-technology/2021/12/as-log4shell-wreaks-havoc-payroll-service-reports-ransomware-attack/>>

Goodwin C and others, 'Quantifying Device Usefulness - How Useful Is an Obsolete Device?' in José Abdelnour Nocera and others (eds), *Human-Computer Interaction – INTERACT 2023*, vol 14145 (Springer Nature Switzerland 2023)

Gordon LA and others, 'Increasing Cybersecurity Investments in Private Sector Firms' [2015] *Journal of Cybersecurity* 3

Goumagias N and others, 'Making Sense of the Internet of Things: A Critical Review of Internet of Things Definitions between 2005 and 2019' (2021) 31 *Internet Research* 1583

Graham E, 'Iranian Hackers Compromised a Federal Agency's Network, CISA and FBI Say' (*Nextgov.com*, 16 November 2022) <<https://www.nextgov.com/cybersecurity/2022/11/iranian-hackers-compromised-federal-agencys-network-cisa-and-fbi-say/379832/>> accessed 5 February 2026

Grau GI, 'An Appraisal of the Proposal for a Directive on Liability for Defective Products' (2023) 12 *Journal of European Consumer and Market Law* 198

Greenberg A, 'After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix' [2015] *Wired* <<https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/>> accessed 27 September 2022

Greenwald G, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (First Edition, Metropolitan Books/Henry Holt 2014)

Guerrini F, 'Consumer Protection In Gaming: European Initiative Targets Video Game Publishers' <<https://www.forbes.com/sites/federicoguerrini/2024/08/30/consumer-protection-in-gaming-european-initiative-targets-video-game-publishers/>>

Guihot M, 'Coherence in Technology Law' (2019) 11 *Law, Innovation and Technology* 311

Haney J, Acar Y and Furman S, '“It's the Company, the Government, You and I”: User Perceptions of Responsibility for Smart Home Privacy and Security' 30th *USENIX Security Symposium (USENIX Security 21)* (2021)

Haney J and Furman S, 'User Perceptions and Experiences with Smart Home Updates' (IEEE Computer Society 2022) <<https://www.computer.org/csdl/proceedings-article/sp/2023/933600a782/1Js0Dlv3Xpe>> accessed 12 January 2023

Haney JM and Furman SM, 'Work in Progress: Towards Usable Updates for Smart Home Devices' in Thomas Groß and Luca Viganò (eds), *Socio-Technical Aspects in Security and Trust* (Springer International Publishing 2021)

——, 'Smart Home Device Loss of Support: Consumer Perspectives and Preferences' *HCI for Cybersecurity, Privacy and Trust: 5th International Conference, HCI-CPT 2023, Held as Part of the 25th HCI International Conference, HCII 2023, Copenhagen, Denmark, July 23–28, 2023, Proceedings* (Springer-Verlag 2023) <https://doi.org/10.1007/978-3-031-35822-7_32> accessed 31 October 2023

- Haney JM, Furman SM and Acar Y, 'Smart Home Security and Privacy Mitigations: Consumer Perceptions, Practices, and Challenges' in Abbas Moallem (ed), *HCI for Cybersecurity, Privacy and Trust* (Springer International Publishing 2020)
- Hasegawa AA and others, 'Understanding Non-Experts' Security-and Privacy-Related Questions on a Q&A Site' *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)* (2022)
- Hawkins AJ, 'BMW Drops Plan to Charge a Monthly Fee for Heated Seats' (*The Verge*, 7 September 2023) <<https://www.theverge.com/2023/9/7/23863258/bmw-cancel-heated-seat-subscription-microtransaction>> accessed 19 November 2025
- Helberger N and others, 'Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability' (2022) 45 *Journal of Consumer Policy* 175
- Hess C and Ostrom E (eds), *Understanding Knowledge as a Commons: From Theory to Practice* (MIT Press 2007)
- Hiesgen R and others, 'The Log4j Incident: A Comprehensive Measurement Study of a Critical Vulnerability' [2024] *IEEE Transactions on Network and Service Management* 1
- Higgs B, Polonsky MJ and Hollick M, 'Measuring Expectations: Forecast vs. Ideal Expectations. Does It Really Matter?' (2005) 12 *Journal of retailing and consumer services* 49
- Hoepman J-H and Jacobs B, 'Increased Security through Open Source' (2007) 50 *Communications of the ACM* 79
- Hoffmann Jörg and Gonzalez Otero Begoña, 'Demystifying The Role Of Data Interoperability In The Access And Sharing Debate' (2021) 11 *JIPITEC* 252
- Hon WK, Millard C and Singh J, 'Twenty Legal Considerations for Clouds of Things' (2016) 2016 *Queen Mary University of London, School of Law Legal Studies Research Paper*
- Humphreys L and others, 'Mapping Recitals to Normative Provisions in EU Legislation to Assist Legal Interpretation' *JURIX* (2015)
- Jacobs B, 'The Authenticity Crisis' (2024) 53 *Computer Law & Security Review* 105962
- Jiang S and Finkle J, 'China's Xiongmai to Recall up to 10,000 Webcams after Hack' [2016] *Reuters* <<https://www.reuters.com/article/us-cyber-attacks-china-idUSKCN12P1TT>> accessed 27 September 2022
- Jin H and others, 'Exploring the Needs of Users for Supporting Privacy-Protective Behaviors in Smart Homes' *CHI Conference on Human Factors in Computing Systems* (ACM 2022)
- Jolly J and Milmo D, 'Inside the Jaguar Land Rover Hack: Stalled Smart Factories, Outsourced Cybersecurity and Supply Chain Woes' *The Guardian* (20 September 2025) <<https://www.theguardian.com/business/2025/sep/20/jaguar-land-rover-hack-factories-cybersecurity-jlr>> accessed 22 September 2025
- Jovanée A, 'Four Classic Command & Conquer Titles Are Now Open Source' <<https://www.polygon.com/news/531365/command-and-conquer-open-source-code-ea>>
- Kalamees P, 'Goods With Digital Elements And The Seller's Updating Obligation' (2021) 2 *JIPITEC* 131

- Kamara I, 'European Cybersecurity Standardisation: A Tale of Two Solitudes in View of Europe's Cyber Resilience' (2024) 37 *Innovation: The European Journal of Social Science Research* 1441
- Kenneally E and Dittrich D, 'The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research' <<https://papers.ssrn.com/abstract=2445102>> accessed 22 January 2025
- Kim N and Ohm P, 'Legacy Switches: A Proposal to Protect Privacy, Security, and the Environment from the Internet of Things' (2023) 84 *Ohio State Law Journal* 101
- Koops EJ, 'Should ICT Regulation Be Technology-Neutral?' in BJ Koops and others (eds), *Starting Points for ICT Regulation* (TMC Asser Press 2006)
- , 'A Taxonomy for Descriptive Research in Law and Technology' in E Palmerini and E Stradella (eds), *Law and technology: The challenge of regulating technological* (Pisa University Press 2013)
- Kostan A and others, 'Exploring Digital Security and Privacy in Relative Poverty in Germany through Qualitative Interviews' 33rd *USENIX Security Symposium (USENIX Security 24)* (2024)
- Krebs B, 'Target Hackers Broke in Via HVAC Company' (*Krebs on Security*, 5 February 2014) <<https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/>> accessed 20 June 2022
- Krol K and others, 'Towards Robust Experimental Design for User Studies in Security and Privacy' *The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER 2016)* (2016)
- Kustosch L and others, 'Measuring Up to (Reasonable) Consumer Expectations: Providing an Empirical Basis for Holding IoT Manufacturers Legally Responsible' *Proceedings of the 32nd USENIX Security Symposium* (2023)
- Kwong JK and Pearlson K, 'Supply Chain Cybersecurity and Small and Medium-Sized Enterprises (SMEs): Exploring Shortcomings in Third Party Risk Management of SMEs'
- Ladisa P and others, 'SoK: Taxonomy of Attacks on Open-Source Software Supply Chains' 2023 *IEEE Symposium on Security and Privacy (SP)* (2023)
- Lambach D and Monsees L, 'Beyond Sovereignty as Authority: The Multiplicity of European Approaches to Digital Sovereignty' (2025) 4 *Global Political Economy* 71
- Lau J, Zimmerman B and Schaub F, 'Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-Seeking Behaviors with Smart Speakers' (2018) 2 *Proceedings of the ACM on Human-Computer Interaction* 1
- Lazarotto B, 'The Right to Data Portability: A Holistic Analysis of GDPR, DMA and the Data Act' (2024) 15 *European Journal of Law and Technology*
- Lechelt S and others, 'Designing for the End of Life of IoT Objects' *Companion Publication of the 2020 ACM Designing Interactive Systems Conference* (ACM 2020) <<https://dl.acm.org/doi/10.1145/3393914.3395918>>
- Li Y and others, 'The More You Ask, the Less You Get: When Additional Questions Hurt External Validity' [2021] *Journal of Marketing Research*

- Li Y and others, 'Ripple Effect in the Supply Chain Network: Forward and Backward Disruption Propagation, Network Health and Firm Vulnerability' (2021) 291 *European Journal of Operational Research* 1117
- Li Y and Xu L, 'Cybersecurity Investments in a Two-Echelon Supply Chain with Third-Party Risk Propagation' (2021) 59 *International Journal of Production Research* 1216
- Limaye Y, 'Fibre Optic Drones: The Terrifying New Weapon Changing the War in Ukraine' *BBC News* (28 May 2025) <<https://www.bbc.com/news/articles/ckgn47e5qyno>> accessed 3 December 2025
- Linåker J, Papatheocharous E and Olsson T, 'How to Characterize the Health of an Open Source Software Project? A Snowball Literature Review of an Emerging Practice' *Proceedings of the 18th International Symposium on Open Collaboration* (ACM 2022) <<https://dl.acm.org/doi/10.1145/3555051.3555067>>
- Liu M, 'Digital Vulnerability: Rethinking Power Imbalances in the Digital Age' (2024) 32 *European Review of Private Law* 827
- Liu P and others, 'How IoT Re-Using Threatens Your Sensitive Data: Exploring the User-Data Disposal in Used IoT Devices' *2023 IEEE Symposium on Security and Privacy (SP)* (2023)
- Ludvigsen KR, Nagaraja S and Daly A, 'Preventing or Mitigating Adversarial Supply Chain Attacks: A Legal Analysis' *Proceedings of the 2022 ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses* (ACM 2022)
- Luna F, 'Elucidating the Concept of Vulnerability: Layers Not Labels' (2009) 2 *IJFAB: International Journal of Feminist Approaches to Bioethics* 121
- Lunden I, 'VanMoof, the e-Bike Startup, Officially Declared Bankrupt in The Netherlands' <<https://techcrunch.com/2023/07/18/vanmoof-goes-vanpoof-bankruptcy/>>
- Lyngaas S, 'US Warns Hundreds of Millions of Devices at Risk from Newly Revealed Software Vulnerability' <<https://www.cnn.com/2021/12/13/politics/us-warning-software-vulnerability/index.html>>
- Lysne O, *The Huawei and Snowden Questions* (Springer International Publishing 2018)
- Mahieu R and others, 'Measuring the Brussels Effect through Access Requests: Has the European General Data Protection Regulation Influenced the Data Protection Rights of Canadian Citizens?' (2021) 11 *Journal of Information Policy* 301
- Malgieri G, *Vulnerability and Data Protection Law* (1st edn, Oxford University Press 2023)
- Malgieri G and Niklas J, 'Vulnerable Data Subjects' (2020) 37 *Computer Law & Security Review* 105415
- Marky K and others, '"I Don't Know How to Protect Myself": Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments' *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society* (2020)
- Martin K and Shilton K, 'Why Experience Matters to Privacy: How Context-Based Experience Moderates Consumer Privacy Expectations for Mobile Applications' (2016) 67 *Journal of the Association for Information Science and Technology* 1871

- Masterman CJ and Viscusi WK, 'The Specific Consumer Expectations Test for Product Defects' (2020) 95 Ind. LJ 183
- Matwyshyn AM, 'CYBER!' (2017) 2017 BYU Law Review 1109
- Melnyk SA and others, 'New Challenges in Supply Chain Management: Cybersecurity across the Supply Chain' (2022) 60 International Journal of Production Research 162
- Meneely A and Williams L, 'Secure Open Source Collaboration: An Empirical Study of Linus' Law' *Proceedings of the 16th ACM conference on Computer and communications security* (ACM 2009)
- , 'Strengthening the Empirical Analysis of the Relationship between Linus' Law and Software Security' *Proceedings of the 2010 ACM-IEEE International Symposium on Empirical Software Engineering and Measurement* (ACM 2010)
- Menn J, Finkle J and Volz D, 'Cyber Attacks Disrupt PayPal, Twitter, Other Sites' [2016] Reuters <<https://www.reuters.com/article/us-usa-cyber-idUSKCN12L1ME>> accessed 27 September 2022
- Mentzer JT and others, 'Defining Supply Chain Management' (2001) 22 Journal of Business Logistics 1
- Merriam SB and Tisdell EJ, *Qualitative Research: A Guide to Design and Implementation* (John Wiley & Sons 2015)
- Mezrich JL, 'Source Code Escrow: An Exercise in Futility?' (2001) 5 Marquette Intellectual Property Law Review 117
- Milenkovic M, *Internet of Things: Concepts and System Design* (Springer International Publishing 2020) <<http://link.springer.com/10.1007/978-3-030-41346-0>>
- Millard C (ed), *Cloud Computing Law* (2nd edn, Oxford University Press 2021)
- Miller C, *Chip War: The Fight for the World's Most Critical Technology* (Scribner 2022)
- Mišćenić E, 'Information, Transparency and Fairness for Consumers in the Digital Environment' in Camilla Crea and Alberto De Franceschi (eds), *The New Shapes of Digital Vulnerability in European Private Law* (Nomos Verlagsgesellschaft mbH & Co KG 2024)
- Morgner P and others, 'Security Update Labels: Establishing Economic Incentives for Security Patching of IoT Consumer Products' *2020 IEEE Symposium on Security and Privacy (SP)* (2020)
- Muffatto M, *Open Source: A Multidisciplinary Approach* (Imperial College Press 2006)
- Naeini PE and others, 'Privacy Expectations and Preferences in an IoT World' *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)* (2017)
- Nasirinejad M and Sampalli S, 'Evaluating Consumer Behavior, Decision Making, Risks, and Challenges for Buying an IoT Product' (2023) 4 IoT 78
- Netherlands Enterprise Agency, 'Supplying Updates Is Mandatory' <<https://business.gov.nl/amendment/supplying-updates-to-become-mandatory/>>
- Nicholson D, 'Python Software Foundation News: The EU's Proposed CRA Law May Have Unintended Consequences for the Python Ecosystem' <<https://pyfound.blogspot.com/2023/04/the-eus-proposed-cra-law-may-have.html>>

Nishijima D and Oguchi M, 'Measuring Product Lifetime Extension Potential by Increasing the Expected Product Lifetime: Methodology and Case Study' (2023) 32 *Business Strategy and the Environment* 1218

Nolte H, Rateike M and Finck M, 'Robustness and Cybersecurity in the EU Artificial Intelligence Act' *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency* (ACM 2025)

Nord Projects, 'Little Printers, a Friendly New Messaging App and Cloud Platform' <<https://nordprojects.co/projects/littleprinters/>>

Norman G, 'Likert Scales, Levels of Measurement and the "Laws" of Statistics' (2010) 15 *Advances in Health Sciences Education* 625

Noura M, Atiquzzaman M and Gaedke M, 'Interoperability in Internet of Things: Taxonomies and Open Challenges' (2019) 24 *Mobile Networks and Applications* 796

——, 'Informal Support Networks: An Investigation into Home Data Security Practices' *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)* (2018)

Nunziato DC, 'The Digital Services Act and the Brussels Effect on Platform Content Moderation' (2023) 24 *Chi. J. Int'l L.* 115

Nusselder S, 'Scrutinising the Interplay between Data Protection and Cybersecurity: A Paradox Shrouded Behind the "State-of-the-Art"' (2025) 11 *European Data Protection Law Review* 145

Nygård AR and Katsikas S, 'SoK: Combating Threats in the Digital Supply Chain' *Proceedings of the 17th International Conference on Availability, Reliability and Security* (ACM 2022)

O'Connor T, Enck W and Reaves B, 'Blinded and Confused: Uncovering Systemic Flaws in Device Telemetry for Smart-Home Internet of Things' *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks* (ACM 2019)

O'Connor T, Jessee D and Campos D, 'Through the Spyglass: Towards IoT Companion App Man-in-the-Middle Attacks' *Cyber Security Experimentation and Test Workshop* (ACM 2021)

O'Carroll L, 'EU Carmakers "Days Away" from Halting Work as Chip War with China Escalates' *The Guardian* (29 October 2025) <<https://www.theguardian.com/business/2025/oct/29/europe-carmakers-china-computer-chip>> accessed 24 November 2025

——, 'Netherlands Suspends State Seizure of Chinese Chipmaker Nexperia' *The Guardian* (19 November 2025) <<https://www.theguardian.com/business/2025/nov/19/netherlands-suspends-seizure-china-chipmaker-nexperia>> accessed 24 November 2025

O'Donnell L, 'EU Recalls Children's Smartwatch That Leaks Location Data' <<https://threatpost.com/eu-recalls-childrens-smartwatch-that-leaks-location-data/141511/>>

——, 'Unpatched Security Flaws Open Connected Vacuum to Takeover' <<https://threatpost.com/unpatched-security-flaws-open-connected-vacuum-to-takeover/153142/>>

Oguchi M and others, 'Consumers' Expectations for Product Lifetimes of Consumer Durables' *2016 Electronics Goes Green 2016+(EGG)* (IEEE 2016)

Oh S-R and Kim Y-G, 'AFaaS: Authorization Framework as a Service for Internet of Things Based on Interoperable OAuth' (2020) 16 International Journal of Distributed Sensor Networks 155014772090638

Ohm M and others, 'Backstabber's Knife Collection: A Review of Open Source Software Supply Chain Attacks' in Clémentine Maurice and others (eds), *Detection of Intrusions and Malware, and Vulnerability Assessment*, vol 12223 (Springer International Publishing 2020)

Oladimeji S and Kerner SM, 'SolarWinds Hack Explained: Everything You Need to Know' <<https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know>>

Omitola T and Wills G, 'Towards Mapping the Security Challenges of the Internet of Things (IoT) Supply Chain' (2018) 126 Procedia Computer Science 441

Open Source Initiative, 'The Open Source Definition' <<https://opensource.org/osd>>

Osborne C, 'Remote Code Execution Flaw Allowed Hijack of Motorola Halo+ Baby Monitors' <<https://portswigger.net/daily-swig/remote-code-execution-flaw-allowed-hijack-of-motorola-halo-baby-monitors>> accessed 27 September 2022

——, 'Researcher Discloses Alleged Zero-Day Vulnerabilities in NUUO NVRmini2 Recording Device' <<https://portswigger.net/daily-swig/researcher-discloses-alleged-zero-day-vulnerabilities-in-nuuo-nvrmini2-recording-device>> accessed 27 September 2022

Overney C and others, 'How to Not Get Rich: An Empirical Study of Donations in Open Source' *Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering* (ACM 2020)

Paganini P, 'Watch out, FLocker Ransomware Targets Android Smart TVs' <<https://securityaffairs.co/wordpress/48383/iot/flocker-ransomware-smart-tvs.html>> accessed 27 September 2022

Parkin S and others, 'Security When It Is Welcome: Exploring Device Purchase as an Opportune Moment for Security Behavior Change' *Proceedings of the Workshop on Usable Security and Privacy (USEC'19)* (Internet Society 2019)

Parry R and Bisson R, 'Legal Approaches to Management of the Risk of Cloud Computing Insolvencies' (2020) 20 Journal of Corporate Law Studies 421

Payne C, 'On the Security of Open Source Software' (2002) 12 Information Systems Journal 61

Phipps S, 'What Is the Cyber Resilience Act and Why It's Dangerous for Open Source' <<https://blog.opensource.org/what-is-the-cyber-resilience-act-and-why-its-important-for-open-source/>> Platjouw FM, *Environmental Law and the Ecosystem Approach* (Routledge 2016)

Piasecki S, 'Expert Perspectives on GDPR Compliance in the Context of Smart Homes and Vulnerable Persons' (2023) 32 Information & Communications Technology Law 385

Pinzger M, Nagappan N and Murphy B, 'Can Developer-Module Networks Predict Failures?' *Proceedings of the 16th ACM SIGSOFT International Symposium on Foundations of software engineering* (ACM 2008)

Poole ES and others, 'Computer Help at Home: Methods and Motivations for Informal Technical Support' *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2009)

Preuss L and others, 'Corporate Scandals: Firm Response Strategies and Subsequent Media Coverage' (2018) 2018 Academy of Management Proceedings 18369

Privacy International, 'We Looked into the Software Support Practices for 5 of the Most Popular Smart Devices (and the Results May Disappoint You)' <<https://privacyinternational.org/report/4965/we-looked-software-support-practices-5-most-popular-smart-devices-and-results-may>>

Purdy K, 'Red Hat's New Source Code Policy and the Intense Pushback, Explained' <<https://arstechnica.com/information-technology/2023/06/red-hats-new-source-code-policy-and-the-intense-pushback-explained/>>

——, 'Valve Releases Full Team Fortress 2 Game Code to Encourage New, Free Versions' <<https://arstechnica.com/gaming/2025/02/valve-releases-full-team-fortress-2-game-code-to-encourage-new-free-versions/>>

Quelle C, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-Based Approach' (2018) 9 European Journal of Risk Regulation 502

Rader E and Wash R, 'Identifying Patterns in Informal Sources of Security Information' (2015) 1 Journal of Cybersecurity 121

Rader E, Wash R and Brooks B, 'Stories as Informal Lessons about Security' *Proceedings of the Eighth Symposium on Usable Privacy and Security* (2012)

Radu R and Amon C, 'The Governance of 5G Infrastructure: Between Path Dependency and Risk-Based Approaches' (2021) 7 Journal of Cybersecurity 1

Ranchordas S and Beck M, 'Vulnerability' in Mareile Kaufmann and Heidi Mork Lomell (eds), *De Gruyter Handbook of Digital Criminology* (De Gruyter 2025)

Ransbotham S, 'An Empirical Analysis of Exploitation Attempts Based on Vulnerabilities in Open Source Software' [2010] Workshop on the Economics of Information Security 1

Raymond E, 'The Cathedral and the Bazaar' (1999) 12 Knowledge, Technology & Policy 23

Rebrean M-L and Malgieri G, 'Vulnerability in the EU AI Act: Building an Interpretation' *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency* (ACM 2025)

Renaud K, Searle R and Dupuis M, 'Shame in Cyber Security: Effective Behavior Modification Tool or Counterproductive Foil?' *New Security Paradigms Workshop* (ACM 2021)

Rich J, 'What Happens When the Sun Sets on a Smart Product?' <<https://www.ftc.gov/business-guidance/blog/2016/07/what-happens-when-sun-sets-smart-product>>

Ricker T, 'Cowboy Releases Cheeky App to Keep VanMoof E-Bike Riders on the Road' <<https://www.theverge.com/2023/7/13/23793591/cowboy-vanmoof-key-app-download-ios-android>>

Rickerby J, 'Resilient Products — How Connected Devices Can Live On.' <<https://medium.com/nord-projects/resilient-products-how-connected-devices-can-live-on-b9c0bb9534e6>>

Riefa C, 'Protecting Vulnerable Consumers in the Digital Single Market' (2022) 33 European Business Law Review 607

Robinson D, 'Nice Smart Device – How Long Does It Get Software Updates?' <https://www.theregister.com/2023/01/16/smart_device_software_support/>

Rodríguez E and others, 'Super-Spreaders: Quantifying the Role of IoT Manufacturers in Device Infections' *20th Annual Workshop on the Economics of Information Security (WEIS 2021)* (2021)

Roose K, 'Did One Guy Just Stop a Huge Cyberattack?' *The New York Times* (3 April 2024) <<https://www.nytimes.com/2024/04/03/technology/prevent-cyberattack-linux.html>> accessed 13 October 2025

Rosenzweig P, 'Cybersecurity and the Least Cost Avoider' [2013] *Lawfare* <<https://www.lawfaremedia.org/article/cybersecurity-and-least-cost-avoider>> accessed 28 November 2025

Rossignol J, 'Foxconn and Compal Will Reportedly Assemble "Apple Watch Series 6" Models Next Year' <<https://www.macrumors.com/2019/10/23/apple-watch-series-6-foxconn-compal/>>

Rostami A and others, 'Being Hacked: Understanding Victims' Experiences of IoT Hacking' *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)* (2022)

Royle OR, 'Amazon Driver Breaks down the AI System Watching Them for Safety Violations like Drinking Coffee While Driving' <<https://fortune.com/2023/02/27/amazon-delivery-driver-breaks-down-ai-surveillance-in-vans/>>

Samonas S and Coss D, 'The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security' (2014) 10 *Journal of Information System Security* 21

Sauer C, Auspurg K and Hinz T, 'Designing Multi-Factorial Survey Experiments: Effects of Presentation Style (Text or Table), Answering Scales, and Vignette Order' (2020) 14 *Methods, data, analyses: a journal for quantitative methods and survey methodology (mda)* 195

Sawik T, 'Balancing Cybersecurity in a Supply Chain under Direct and Indirect Cyber Risks' (2022) 60 *International Journal of Production Research* 766

Schauer S, Polemi N and Mouratidis H, 'MITIGATE: A Dynamic Supply Chain Cyber Risk Assessment Methodology' (2019) 12 *Journal of Transportation Security* 1

Schmitz-Berndt S and Chiara PG, 'One Step Ahead: Mapping the Italian and German Cybersecurity Laws against the Proposal for a NIS2 Directive' *International Cybersecurity Law Review* 163

Schneier B, 'Ring Gives Videos to Police without a Warrant or User Consent - Schneier on Security' <<https://www.schneier.com/blog/archives/2022/08/ring-gives-videos-to-police-without-a-warrant-or-user-consent.html>> accessed 27 September 2022

Schryen G, 'Is Open Source Security a Myth?' (2011) 54 *Communications of the ACM* 130

Schmitz-Berndt S and Chiara PG, 'One Step Ahead: Mapping the Italian and German Cybersecurity Laws against the Proposal for a NIS2 Directive' (2022) 3 *International Cybersecurity Law Review* 163

Schneier B, 'Backdoor in XZ Utils That Almost Happened' (*Schneier on Security*, 11 April 2024) <<https://www.schneier.com/blog/archives/2024/04/backdoor-in-xz-utils-that-almost-happened.html>> accessed 2 November 2025

Schulte-Nölke H, 'Digital Obligations of Sellers of Smart Devices under the Sale of Goods Directive 771/2019' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Smart Products* (Nomos 2022)

Schulz C-H, 'Open Source Software and Security: Practices, Governance, History, and Perceptions' in Amanda Brock (ed), *Open Source Law, Policy and Practice* (2nd edn, Oxford University Press 2022)

Schwarz N and others, 'Response Scales: Effects of Category Range on Reported Behavior and Comparative Judgments' (1985) 49 *Public opinion quarterly* 388

Seng N, 'Cybersecurity Regulation—Types, Principles, and Country Deep Dives in Asia' (2024) 5 *International Cybersecurity Law Review* 387

Serror M and others, 'Challenges and Opportunities in Securing the Industrial Internet of Things' (2021) 17 *IEEE Transactions on Industrial Informatics* 2985

Setz B and others, 'A Comparison of Open-Source Home Automation Systems' (2021) 9 *IEEE Access* 167332

Seuring S and Müller M, 'From a Literature Review to a Conceptual Framework for Sustainable Supply Chain Management' (2008) 16 *Journal of Cleaner Production* 1699

Shank DB and others, 'Knowledge, Perceived Benefits, Adoption, and Use of Smart Home Products' (2021) 37 *International Journal of Human–Computer Interaction* 922

Sharma A, 'Hive Claims Ransomware Attack on Tata Power, Begins Leaking Data' <<https://www.bleepingcomputer.com/news/security/hive-claims-ransomware-attack-on-tata-power-begins-leaking-data/>>

—, 'Self-Propagating Supply Chain Attack Hits 187 Npm Packages' (*BleepingComputer*) <<https://www.bleepingcomputer.com/news/security/self-propagating-supply-chain-attack-hits-187-npm-packages/>>

Sharma C, 'Tragedy of the Digital Commons' (2023) 101 *North Carolina Law Review* 1129

Sheikh H, 'European Digital Sovereignty: A Layered Approach' (2022) 1 *Digital Society* 25

Shepardson D, 'US Agency Votes to Tighten Restrictions on Chinese Tech Companies Deemed Threats' *Reuters* (28 October 2025) <<https://www.reuters.com/business/media-telecom/us-agency-votes-tighten-restrictions-chinese-tech-companies-deemed-threats-2025-10-28/>> accessed 2 February 2026

Shirvani G and Ghasemshirazi S, 'Towards Sustainable IoT: Challenges, Solutions, and Future Directions for Device Longevity' <<https://arxiv.org/abs/2405.16421>>

Shklovski I and others, 'Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use' *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (ACM 2014)

Shvartzshnaider Y and others, 'Learning Privacy Expectations by Crowdsourcing Contextual Informational Norms' (2016) 4 Proceedings of the AAAI Conference on Human Computation and Crowdsourcing 209

Shvartzshnaider Y, Sanfilippo MR and Apthorpe N, 'Contextual Integrity as a Gauge for Governing Knowledge Commons' in Madelyn Rose Sanfilippo, Brett M Frischmann and Katherine J Strandburg (eds), *Governing Privacy in Knowledge Commons* (Cambridge University Press 2021)

Smith PM, 'Copyright, Contract, and Licensing in Open Source' in Amanda Brock (ed), *Open Source Law, Policy and Practice* (2nd edn, Oxford University Press 2022)

Somaini L, 'The Right to Data Portability and User Control: Ambitions and Limitations' (2018) 3 MediaLaws

Su D and Steiner PM, 'An Evaluation of Experimental Designs for Constructing Vignette Sets in Factorial Surveys' (2020) 49 Sociological Methods & Research 455

Sullivan AK, 'Piracy in the Horn of Africa and Its Effects on the Global Supply Chain' (2010) 3 Journal of Transportation Security 231

Swain G, 'Wave of Npm Supply Chain Attacks Exposes Thousands of Enterprise Developer Credentials' (*InfoWorld*, 28 August 2025) <<https://www.infoworld.com/article/4047739/wave-of-npm-supply-chain-attacks-exposes-thousands-of-enterprise-developer-credentials.html>> accessed 18 September 2025

—, 'Massive Npm Supply Chain Attack Hits 18 Popular Packages with 2B Weekly Downloads' (*CSO Online*, 9 September 2025) <<https://www.csoonline.com/article/4053725/massive-npm-supply-chain-attack-hits-18-popular-packages-with-2b-weekly-downloads.html>> accessed 18 September 2025

Tabassum M and others, 'Investigating Users' Preferences and Expectations for Always-Listening Voice Assistants' (2019) 3 Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 1

Tabassum M, Kosinski T and Lipford HR, '"I Don't Own the Data": End User Perceptions of Smart Home Device Data Practices and Risks' *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)* (2019)

Taekema S, 'Theoretical and Normative Frameworks for Legal Research: Putting Theory into Practice' [2018] Law and Method

Tajti(Thaythy) T, 'Unprotected Consumers in the Digital Age: The Consumer-Creditors of Bankrupt, Abandoned, Defunct and of Zombie Companies' (2019) 24 Tilburg Law Review 3

Tang J, Birrell E and Lerner A, 'Replication: How Well Do My Results Generalize Now? The External Validity of Online Privacy and Security Surveys' *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)* (2022)

Teo SA, 'Artificial Intelligence, Human Vulnerability and Multi-Level Resilience' (2025) 57 Computer Law & Security Review 106134

Tian H and others, 'Tech Pains: Characterizations of Lived Cybersecurity Experiences' 2020 *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (2020)

Tomassetti AJ, Dalal RS and Kaplan SA, 'Is Policy Capturing Really More Resistant Than Traditional Self-Report Techniques to Socially Desirable Responding?' (2016) 19 *Organizational Research Methods* 255

Toulas B, 'Over 30% of Log4J Apps Use a Vulnerable Version of the Library' (*BleepingComputer*) <<https://www.bleepingcomputer.com/news/security/over-30-percent-of-log4j-apps-use-a-vulnerable-version-of-the-library/>> accessed 6 November 2025

Tourangeau R, Rips LJ and Rasinski K, *The Psychology of Survey Response* (Cambridge University Press 2000)

Tuohy JP, 'Insteon Customers Turned Insteon's Lights Back on' <<https://www.theverge.com/2022/6/9/23161803/insteon-customers-bought-company-restored-service>>

Turner S and others, 'The Exercisability of the Right to Data Portability in the Emerging Internet of Things (IoT) Environment' (2021) 23 *New Media & Society* 2861

Turner S and Tanczer LM, 'In Principle vs in Practice: User, Expert and Policymaker Attitudes towards the Right to Data Portability in the Internet of Things' (2024) 52 *Computer Law & Security Review* 105912

UK National Cyber Security Center, 'Smart Devices: New Law Helps Citizens to Choose Secure Products' <<https://www.ncsc.gov.uk/blog-post/smart-devices-law>>

Urquhart L, Lodge T and Crabtree A, 'Demonstrably Doing Accountability in the Internet of Things' (2019) 27 *International Journal of Law and Information Technology* 1

Urquhart L, Sailaja N and McAuley D, 'Realising the Right to Data Portability for the Domestic Internet of Things' (2018) 22 *Personal and Ubiquitous Computing* 317

Van De Zande T and Jansen S, 'Business Continuity Solutions for SaaS Customers' in Björn Regnell, Inge Van De Weerd and Olga De Troyer (eds), *Software Business*, vol 80 (Springer Berlin Heidelberg 2011)

van 't Schip M, 'The Internet of Forgotten Things: European Cybersecurity Regulation and the Cessation of Internet of Things Manufacturers' (2025) 57 *Computer Law & Security Review* 106152

Van Daalen O, *From Encryption to Quantum Computing: The Governance of Information Security and Human Rights*, vol 38 (TMC Asser Press 2025)

Vandezande N, 'Cybersecurity in the EU: How the NIS2-Directive Stacks up against Its Predecessor' (2024) 52 *Computer Law & Security Review* 105890

Vats T, Sailaja N and Anselmo Polido Lopes F, 'Exploration of User Perspectives around Software and Data-Related Challenges Associated with IoT Repair and Maintenance against Obsolescence: User Study on Software and Data Interactions and Considerations for IoT Repair and Maintenance against Obsolescence' *Proceedings of the 13th Nordic Conference on Human-Computer Interaction* (2024)

Veale M and Brown I, 'Cybersecurity' (2020) 9 *Internet Policy Review*

Von Ditzfurth L and Lienemann G, 'The Data Governance Act: – Promoting or Restricting Data Intermediaries?' (2022) 23 *Competition and Regulation in Network Industries* 270

Walden I, 'Open Source as Philosophy, Methodology, and Commerce: Using Law with Attitude' in Amanda Brock (ed), *Open Source Law, Policy and Practice* (2nd edn, Oxford University Press 2022)

- Wallis T, Johnson C and Khamis M, 'Interorganizational Cooperation in Supply Chain Cybersecurity: A Cross-Industry Study of the Effectiveness of the UK Implementation of the NIS Directive' (2021) 48 *Information & Security: An International Journal* 36
- Wang-Mlynek L and Foerstl K, 'Barriers to Multi-Tier Supply Chain Risk Management' (2020) 31 *The International Journal of Logistics Management* 465
- Webmink In Draft, 'Fixing The CRA For Open Source' <<https://the.webm.ink/fixing-the-cra-for-open-source>>
- Wheeler DA, 'F/LOSS Is Commercial Software' [2009] Open Source Business Resource <<http://timreview.ca/article/229>>
- Wiesemann C, 'On the Interrelationship of Vulnerability and Trust' in Christine Straehle (ed), *Vulnerability, Autonomy, and Applied Ethics* (Routledge 2016)
- Wieser H, Tröger N and Hübner R, 'The Consumers' Desired and Expected Product Lifetimes' [2015] *Product Lifetimes And The Environment*
- , 'The Security of Personal Data under the GDPR: A Harmonized Duty or a Shared Responsibility?' (2017) 7 *International Data Privacy Law* 165
- Woods DW and Ceross A, 'Blessed Are The Lawyers, For They Shall Inherit Cybersecurity' *Proceedings of the 2021 New Security Paradigms Workshop* (Association for Computing Machinery 2022)
- Yadav P and others, 'Network Service Dependencies in Commodity Internet-of-Things Devices' *Proceedings of the International Conference on Internet of Things Design and Implementation* (ACM 2019) <<https://dl.acm.org/doi/10.1145/3302505.3310082>>
- Yao Y and others, 'Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes' *Proceedings of the 2019 chi conference on human factors in computing systems* (2019)
- Zeng E, Mare S and Roesner F, 'End User Security and Privacy Concerns with Smart Homes' *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)* (2017)
- Zeng E and Roesner F, 'Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study' *28th USENIX Security Symposium (USENIX Security 19)* (USENIX Association 2019)
- Zhang S and others, '"Did You Know This Camera Tracks Your Mood?": Understanding Privacy Expectations and Preferences in the Age of Video Analytics' (2021) 2021 *Proceedings on Privacy Enhancing Technologies*
- Zhang Y and others, 'Companies' Participation in OSS Development—An Empirical Study of OpenStack' (2021) 47 *IEEE Transactions on Software Engineering* 2242
- Zreikat AI and others, 'The Integration of the Internet of Things (IoT) Applications into 5G Networks: A Review and Analysis' (2025) 14 *Computers* 250

Legislation

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on

the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)

Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa (Border Interoperability Regulation)

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)

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Digital Operational Resilience Act)

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

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)

Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act)

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

Regulation (EU) 2024/1781 of the European Parliament and of the Council of 13 June 2024 Establishing a Framework for the Setting of Ecodesign Requirements for Sustainable Products, Amending Directive (EU) 2020/1828 and Regulation (EU) 2023/1542 and Repealing Directive 2009/125/EC (Ecodesign Regulation)

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (European Health Data Space Regulation)

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive')

Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (Radio Equipment Directive)

Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules of Information Society services

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS1 Directive)

Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (Sale of Goods Directive)

Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on Certain Aspects Concerning Contracts for the Sale of Goods, Amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and Repealing Directive 1999/44/EC (Digital Content and Digital Services Directive)

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)

Directive (EU) 2024/1799 of the European Parliament and of the Council of 13 June 2024 on common rules promoting the repair of goods and amending Regulation (EU) 2017/2394 and Directives (EU) 2019/771 and (EU) 2020/1828 (Right to Repair Directive)

Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC (Product Liability Directive)

Commission Delegated Regulation (EU) 2022/30 of 29.10.2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive

California Consumer Privacy Act

Case law

Case C-210/96 *Gut Springenheide GmbH and Others v Oberkreisdirektor des Kreises Steinfurt Ä Amt für Lebensmittelüberwachung* ECLI:EU:C:1998:369, [1998] ECR I-4681

Case C-162/97 *Nilsson and others* ECLI:EU:C:1998:554, [1998] ECR I-7477

Case C-220/98 *Estée Lauder Cosmetics GmbH & Co. OHG v Lancaster Group GmbH* ECLI:EU:C:2000:8, [2000] ECR I-135

Case C-646/22 *Compass Banca SpA v Autorità Garante della Concorrenza e del Mercato (AGCM)* ECLI:EU:C:2024:957

HR 6 oktober 1989 ECLI:NL:HR:1989:AB9521 (*Beklamel*)

Florida Court of Appeals, Fourth District, *Grieco v. Daiho Sangyo, Inc.* (15 June 2022)

United States District Court For The Western District Of Pennsylvania, *Cohen v. Johnson & Johnson* (5 October 2022)

Acknowledgements

Over the past few years I have felt supported, inspired, and uplifted by so many people, inside and outside academia. I am very grateful to have the space here to thank (some of) them.

I can only start at the beginning of my academic journey, in Groningen. I had the pleasure of working with some wonderful mentors, who set me up for this PhD journey way back when. Thank you Sofia, for daring to tell me that I needed to shift paths when I most needed to hear it. Thank you to the wonderful people at the 'sectie IT-recht', especially Aline, for a research internship that guided my future interests. Finally, thank you Jeanne and Florian for your full belief and support in writing a socio-legal master's thesis – support that has remained ever since.

I am so happy that I could foster this interdisciplinary interest at iHub. The future is interdisciplinary, as this thesis posits, and iHub exemplifies that future. Thank you to all iHubbies, of which there are – thankfully! – too many to name here. In particular, I am grateful for the wonderful group of (early career) academics that I shared the floor with, including Yong Yong, Marvin, Tim, Liz, Yana, Lisa, Farid, Nina, Jip and to the new cohort who have made the 19th floor feel even more vibrant, including Rik, Emma, Floris and Ana. Thank you Tamar, Bart, and Laura: for creating and fostering this unique space and making it so welcoming and inspiring.

I was also lucky enough to find a second academic home in Edinburgh for a short while. Lachlan: thank you for a wonderful research visit, where I gained even deeper interdisciplinary insights into the world of the Internet of Things. I hope, but am almost certain, that our collaboration is 'to be continued'.

This work would not have been possible without the INTERSCT project and the funding from NWO. Thank you to all the members of WP5 – we have proven that 'governance' is a cornerstone of any research agenda, including cybersecurity. Lorenz, thank you for bringing me onto your wonderful research work. I truly enjoyed and learned a lot from our collaborations, but also our shared dinners and chats over the last few years.

A thesis at the intersection of cybersecurity and law is simply impossible without open-minded and interdisciplinary supervisors. Bart, you always articulate what I *really* want to say within a few minutes of hearing me pitch a research idea. Thank you for teaching me how to present my voice. Pieter, your door was – and is – always open for support. I passed by your (digital) office many times and you never ceased to help me with your encyclopaedic knowledge of the law. Thank you. Frederik, our shared excitement about not just this field of research, but also wonderful music and food, has uplifted me many times over the past few years. Thank you – and I *promise* never to write a passive sentence again.

A big thank you to all my friends and family for continuously asking me about my project over the past few years. Thank you especially to Liv, Tristen, Karin, Ger, Sarah and 'Gorro' for caring about this topic because I cared about it.

The same goes for my dear parents, who have stood by my side and had my back not only during the writing of this thesis – which has made me the ‘privacy guy’ of the family – but for the past almost thirty years. A thank you does not do all that support justice.

Laurie, every single word in this thesis has passed by your keen and critical eyes. Every single struggle was alleviated by not just your unrelenting intelligence, kindness and support, but also your willingness to fully engulf yourself in a topic that is not necessarily yours. Thank you for everything - if I had my way, every day would be your parade.

Summary

A modern digital product is not a singular object, it is the sum of its parts. Digital products depend on numerous components, including open-source software, cloud servers, natural resources and chips.

Cybersecurity threats emerge out of this entangled landscape. Imagine, for instance, that threat actors infiltrate your text editing software and add some malicious code, which your computer automatically installs when updating the software. Such 'supply chain attacks' are not rare. As digital product components increase, so does the attack surface of the digital product.

Indeed, digital production stems from complex supply chains. For instance, the supply chain consists of both the mining company extracting the necessary natural resources as the cloud server on which a product stores data. Moreover, there are technologies, market dynamics, and policies embedded in the functioning of a product, such as in the provision of cloud services. Together, the production and functioning of a modern digital product entails a complex landscape of different actors and processes, which this dissertation defines as 'digital product interdependencies'. Primarily, this dissertation illustrates such interdependencies through Internet of Things devices, digital products which combine hardware and software components with external connectivity (e.g., a smart vacuum).

Over the past few years, the problems of digital product interdependencies are appearing on the academic and political agenda. There are two prominent responses: supply chain cybersecurity and digital sovereignty. Supply chain cybersecurity refers to strategies and policies that aim to ensure adequate cybersecurity throughout supply chains. Digital sovereignty efforts, for instance in the EU, focus on the independence of digital services from foreign states and/or bad actors. In the EU, the field of cybersecurity law is intertwined with these efforts. This dissertation therefore asks: To what extent does, and how could, EU cybersecurity law address the cybersecurity challenges raised by the increasing interdependencies in digital products, as exemplified by Internet of Things devices?

The dissertation starts with a general overview of supply chain cybersecurity, a topic explicitly regulated under the NIS2 Directive. Supply chain cybersecurity is a nascent topic, one which academics and policy makers are developing only over the past few years. However, the topic already appears in EU cybersecurity law: the NIS2 Directive specifically mandates that entities in critical sectors, such as hospitals in the health sector, ensure the 'supply chain security' of their 'network and information systems'. As a result, the NIS2 Directive only places supply chain security in a lateral role among a list of other requirements. Moreover, supply chain security is a requirement for entities in critical sectors, not for digital product manufacturers or developers. This means that a hospital would have to ensure that all their network and information systems come from a secure supply chain; a practically unattainable task.

The regulation of digital product interdependencies through supply chain cybersecurity is currently insufficient, but this insufficiency could be alleviated if EU cybersecurity law regulates components individually. Unfortunately, this is currently not the case. Open-source software, for instance, presented a complex regulatory puzzle for the EU legislators when

they created the Cyber Resilience Act. The Commission fully included open-source software in the scope of this Act, which contains cybersecurity requirements for virtually all software and hardware products. In response, the Council and Parliament largely exempted open-source software, because developers held that they could not cope with the Act's strict requirements. This stance is not surprising, as open-source software is often developed by volunteers, academics, or developers receiving limited financial funding. The struggles of the EU legislators in the regulation of open-source software are emblematic for the regulation of many digital product components. Open-source software is merely a single cog in the wheel—a cog which already requires a complex and specific regulatory puzzle.

The dissertation arrives at the same conclusion for manufacturers. Consumers and manufacturers remain connected, even after purchase: consumers, for instance, expect that manufacturers provide sufficient post-purchase support in case of cyber incidents. Furthermore, consumers expect that manufacturers support Internet of Things devices for longer than five years, the baseline in the Cyber Resilience Act. Both studies demonstrate that consumers depend on the manufacturer to keep the product secure and supported. Indeed, recent incidents demonstrate that if a manufacturer of a digital product ceases to exist, the end user is left with a device that becomes defunct or bereft of updates. This is a problem rooted in digital product interdependencies: the manufacturer depends on an external service for, for instance, data storage, which the consumer, who depends on the manufacturer, can no longer access after the manufacturer ceases to exist. And precisely because the manufacturer ceases to exist, they escape virtually all regulatory scrutiny. Under current EU cybersecurity law, consumers are therefore left with little remedy.

This lack of a remedy is especially problematic for consumers that are rendered vulnerable in digital environments, such as children. The Cyber Resilience Act purports to protect vulnerable consumers in its preamble, but there is little reason for this statement in the actual provisions. This dissertation studies the Cyber Resilience Act from the perspective of two dominant theories on human vulnerability and finds that the Act hardly considers the vulnerability of consumers in the context of cybersecurity. Vulnerable consumers, in contrast to 'regular' consumers, are largely overlooked by EU cybersecurity law, as with open-source software over 'regular' software, or manufacturers that cease to exist over 'regular' manufacturers.

Overall, EU cybersecurity law insufficiently regulates digital product interdependencies, both on the general and individual level. This dissertation therefore proposes an alternative regulatory paradigm for digital products. Regulators should view digital products as ecosystems, not as finished, individual objects. And as environmental law protects both ecosystems and individual organisms, so too must EU cybersecurity law protect digital product ecosystems and individual components that warrant specific cybersecurity measures. There are three steps to this novel regulatory approach: i) the visualisation of digital product ecosystems, which allow for the identification of individual components that warrant specific attention; ii) regulating the security of digital product ecosystems, instead of the security of individual digital products; iii) stimulating the production and adoption of interoperable and open-source components, which offer end users more control over and visibility of the interdependencies embedded in their digital product. This approach will help policy makers and practitioners address the rise of digital product interdependencies and associated cybersecurity risks.

Samenvatting

Een modern digitaal product is niet een op zichzelf staand object, maar de som van zijn delen. Digitale producten zijn afhankelijk van talrijke componenten, waaronder open-source software, cloudservers, natuurlijke bronnen en chips.

Dit verweven landschap bevat risico's met betrekking tot cyberbeveiliging. Elke computer bevat bijvoorbeeld software voor tekstverwerking; kwaadwillenden kunnen deze software infiltreren en een update toevoegen waarmee ze controle over de gehele computer kunnen krijgen. Via de software komen ze dan dus de computer binnen. Dergelijke aanvallen op digitale toeleveringsketen komen steeds vaker voor. Naarmate het aantal componenten van digitale producten toeneemt, vergroot ook het aanvalsoppervlak van het digitale product.

Digitale producten vereisen complexe toeleveringsketens. De toeleveringsketen bestaat bijvoorbeeld zowel uit het mijnbouwbedrijf dat de benodigde natuurlijke hulpbronnen wint als uit de cloudserver waarop een product gegevens opslaat. Naast het productieproces zijn er technologieën, marktdynamieken en beleidsmaatregelen ingebed in het functioneren van een product, zoals bij het aanbieden van clouddiensten. Samen vormen de productie en werking van een modern digitaal product een complex landschap van verschillende actoren en processen, dat dit proefschrift definieert als 'digitale productafhankelijkheden'. Dit proefschrift illustreert dergelijke afhankelijkheden voornamelijk aan de hand van Internet of Things-apparaten, digitale producten die hardware- en softwarecomponenten combineren met externe connectiviteit (bijvoorbeeld een slimme stofzuiger).

De afgelopen jaren zijn de problemen van digitale productafhankelijkheden op de academische en politieke agenda verschenen. Er zijn twee prominente reacties: 'supply chain cybersecurity', oftewel de cyberbeveiliging van de toeleveringsketen, en digitale soevereiniteit. Cyberbeveiliging van de toeleveringsketen verwijst naar strategieën en beleidsmaatregelen die gericht zijn op het waarborgen van adequate cyberbeveiliging in de hele toeleveringsketen. Inspanningen op het gebied van digitale soevereiniteit, bijvoorbeeld in de EU, zijn gericht op de onafhankelijkheid van digitale diensten van buitenlandse staten en/of kwaadwillende actoren. De cyberbeveiligingswetgeving van de EU is sterk verweven met deze inspanningen. Dit proefschrift stelt daarom de vraag: in hoeverre kan EU-cyberbeveiligingswetgeving de problematiek rondom cyberbeveiliging aanpakken die voortvloeit uit de toenemende onderlinge afhankelijkheden in digitale producten, zoals bij Internet of Things-apparaten?

Het proefschrift begint met een algemeen overzicht van cyberbeveiliging in de toeleveringsketen, een onderwerp dat expliciet wordt geregeld in de NIS2-richtlijn. Cyberbeveiliging in de toeleveringsketen is een nieuw onderwerp, dat academici en beleidsmakers pas de afgelopen jaren hebben ontwikkeld. Het onderwerp komt echter al voor in EU-cyberbeveiligingswetgeving: de NIS2-richtlijn schrijft specifiek voor dat entiteiten in kritieke sectoren, zoals ziekenhuizen, de 'beveiliging van de toeleveringsketen' van hun 'netwerken en informatiesystemen' moeten waarborgen. Mede doordat het concept van de beveiliging van de toeleveringsketen nog in ontwikkeling is, lijkt deze eis weggestopt in een lijst van andere beveiligingsverplichtingen. Bovendien is de beveiliging van de toeleveringsketen een vereiste voor entiteiten in kritieke sectoren, niet voor fabrikanten of ontwikkelaars van digitale

producten. Deze verdeling van verantwoordelijkheden betekent dat een ziekenhuis ervoor zou moeten zorgen dat al hun netwerk- en informatiesystemen afkomstig zijn uit een veilige toeleveringsketen, wat in de praktijk een onhaalbare taak is.

De regulering van digitale productafhankelijkheden via NIS2 is momenteel dus ontoereikend, maar deze ontoereikendheid zou kunnen worden verholpen als EU-cyberbeveiligingswetgeving componenten afzonderlijk reguleert. Helaas is dit momenteel niet het geval. Open-source software vormde bijvoorbeeld een complexe puzzel voor de Europese wetgevers toen zij de Cyber Resilience Act opstelden. De Commissie nam open-source software volledig op in het toepassingsgebied van deze wet, die cyberbeveiligingseisen bevat voor vrijwel alle software- en hardwareproducten. In tegenstelling tot dit brede toepassingsgebied hebben de Raad en het Parlement open-source software grotendeels buiten het toepassingsbereik geplaatst, omdat ontwikkelaars van mening waren dat zij niet konden voldoen aan de strenge eisen van de wet. Dit standpunt komt voort uit het feit dat open-source software vaak wordt ontwikkeld door vrijwilligers, academici of ontwikkelaars die maar beperkte financiële middelen ontvangen. De moeizame regulering van open-source software is symbolisch voor de regulering van veel digitale productcomponenten. Open-source software is slechts een radertje in het wiel—een radertje dat op zichzelf al een complex wetgevingstraject vereist.

Dit proefschrift komt tot dezelfde conclusie voor fabrikanten. Consumenten en fabrikanten blijven ook na de aankoop met elkaar verbonden: consumenten verwachten bijvoorbeeld dat fabrikanten voldoende ondersteuning bieden als er na de aankoop bijvoorbeeld een datalek plaatsvindt. Bovendien verwachten consumenten dat fabrikanten Internet of Things-apparaten langer dan vijf jaar ondersteunen, wat de basisnorm is in de Cyber Resilience Act. Beide studies tonen aan dat consumenten afhankelijk zijn van de fabrikant wat betreft de beveiliging en ondersteuning van het product. Recente incidenten bewijzen deze dynamiek: als een fabrikant van een digitaal product ophoudt te bestaan, blijft de eindgebruiker achter met een apparaat dat niet meer werkt of niet meer wordt geüpdate. Dit is een probleem dat voortkomt uit digitale productafhankelijkheden: de fabrikant is afhankelijk van een externe dienst voor bijvoorbeeld gegevensopslag, waartoe de consument, die afhankelijk is van de fabrikant, geen toegang meer heeft nadat de fabrikant is opgehouden te bestaan. En juist omdat de fabrikant is opgehouden te bestaan, vallen zij buiten het toepassingsbereik van veel EU-cyberbeveiligingswetgeving. Onder huidige EU-cyberbeveiligingswetgeving beschikken consumenten dus over weinig rechtsmiddelen.

Dit gebrek aan rechtsmiddelen is vooral problematisch voor consumenten die kwetsbaar zijn in digitale omgevingen, zoals kinderen. De Cyber Resilience Act beoogt volgens de preambule kwetsbare consumenten te beschermen, maar dit blijkt niet uit de daadwerkelijke wetsbepalingen. Dit proefschrift bestudeert daarom de Cyber Resilience Act vanuit het perspectief van twee dominante theorieën over menselijke kwetsbaarheid en concludeert dat de wet nauwelijks rekening houdt met de kwetsbaarheid van consumenten in de context van cyberbeveiliging. Kwetsbare consumenten worden, in tegenstelling tot 'gewone' consumenten, grotendeels over het hoofd gezien door de EU-cyberbeveiligingswetgeving, net als open-source software ten opzichte van 'gewone' software, of fabrikanten die ophouden te bestaan ten opzichte van 'gewone' fabrikanten.

Over het algemeen reguleert EU-cyberbeveiligingswetgeving onvoldoende de onderlinge afhankelijkheden van digitale producten, zowel op algemeen als op individueel niveau. Dit proefschrift stelt daarom een alternatief juridisch kader voor digitale producten voor.

De wetgever moet digitale producten beschouwen als ecosystemen, niet als individuele objecten. Zoals milieuwetgeving zowel ecosystemen als individuele organismen beschermt, moet ook EU-cyberbeveiligingswetgeving zowel digitale productecosystemen als individuele componenten beschermen die specifieke maatregelen vereisen. Dit nieuwe juridische kader vereist drie elementen: i) het onthullen van digitale productecosystemen, waardoor individuele componenten kunnen worden geïdentificeerd die specifieke aandacht verdienen; ii) het reguleren van de veiligheid van digitale productecosystemen, in plaats van de veiligheid van individuele digitale producten; en iii) het stimuleren van de productie en het gebruik van interoperabele en open-source componenten, die eindgebruikers meer controle en inzicht bieden in de onderlinge afhankelijkheden van hun digitale product. Deze aanpak zal zowel beleidsmakers als de praktijk helpen om de toename van digitale productafhankelijkheden en de daarmee samenhangende beveiligingsrisico's aan te pakken.

Curriculum Vitae

Mattis van 't Schip studied Dutch Law (LL.B., specialisation IT Law) and the Research Master in Law (LL.M., cum laude) at the University of Groningen. During his LL.M., he spent a semester at the George Washington University in Washington D.C., United States of America.

His PhD track was part of the INTERSCT project on the cybersecurity of the Internet of Things. Mattis hence co-operated with a host of colleagues across law & technology, computer science, and social-empirical fields. He is highly interested in this type of interdisciplinary work, also due to his position at iHub, Radboud University's 'Interdisciplinary research hub on digitalization and society'. He further deepened this interest during a two-month research visit at the University of Edinburgh, in collaboration with Dr. Lachlan Urquhart. During the research visit, Lachlan and Mattis hosted an interdisciplinary workshop on the cybersecurity of the Internet of Things.

During his PhD, Mattis presented his work at a range of legal and non-legal conferences, including TILTing, Digital Legal Talks, and the ONE Conference. He also co-led a workshop for early career scholars working on European cybersecurity law, guest lectured at the University of Groningen and in lectures from colleagues across disciplines at Radboud University (e.g., ethics, AI studies). Mattis peer-reviewed for Computer Law & Security Review, the FAccT conference, CPDP, and Internet Policy Review, among others. After finalising his PhD, Mattis will remain at Radboud University as a post-doctoral researcher.