

CompLex



Senter for rettsinformatikk / Avdeling for forvaltningsinformatikk

Christiane Hunsbedt

Security Requirements for Connected Consumer Products

Poorly secured toys and smartwatches for children: Is current legislation adequate to restrict their market access, and how may this be regulated going forwards?

1/2021



UiO : Det juridiske fakultet

Henvendelser om denne bok kan gjøres til:

Senter for rettsinformatikk

Postboks 6706 St. Olavs plass

0130 Oslo

Tlf. 22 85 01 01

<http://www.jus.uio.no/ifp/om/organisasjon/seri/>

ISSN 2703-8777 Complex (online)

Grafisk produksjon: 07 Media AS – 07.no

Preface

This paper is based on a Master thesis written under the aegis of the project “Security in Internet Governance and Networks: Analysing the Law” (SIGNAL). Work on the SIGNAL project has been undertaken by the Norwegian Research Center for Computers and Law (NRCCL) attached to the Department of Private Law, University of Oslo. The Norwegian Research Council and UNINETT Norid AS have funded the project. Thanks go to these institutions for support. I also wish to thank all project members for their contributions and advice during the writing process, particularly my supervisor Professor Tobias Mahler, and Professor Lee Bygrave, Luca Tosoni, and Peter Davis. Special thanks go to Drífa Hrund Daníelsdóttir for discussing with me the decisions of the Icelandic Consumer Agency. Thanks go also to Karianne Stang for her support and encouragement. I am grateful to the various stakeholders who have contributed to my research, especially the Norwegian Directorate for Civil Protection (DSB) where Astrid Lie Olsen was highly enthusiastic in clarifying pertinent questions, as well as the Norwegian Consumer Council (Forbrukerrådet), the European Consumer Organisation (BEUC), the Norwegian Communications Authority (Nkom), the Icelandic Consumer Agency (Neytendastofa), and the Icelandic Post and Telecom Administration (PFS). They have all provided useful insights into current legal interpretations, relevant challenges, and regulatory needs for improved consumer product security. However, any errors in this paper are my responsibility alone. The original thesis was finalised in August 2020, and this paper is a shortened-down version with some minor updates. References to legal instruments are to their amended state as of 1 March 2021.

Oslo, 14 March 2021

Christiane Hunsbedt

Contents

Preface.....	3
Abbreviations	6
Abstract	8
1 Introduction	9
1.1 Outline	10
1.2 Factual Delimitations.....	11
1.3 Types of Safety-Related Risks in Connected Products	12
2 Legal Overview	16
2.1 EU Product Safety Legislation	16
2.1.1 Possible Different Safety Scopes under Relevant Product Safety Directives.....	18
2.1.1.1 The General Product Safety Directive vs. the Radio Equipment Directive	18
2.1.1.2 The Radio Equipment Directive vs. the Toy Safety Directive.....	19
2.2 Some Adjoining Legal Frameworks.....	19
2.2.1 Data Protection Regulation.....	19
2.2.2 Cybersecurity Act.....	21
2.2.3 Security of Network and Information Systems Directive.....	22
2.2.4 Summary	23
3 To What Extent Are Exploitable Security Weaknesses Encompassed under the Product Safety Directives?.....	24
3.1 The Directives' Criteria for Relevant Risks.....	25
3.1.1 Harm: Physical or Health Impacts.....	26
3.1.1.1 Protection of the Safety and Health of Persons.....	26
3.1.1.2 Protection of Property under RED Article 3(1)(a).....	27
3.1.1.3 Summary	28
3.1.2 Causality: The Relevance of Risks Involving Third-Party Interference	28
3.1.2.1 What It Entails that the “Product” Must Be Safe.....	28
3.1.2.2 Summary	29
3.1.3 Dynamic Interpretation and EU Law Objectives.....	30
3.2 Summary	31

4	Administrative Practice on “Security-for-Safety”	32
4.1	Safety Gate Alerts	32
4.2	Icelandic Market Surveillance Authorities	33
4.2.1	Legal Basis for the Decisions	33
4.2.2	Choice of Law: Lex Generalis vs. Lex Specialis	34
4.3	Norwegian Market Surveillance Authorities	35
4.4	Summary	36
5	Possible Regulatory Approaches to Consumer Product Security.	38
5.1	Regulatory Needs	38
5.2	An Extended Safety Scope under EU Product Safety Legislation. . .	39
5.3	Delegated Acts under RED Article 3(3)(e-f)	41
5.4	A New Cybersecurity Law	44
5.5	Summary and De Lege Ferenda	45
6	Summary and the Way Forward	47
	Table of references.	49

Abbreviations

BEUC	Bureau Européen des Unions de Consommateurs (The European Consumer Organisation)
CJEU	Court of Justice of the European Union
CCC	Cybercrime Convention
CEN	Comité Européen de Normalisation (The European Committee for Standardization)
CENELEC	Comité Européen de Normalisation Électrotechnique (The European Committee for Electrotechnical Standardization)
CSA	Cybersecurity Act
DA	Delegated Act
DSB	Direktoratet for Samfunnssikkerhet og Beredskap (The Norwegian Directorate for Civil Protection)
EO	Economic Operator (i.e., manufacturers, authorised representatives, importers, and distributors)
EEA	European Economic Area
ETSI	European Telecommunications Standards Institute
EU	European Union
GDPR	General Data Protection Regulation
GPSD	General Product Safety Directive
LVD	Low Voltage Directive
MS	Member State

MSA	Market Surveillance Authority
NISD	Security of Network and Information Systems Directive
NLF	New Legislative Framework
PFS	Póst- og Fjarskiptastofnun (The Icelandic Post and Telecom Administration)
PSL	EU Product Safety Legislation
RED	Radio Equipment Directive
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
TSD	Toy Safety Directive

Abstract

This paper examines the ability of current EU product safety law to address risks of “security-for-safety”, i.e., where security weaknesses can lead to physical safety impacts. Product safety legislation holds the advantage of mechanisms to restrict products’ market access. The applicability of these rules for security risks has been subject to discussions and diverging national administrative practice over the last few years. This paper seeks to provide some clarity on the current remit of relevant directives and on what criteria their scopes rely. Central factors for the relevance of “security-for-safety” risks regard the physicality of impacts and the causality between the product and the harm. It will be argued that certain risks relying on intentional actions fit under the analysed directives. However, for risks where the causal link between the product vulnerability and the physical impact is weak, there is currently a legal gap. This points towards a need for regulatory updates. The paper therefore proceeds to discuss three proposed regulatory approaches to product security. Considering strengths and shortcomings of these approaches, the paper leans towards addressing current regulatory gaps and needs under a new, holistic cybersecurity law.

1 Introduction

In 2016 and 2017, the Norwegian Consumer Council (Forbrukerrådet) uncovered security risks in several toys and smartwatches for children.¹ Several products were revealed to allow third parties to listen in and even speak with the users, access their personal data, and track their locations.² At the core of the problem was a lack of simple technical safeguards: the risks would have been significantly reduced had the manufacturers of the products implemented basic security measures.³

Besides raising general awareness of lax security in connected products, these investigations highlighted shortcomings in the legal framework. It is currently not clear whether non-secure devices can be removed from the market. This creates uncertainties for businesses who produce and market products, and for authorities enforcing the rules. It also puts a strain on what reasonable expectations consumers can have in respect of devices they buy and use.

Market surveillance authorities (MSAs) have traditionally considered product safety legislation (PSL) as not dealing with cybersecurity risks.⁴ However, when physical objects are connected to computer systems, safety and security become mutually dependent and their distinction is obscured. The traditional approach of MSAs has therefore been characterised by the European Consumer Organisation (BEUC) as “completely outdated” and “too narrow” to protect consumers.⁵ BEUC has instead advocated the relevance of “security-for-safety” risks (i.e., situations where safety relies on security measures) under PSL.⁶ “Security-for-safety” could refer to all security weaknesses with a potential to induce physical harm, or it may be defined more narrowly (see Section 1.3).

An exceptionally wide interpretation of “safety” applied by the Icelandic Consumer Agency (Neytendastofa) in 2018 prompted new discussions across the

1 Forbrukerrådet 2016 (*#ToyFail*), Forbrukerrådet 2017b (*#WatchOut*).

2 Forbrukerrådet 2017b, p. 3.

3 Forbrukerrådet 2016, pp. 34-35.

4 ANEC and BEUC 2018, p. 10.

5 Ibid., pp. 5, 10.

6 Ibid., pp. 10-11. BEUC applies a wide definition of “security-for-safety”, which is apparent, i.e., from their consideration that Neytendastofa’s decision 42/2018 (see Section 4.2) is encompassed (ANEC and BEUC 2019, p. 21).

EU.⁷ In early 2020, the European Commission (hereinafter “the Commission”) indicated that the “safety” concept in EU product safety legislation should be understood as “extended”, covering “also cyber risks”.⁸ However, the Commission did not spell out the implications of its stance, leaving unclear the extent to which cybersecurity risks are currently encompassed and whether explicit legal amendments are necessary.⁹

1.1 Outline

After some central definitions, relevant “security-for-safety” risks are categorised in Section 1.3. Section 2 then describes EU product safety legislation (PSL). As product safety directives regulate products’ market access,¹⁰ they are the main focus of this paper. Some adjoining frameworks are, however, also mentioned.

The ability of relevant PSL to address different “security-for-safety” risks is examined in Section 3 under the research question: “to what extent do the general product safety requirements of the Radio Equipment Directive (RED), Toy Safety Directive (TSD) and General Product Safety Directive (GPSD) encompass security weaknesses in connected toys and smartwatches for children when they can be exploited to cause harm”. A pivotal factor is whether causal requirements exclude all risks catalysed by third-party interference. Based on the analyses, a likely scope of the directives’ requirements is proposed.

The practical significance of these discussions is illustrated by diverging national interpretations, both in choice of law and perceived legal scope (Section 4). Thereafter, three proposed approaches to address legislative gaps are explored in Section 5: (i) extending the scopes of current product safety directives; (ii) delegated acts under the RED; and (iii) developing an entirely new framework. These approaches’ strengths and shortcomings in effectively dealing with exploitable product security weaknesses are assessed against regulatory needs. Section 6 then summarises and concludes the paper.

7 Neytendastofa decisions 42/2018 and 46/2018, Áfrýjunarnefnda decision 1/2019, Safety Gate alert A12/0157/19 (*Enox Safe-Kid-One*).

8 COM(2020) 64 (*Report*), p. 6.

9 The latter was recommended by ANEC and BEUC in 2018 (p. 11), whatever the current scope. 10 There is an apparent need for legal mechanisms to prevent market access for non-secure products. It has occurred that products with disclosed vulnerabilities have remained available for consumer purchase (see BEUC 2019, Forbrukerrådet 2017a, Forbrukerrådet 2019b, p. 4). Further, more recent tests have revealed that smartwatches previously examined by Forbrukerrådet (2017b) still have lax security (Stykas 2019).

1.2 Factual Delimitations

The discussions herein concern market access requirements for wirelessly connected toys and children's smartwatches with exploitable security weaknesses. Wirelessly connected "toys"¹¹ and smartwatches consist of physical goods with built-in computer functionalities,¹² including a wireless connection to the Internet,¹³ either directly or via another device (e.g., by Bluetooth). Children's products are in focus as their lower age and maturity impel a higher need for product security and safety.¹⁴ The discussions herein will nevertheless frequently be relevant for a wider category of consumer connected devices.

Connected products can be referred to as "cyber-physical systems".¹⁵ The key aspect of such systems is interaction between the physical and digital worlds, for instance sensing and processing data (e.g., voice recordings or geolocation) to perform actions with (intended or unintended) physical impacts. Connected products are often inextricably linked with their services, as these may be necessary for the devices to work as intended. This gives rise to the term "associated services".¹⁶ Such services are *part of the product*, where the product is connected to a network, and *necessary for the physical product's functioning*, for example its communication with another device or back-end servers.¹⁷ The physical product and its associated services are herein considered parts of the "product" as a whole. Security weaknesses in these services can affect the physical product and its surroundings.

Security can be understood as "the absence or limitation of vulnerabilities or threats".¹⁸ For a security risk to be present, the threat must be sufficiently probable and the potential harm severe enough. Risks discussed herein often rely on

11 Understood in accordance with TSD Art. 2(1).

12 Smartwatches for children are not considered toys, even if they can access interactive games (TSD Annex I Art. 14, see European Commission 2016 (*Guidance to the TSD*), p. 84), but wireless communications properties make them subject to the RED.

13 Wirelessly connected products apply radio waves (RED Art. 2(4)), making them "radio equipment" subject to the RED (Art. 2(1)). Wired connected products are instead subject to the Low Voltage Directive (LVD), to which the RED is *lex specialis*. Security weaknesses and measures (although depending on the applied technology) can be similar regardless of whether the products use wires.

14 For instance, children are more vulnerable to develop putative friendships with such devices, confide in them, share sensitive data, or trust information or instructions they provide (Westlund 2017, Shasha et al. 2019).

15 See Fink et al. 2018, p. 4.

16 Defined in ETSI 303 645, p. 9.

17 Standalone services are outside the GPSD scope (rec. 9). Discussed in COM(2020) 64 (*Report*), pp. 10-11.

18 Tamò-Larrieux 2018, p. 105.

exploitation of product weaknesses (e.g., inadequate authentication or encryption mechanisms)¹⁹ to gain unauthorised digital access to stored or transmitted information (hacking)²⁰.

Although both “security” and “safety” regard protection from “danger”,²¹ they have traditionally been considered separate concepts. Neither is easily defined,²² but as a rough indication, safety appears more associated with accidental harm to persons (or perhaps even physical property), while “security” focuses on *intentional* interference by a third party with a broader variety of possible consequences (including impacts on a system’s integrity, confidentiality or availability).²³ The latter needs not (though it may) involve physical injuries; security can also impact, for instance, personal data or mental states, including “a feeling of safety”.²⁴ This highlights the close relationship between the concepts. Security measures may sometimes be a necessary component to reduce risks of physical danger. The two concepts can then overlap. Their distinction is increasingly obscured as technology advances.

The focus herein is on risks that rely both on weaknesses within the system and on their exploitation by a third party to cause harm (i.e., exploitable security weaknesses), particularly physical harm. Intentionality (more associated with security) and physicality of impacts (more associated with safety) will therefore be central factors in the following discussions.

1.3 Types of Safety-Related Risks in Connected Products

“Security-for-safety” in the wide sense can include any security weakness that can cause – more or less directly – a product to induce physical harm, at least if

19 As frequently uncovered in children’s connected products (e.g., Strick 2019, pp. 23–31, Valente and Cardenas 2017, Chu et al. 2018).

20 The term “hacking” is used herein regardless of the skills required or whether the actions are covered by criminal law.

21 Oxford University Press 2007, pp. 2647, 2733.

22 This challenge is augmented by the fact that most EU languages apply only one term for both concepts. Only three language versions of the GPSD (see Art. 2(b)), RED (see Art. 3(1)(a)), and TSD (see Art. 10(2)) – concentrating on “safety” – apply a different term from the “security”-focused Art. 5(f) of the GDPR: English (“safety” and “security”), Bulgarian (“безопасен” and “сигурност”) and Estonian (“ohutus” and “turvalisuse”). Still, the use of wider-reaching terms in several languages does not preclude a narrower construction (e.g., equivalent to the English “safety” term) in legal texts.

23 Karanikas 2018, pp. 547–548, Oxford University Press 2007, pp. 2647, 2733.

24 Oxford University Press 2007, p. 2733.

persons are affected.²⁵ A narrower definition could be limited, for instance, to direct “security-for-safety” as elaborated below. It is useful to distinguish between different types of scenarios to facilitate assessment of what “security-for-safety” risks may be encompassed under current and future legislation.²⁶ The categories below are separated based on whether *third-party intentional actions* are required to make the risks unfold, whether there are potential *physical harm* impacts, and how *directly* that harm is caused by the product. These factors correspond with legal criteria under the relevant directives (see Sections 3.1.1-3.1.2) and will aid the legal discussions. Note that there may be vague distinctions and partial overlaps between the categories. They should therefore be considered with some flexibility.

Type 0: Traditional Safety

Several risks are undisputedly encompassed by the product safety directives and can be referred to as traditional safety risks. Product properties then present a risk of *direct harm to persons*,²⁷ *without involvement of intentional actions*.

Risks involving “traditional safety” do not rely on the product to be connected. For instance, small parts in toys can be a choking hazard. They also include digital malfunctions: a software error impacting the brakes in a car can cause serious harm.²⁸ Persons may also be harmed due to malfunctions in, for instance, heating equipment, kitchen appliances, or certain toys.

Type 0 risks entail:

- physical harm;
- directly from the product;
- no intentional third-party interference.

Moving on to the more disputed categories, three types of scenarios are drawn up for the purposes of this paper. Contrary to type 0, these all rely on *third-party exploitation of security weaknesses*:

Type 1: Direct “Security-for-Safety”

Type 1 risks involve a hacker *exploiting security weaknesses* to cause *physical or health harm*. The harm must emanate *directly* from the physical product. For

²⁵ This wide understanding of “security-for-safety” is applied by BEUC (ANEC and BEUC 2019, p. 21), though it is not clear whether they also include harm to property.

²⁶ A similar categorisation is made in European Commission 2020a (*Sub-Group on AI working document*), p. 2. Types 1 and 2 herein build on two of their categories, while “traditional safety” and “fraud” are additional.

²⁷ Or “property” under RED Art. 3(1)(a), see Section 3.1.1.2.

²⁸ E.g., Safety Gate alert A12/00154/20.

toys and wearables, a hacker might, for instance, induce the product to emit loud noise or to overheat and start burning, thereby causing harm. These are *direct* “security-for-safety” risks. There are no reported cases of such risks being uncovered in toys, but the Jeep mentioned in Section 4.1 is an example.

Type 1 risks entail:

- physical harm;
- directly from the product;
- third-party intentional interference combined with product weaknesses.

Type 2: “Personal Security” (Indirect “Security-for-Safety”)

Risks affecting “personal security” are more frequently uncovered.²⁹ Like type 1 risks, they rely on *third-party exploitation* of security weaknesses and may lead to *physical or health harm*. However, contrary to type 1 risks, the harm would be *less directly* caused by the product itself; more operations take place between the weaknesses and the harm, and the harm is more performed by the third party using the toy or smartwatch “as a tool”.³⁰ A hacker may gain personal information, build trust, or make the child behave in a way which enables him/her to harm the child. For instance, access to a smartwatch’s geolocation could facilitate physical access to the user. A child can also be manipulated, for example, to open the front door to facilitate wrongdoings. Still, both the product weakness and the third party are necessary causes for the harm.³¹

Type 2 risks entail:

- physical harm;
- less directly from the product;
- third-party intentional actions, based on weaknesses in the product.

Type 2 should be seen against risks with purely digital impacts and no potential for physical harm to persons. This limit is vague and will not be elaborated herein. However, one more scenario, straddling this limit, must be mentioned:

29 E.g., Cayla and i-Que (Forbrukerrådet 2016, Forbrukerrådet 2017b), and Dino (Valente and Cardenas 2017).

30 COM(2020) 65 (*White Paper*), p. 12, fn. 36.

31 The likelihood for these scenarios to unfold (hereunder also the effort required to exploit a weakness) is rather part of case-by-case risk assessments (see GPSD Art. 2(b)) considering probability and severity. Such assessments are not explored herein.

Type 3: Fraud Causing Loss of Value³²

Fraud relies on *third parties' intentional actions*. However, as it does not entail physical harm to persons, the directness factor fits poorly for these scenarios. The risk is rather that the device owner suffers a *loss of value*, which can be regarded as a kind of property. An example is the possibility described for hackers to make the Enox smartwatch “dial premium-rate phone numbers”³³ to cause financial loss. It is disputable whether such risks can be considered to involve safety-related harm (to property, see Section 3.1.1.2), but the possibility calls for a separate fraud category here to facilitate further discussions.

Risks uncovered in toys and smartwatches are usually types 2 or 3.³⁴ For instance, the Enox smartwatch could be made to call expensive numbers, thereby enabling *fraud*.³⁵ Unauthorised access to *personal data* is a common risk (e.g., access to Enox' location history)³⁶ as are other *privacy* infringements (e.g., listening in on children's conversations with their toys).³⁷ Still, situations can be envisaged under types 0 and 1 that do not include any of these aspects. This should be kept in mind for Section 5.

The criteria separating the above scenarios will contribute to assess what risks are currently addressed under the RED, TSD and GPSD.

32 This category is added to create a bridge between the risk categories here and the legal discussions in Section 3 and is without prejudice to any legal definitions of fraud.

33 Neytendastofa decision 42/2018, p. 3.

34 Testing of the doll “My friend Cayla” and the robot “i-Que” revealed, i.e., risks of hacking (Bouvet 2016, p. 12). Their Bluetooth connection required no authentication, making it easy for anyone to pair with the toys and communicate with the users (ibid., pp. 12-13). Such basic safeguards have been revealed in several Bluetooth-connected toys (Smithers 2017). Smartwatches have been found not to encrypt their data communications with the back-end servers, allowing eavesdropping, access to the child's geolocation, or manipulation of data in the watches, hereunder what calls they would accept (Neytendastofa decisions 42/2018 and 46/2018, Mnemonic 2017, pp. 11-20). Valente and Cardenas (2017, pp. 22-23) discovered shortcomings in the wifi-connected toy dinosaur “Dino”: voice commands sent to its back-end server were secured by encryption, but use of a small pool of encryption keys identical for all Dino toys facilitated eavesdropping. Lacking authentication mechanisms also made “audio injection” possible (ibid., p. 23), although cumbersome.

35 Neytendastofa decision 42/2018, p. 3.

36 Ibid.

37 Smithers 2017, Valente and Cardenas 2018, pp. 22-23.

2 Legal Overview

This section provides a preliminary description of product safety legislation, as a foundation for the Section 3 analyses, followed by a brief overview of some central frameworks that apply in parallel.

2.1 EU Product Safety Legislation

European product safety legislation (PSL) consists of several instruments,³⁸ where the General Product Safety Directive (GPSD) applies to the extent that sector-specific legislation does not (see Section 2.1.1.1).³⁹ Instruments aimed at specific product categories or properties include the Radio Equipment Directive (RED) for wirelessly connected products and the Toy Safety Directive (TSD) for toys. References to “the product safety directives” throughout this paper comprise the RED, TSD and GPSD.

Product safety law has two main aspects. Firstly (and the focus herein), it poses proactive requirements for economic operators (EOs), particularly manufacturers,⁴⁰ to ensure compliance as a condition for placing products on the market.⁴¹ Secondly, products’ fulfilment of safety requirements is controlled through market surveillance mechanisms.⁴²

The general safety requirements set out in the GPSD, RED and TSD are broad and vague. This is characteristic of New Approach legislation, which refers to a change in legislative approach during the mid-1980s from more detailed directives to broadly phrased requirements.⁴³ The directives are therefore complemented by voluntary standards to make compliance more manageable. Compli-

38 Binding and to be transposed by all EU Member States (TFEU Art. 288) and EEA EFTA countries (Norway, Iceland and Lichtenstein) (EEA Agreement Art. 7).

39 *Lex specialis*, OJ C 272/1 2016 (*Blue Guide*), p. 23.

40 Decision 768/2008/EC Annex I, Art. R2, compare R4-R5. “Manufacturer” is defined in Decision 768/2008/EC Annex I, Art. R1(3). “Economic operators” (EOs) are manufacturers, authorised representatives, importers, and distributors (Decision 768/2008/EC Annex I, Art. R1(7)).

41 Placement on the market refers to the first time a product is made available in the EU/EEA area (Decision 768/2008/EC Annex I, Art. R1(2)).

42 See TSD Art. 3(15).

43 OJ C 272/1 2016 (*Blue Guide*), pp. 7-9.

ance with “harmonised standards” provides a presumption of conformity with the directives.⁴⁴

The TSD and RED currently have no harmonised standards for exploitable cyber weaknesses. Existing standards focus on traditional safety risks (type 0).⁴⁵ It is, however, the directives’ requirements, and not the standards, that are mandatory: the directives can encompass more than the harmonised standards, which could be the situation for certain cybersecurity risks. EOs must then find other ways to ensure compliance.

The New Approach was developed further into the New Legislative Framework (NLF) in 2008, providing a more complete system with conformity assessments, accreditation, and market surveillance.⁴⁶ EOs demonstrate compliance based on conformity assessments and declarations.⁴⁷ CE marks signal a product’s compliance, both to authorities and consumers.⁴⁸ Insufficient documentation or marking equals “formal non-compliance”.⁴⁹

The directives oblige the Member States to transpose the rules into national law.⁵⁰ The national rules are enforced by market surveillance authorities (MSAs).⁵¹ If a product poses sufficient risks, the relevant MSA can require its withdrawal from the market, recall from consumers, or ban its marketing or supply.⁵²

44 GPSD Art. 3(2)(2), RED Art. 16, TSD Art. 13. Harmonised standards are standards developed by recognised EU standards organisations (CEN, CENELEC or ETSI) and adopted based on a request from the Commission and referenced in the Official Journal of the European Union (Regulation 1025/2012 Art. 2(1)(b-c)).

45 European Commission 2019b (*TSD harmonised standards*), European Commission 2020b (*RED harmonised standards*).

46 OJ C 272/1 2016 (*Blue Guide*), pp. 9-10.

47 Decision 768/2008/EC Annex I, Art. R1(12).

48 Decision 768/2008/EC Annex I, Art. R1(16), Regulation 765/2008 Art. 30. CE marks (Conformité Européenne) are mandatory under the RED (Art. 20) and TSD (Art. 16(1)), but not under the GPSD since it is older than the NLF.

49 Decision 768/2008/EC Annex I, Art. R34, OJ C 272/1 2016 (*Blue Guide*), p. 107. Formal shortcomings have constituted decisive grounds for several decisions on connected products, e.g., Nkom case 2017/4446.

50 GPSD Art. 21(1), see TFEU Art. 288(3), EEA Agreement Art. 7(b).

51 Market surveillance is regulated under Regulations 765/2008 and 2019/1020. See COM(2017) 795 (*Proposal*) as part of the new “Goods Package” (COM(2017) 787).

52 GPSD Art. 8(1)(d-e), see Art. 2(h) (withdrawal) and Art. 2(g) (recall). MSA measures must always be proportional to the kind and level of risk (Regulation 765/2008 Art. 21(1), OJ C 272/1 2016 (*Blue Guide*), p. 107). Recall, being the most serious measure, should be a “last resort” (GPSD Arts. 5(1)(5) and 8(2)(3)).

2.1.1 Possible Different Safety Scopes under Relevant Product Safety Directives

Products must often comply with several, simultaneously applicable product safety instruments.⁵³ The *lex specialis* principle then gives preference to the stricter or more specific requirements.⁵⁴ Both the TSD and RED are *lex specialis* to the GPSD. If a type of risk is not regulated by sector specific legislation, but is encompassed under the GPSD, this *lex generalis* directive will complement applicable *lex specialis* to fill the gaps.⁵⁵ The GPSD can *only* be used if and to the extent the sector-specific instruments do not adequately cover the risks.⁵⁶

Possible differences between the safety scopes of the RED, TSD and GPSD are therefore decisive for what instruments apply. The following subsections consider the relative scopes of the directives *if* and to the extent they can deal with exploitable security weaknesses in products. They do not anticipate the conclusions to the *de lege lata* interpretations, but rather provide a necessary foundation for them.

2.1.1.1 The General Product Safety Directive vs. the Radio Equipment Directive

Since the GPSD shall ensure product safety when *lex specialis* requirements are lacking or inadequate,⁵⁷ its general safety requirement is likely not narrower than those of the sector-specific directives. The GPSD requirement might, however, be wider.

The sectoral directives cover risks also beyond their specialised focuses. For instance, although the RED is aimed at radio wave properties, it covers “*all health and safety risks*”.⁵⁸ This points to the broadest possible inclusion of risks, equivalent to the risk scope under the GPSD. The consequence would be that when the RED applies, the GPSD safety provisions do *not* apply.⁵⁹

Although a relatively complete overlap of risk scopes between the RED and GPSD appears likely, the diverging approach of the Icelandic Consumer Agency

53 OJ C 272/1 2016 (*Blue Guide*), pp. 22-23.

54 Eckhoff 2001, p. 357.

55 GPSD Art. 1(2)(2).

56 GPSD Art. 1(2)(2)(a), rec. 12.

57 GPSD Art. 1(2), rec. 5.

58 European Commission 2019c (*Guide to RED*), p. 36, emphasis added. See similarly European Commission 2016 (*LVD Guidelines*), p. 60. Although not legally binding, Commission statements are occasionally taken into account for the interpretation of EU legislation (see Opinion by Advocate General Hogan in Case C-523/18 *Engie Cartagena S.L. v. Ministerio para la Transición Ecológica*, para. 43).

59 Similarly stated in European Commission 2019a (*Comparison/Differences between RED and other acts*), p. 2.

(Neytendastofa) (see Section 4.2) calls for including the GPSD in the discussions herein.

2.1.1.2 The Radio Equipment Directive vs. the Toy Safety Directive

The RED and the TSD are both applicable *lex specialis* for wirelessly connected toys. Preference should then be given to the more specific of the two. Which instrument this is, can be debated. Toy aspects could be considered more specialised than an internet connection.⁶⁰ Meanwhile, where the risks rely on radio-wave properties, the RED may be closer to address them.

There exists little guidance for whether the requirements of the TSD and the RED cover all the same risks. Considering the TSD safety scope as equivalently broad to that of the RED and GPSD would ensure a more consistent use of terms. The alternative – to apply different general safety scopes for each directive – could foster uncertainty and create coordination challenges between MSAs, thereby impeding enforcement. It therefore seems reasonable to assume that these directives provide similar general safety requirements. Although minor differences are possible, this assumption of overlap underlies the approach of considering all three directives in parallel in Section 3.

2.2 Some Adjoining Legal Frameworks

Several EU legal frameworks are relevant for exploitable security weaknesses and apply in addition to the product safety rules. None of them provide the same possibilities to restrict market access, although certain enforcement mechanisms may ultimately have similar effects. In the following, the relevance of the GDPR, CSA, and NISD is briefly examined.

2.2.1 Data Protection Regulation

The GDPR and ePrivacy Directive apply to processing of personal data,⁶¹ also when embedded in consumer products and services. “Personal data” refers to “any information relating to an identified or identifiable natural person”,⁶² here-

60 At least for “traditional” safety aspects, see *ibid.*, p. 3.

61 GDPR Art. 2(1), ePrivacy Directive Art. 3(1). The ePrivacy Directive requires, i.a., confidentiality of communications (Art. 5) and appropriate security measures (Art. 4(1)). This directive is to be replaced with the ePrivacy Regulation (COM(2017) 10) as *lex specialis* to the GDPR for privacy and personal data in electronic communications. For security, this proposal refers to compliance with GDPR Art. 32 “to avoid potential overlap” (Burton 2020, p. 632). The focus herein therefore remains on the GDPR.

62 GDPR Art. 4(1). The threshold for what is “personal data” is cast low (C-434/16 *Peter Nowak v. Data Protection Commissioner*, para. 34, see Bygrave and Tosoni 2020, pp. 109-113).

under user photos, speech recordings, and identifiable geolocations. Unauthorised access to such data affects personal data security.⁶³

Not all products process personal data, and not all security risks involve personal information. For instance, the Norwegian Consumer Council (Forbrukerrådet) considers the GDPR inapplicable if a water boiler can be hacked to create dangerous situations.⁶⁴ To clarify, this relies on case-specific factors; if personal data are linked to the water boiler, the GDPR may apply. The point is that not all security risks discussed herein are covered by the GDPR, increasing the importance of other instruments' abilities to address them.

Where the GDPR applies, Article 25 prescribes “appropriate measures” to be built-in from the design stage and made the default settings,⁶⁵ and Article 32 requires “appropriate” security measures.⁶⁶ Specifications on how to comply are expected to be set out in codes of conduct and certification schemes under Articles 40 and 42 respectively.⁶⁷ These are voluntary soft law mechanisms, but they can be useful for the industry to achieve and demonstrate compliance.⁶⁸

The GDPR places obligations on data controllers and processors.⁶⁹ Unless they also hold these roles, EOs manufacturing, importing, or selling products are not made responsible.⁷⁰ Although legally non-binding,⁷¹ the recitals mention that producers “should be encouraged to take into account”⁷² data protection in the product design and development. This demonstrates a desire or perceived need to distribute responsibility between more actors.

Data protection authorities cannot directly ban a product's market access. However, they can ban non-compliant processing of personal data,⁷³ which may equal stopping the associated service. This can force the product off the market

63 Tosoni 2020a, p. 192.

64 Forbrukerrådet 2019a, p. 3.

65 See GDPR rec. 78.

66 See GDPR rec. 83. This can include encryption (Art. 32(1)(a)), and confidentiality and integrity safeguards (Art. 32(1)(b)). What is “appropriate” relies on a case-by-case assessment (see Tamò-Larrieux 2018, p. 169).

67 GDPR Arts. 25(3), 32(3), see also Art. 40(2)(h). See Bygrave 2020, p. 577.

68 Although this paper focuses on hard law, softer measures are important for industry practices (Eliantonio and Stefan 2018, p. 462, NOU 2018:14 Chapter 7).

69 GDPR Chapter 4. Art. 32 obliges data controllers and processors. Art. 25 only mentions controllers, although processors are indirectly caught by Art. 25 obligations through Art. 28(1). See Bygrave 2020, p. 578.

70 CSES and Tech4i2 (2020a (*Impact Assessment*), pp. 29-30) point to this as a legal gap.

71 Case C-136/04 *Deutsches Milch-Kontor GmbH v. Hauptzollamt Hamburg-Jonas*, para. 32.

72 GDPR rec. 78.

73 GDPR Art. 58(2)(f).

in practice. In addition, fines and reputational damage may serve as deterrents.⁷⁴ The GDPR can thus have significant effects on product security.

Toys and smartwatches without functional services can nevertheless remain for sale on the market, and children who already own them can find them useless – for instance that the toy will not speak anymore.⁷⁵ Applying the GDPR on product security thus leaves consumer protection issues,⁷⁶ which points towards a need for market restrictive mechanisms for non-secure products.

2.2.2 Cybersecurity Act

The Cybersecurity Act (CSA) includes a cybersecurity certification framework for digital products, services, and processes.⁷⁷ The CSA was adopted in 2019 and specified schemes are expected to be rolled out gradually. They have potential to cover a wide range of products and services, and of cybersecurity risks, both upon design and throughout product lifecycles.⁷⁸ Although their contents and impacts are still unknown, these schemes can become significant for dealing with product security.

A point of criticism against CSA schemes is that their voluntary nature may compromise their uptake.⁷⁹ On the other hand, certified products may get a competitive advantage against non-certified products, particularly if compliance is made visible.⁸⁰ There is, however, also a risk that security differences throughout the market increase if some manufacturers comply while others do not.

“Security-by-design” appears a pivotal aim for CSA schemes.⁸¹ Recital references to the related “privacy by design”⁸² fosters an expectation that the CSA will “attempt to complement the aims of Article 25 GDPR”.⁸³ This can lead to consid-

74 Data protection authorities can impose fines (GDPR Art. 58(2)(i), see Art. 83).

75 This happened for Dino (Fowler 2018). Consumer purchases legislation may then be relevant (e.g., the Sale of Goods Act (kjøpsloven) in Norway). The applicability of such rules on service-related defects calls for further assessments (NOU 2018:14, p. 61). NOU 2018:14 (p. 88) points to a need for effective access to purchase cancellation based on cybersecurity shortcomings.

76 Forbrukerrådet 2019b, p. 4.

77 CSA Title III.

78 See CSA Art. 51.

79 See, i.a., ANEC and BEUC 2019, p. 9. See also CSA Art. 56(2). The uptake of CSA schemes remains to be seen. If insufficient, Art. 56(3) contains a possibility to make them mandatory, although this would be some way ahead.

80 E.g., by labels (CSA Art. 54(1)(i)).

81 See CSA Art. 51(1)(i), recs. 2 and 12.

82 CSA rec. 41.

83 Bygrave 2020, p. 579.

erable overlaps between the CSA, GDPR, and current or future PSL requirements, where the instruments may support each other or cause unfortunate fragmentation (see Section 5).

2.2.3 Security of Network and Information Systems Directive

The NIS Directive requires essential service operators and digital service providers to take “appropriate and proportionate” measures to manage security risks to their systems.⁸⁴ Toys and smartwatches do not contain essential services. However, if data is transferred between the toy or smartwatch and a cloud service, the service provider is subject to NISD requirements.⁸⁵

Lax security in the cloud can weaken the overall security of the cyber-physical system. Still, there is no indication that possible physical impacts (which could be quite removed from the cloud service as such) have any significant part in NISD security risk assessments. Further, although infringements can lead to penalties,⁸⁶ the services are not thereby stopped. Neither will lax security directly affect the products’ market access.

Note also that several product challenges are not related to cloud services, for example risks involving unauthorised access to data stored on the device, or data transmissions via non-secure Bluetooth connections. These are outside the NISD’s remit.

The NISD’s scope has been criticised,⁸⁷ and the Commission has proposed a new directive – NISD2 – to replace it. This proposal encompasses more sectors, including the manufacture of electronic and electrical equipment.⁸⁸ The NISD2 could thus address connected watches and toys. In addition, stricter enforcement mechanisms are proposed, including administrative fines,⁸⁹ which could provide more bite. The proposed NISD2’s abilities and adequacy for addressing current challenges call for further assessments. However, it will not include market access mechanisms like those set out by PSL.

⁸⁴ NISD Arts. 14(1) and 16(1). See too Art. 4(4-6).

⁸⁵ NISD Art. 16, see Annex III, nr. 3. See definition in Art. 4(19), rec. 17. The is unless the service provider is exempted as a micro or small enterprise (NISD Art. 16(11)).

⁸⁶ NISD Art. 21.

⁸⁷ ANEC and BEUC 2019, pp. 24-25, COM(2020) 823 (*Proposal*), p. 3.

⁸⁸ COM(2020) 823 (*Proposal*) Annex II, 5(c-d), see Eurostat 2008, Section C, Divisions 26-27.

⁸⁹ COM(2020) 823 (*Proposal*) Art. 31.

2.2.4 Summary

Several EU frameworks have relevance for exploitable product security weaknesses. However, they are aimed at various actors and risks and provide different enforcement mechanisms. Only product safety legislation explicitly provides market restrictive mechanisms, which appears central to remedy the challenges discussed herein. Still, the roles of the GDPR, CSA, and possible NISD2 – and their expected underlying softer mechanisms – require attention.⁹⁰

90 Both the GDPR and CSA are relatively new instruments, and specifications are still expected (e.g., codes of conduct and certification schemes), making it difficult to yet assess their full scopes and efficiency.

3 To What Extent Are Exploitable Security Weaknesses Encompassed under the Product Safety Directives?

Product safety legislation (PSL) pertains to the “safety” of products.⁹¹ A variety of security risks can more or less directly lead to safety impacts (“security-for-safety”). This has fostered the argument that “products will not be safe if they are insecure”.⁹² Security may thus be a necessary consideration under product safety provisions. This section examines *to what extent the RED, TSD and GPSD general product safety requirements encompass security weaknesses in connected toys and children’s smartwatches when they can be exploited to cause harm.*

The Section 1.3 categorisation provides a starting point for considering what “security-for-safety” scenarios may be relevant under the directives. Type 0 risks (traditional safety) are undisputedly encompassed. The legislation’s applicability for types 1 (direct “security-for-safety”), 2 (“personal security”), and 3 (fraud causing loss of value) is less certain. These risks rely on purposeful exploitation of weaknesses, which makes causality requirements central for their relevance (Section 3.1.2).

Whatever the conclusion – whether all, some, or no “security-for-safety” risks are encompassed – legal gaps for product security will remain (as discussed in Section 5). The cases mentioned in Section 4 nevertheless demonstrate the practical significance of de lege lata assessments. Furthermore, being contained in existing provisions holds the advantage of immediate enforceability, thereby shortening consumers’ exposure to dangerous products.

The starting point for interpreting existing legislation is the EU frameworks themselves,⁹³ where the provisions’ “wording, context and objectives” are cen-

91 The assessment of what is a “safe product” can be divided into two. First, the risks must be within the directives’ scopes. This is the focus herein. Even if the risks are relevant under the directives, they are not automatically “dangerous” (GPSD Art. 2(c), contra “safe” in GPSD Art. 2(b)). Instead, a risk assessment must be performed to determine whether the product is safe (GPSD Art. 2(b). See Regulation 765/2008 Art. 20), i.e., whether the potential hazards are sufficiently probable and severe to require measures. Risk assessments are highly case-specific and not explored herein.

92 As mentioned in CSES and Tech4i2 2020a (*Impact Assessment*), p. 113.

93 The CJEU has exclusive competence for binding interpretation of EU legislation (TEU Art. 19(3)(b), TFEU Art. 267(1)(b)), but there does not seem to exist any CJEU rulings that shed light on the relevance of security under PSL.

tral factors.⁹⁴ Vague phrasings increase the necessity of looking beyond the legal wording and consider also the directives' internal context, as well as the legal objectives of both the safety requirements and of EU law in general.⁹⁵ The role of technological developments in creating legal challenges prompts a need to discuss to what extent the provisions can be interpreted dynamically to minimise legal lacunae.

3.1 The Directives' Criteria for Relevant Risks

The Radio Equipment Directive (RED) applies both to smartwatches and toys. The latter is also subject to the Toy Safety Directive (TSD). In addition, the General Product Safety Directive (GPSD) is *lex generalis*. These three instruments are herein referred to as the “product safety directives”.

The RED, TSD and GPSD will be assessed in parallel, as the presumption made in Section 2.1.1 that they contain equivalent scopes for exploitable security weaknesses can justify occasionally drawing from all three to support a common interpretation. Nevertheless, bearing in mind that the Icelandic Consumer Agency (Neytendastofa) appears to take a different approach (see Section 4.2), the possibility for varying safety remits cannot be discarded in advance. Still, the GPSD is applicable only if the RED and TSD cover a narrower risk scope.

The directives set out criteria for relevant risks under the legislation, particularly for harm impacts and risk causes. Their general safety requirements are worded as follows:

The RED requires radio equipment to “be *constructed so as to ensure* [...] the *protection of health and safety of persons and of domestic animals and the protection of property*”.⁹⁶

For toys, the TSD provides that they “shall *not jeopardise the safety or health of users or third parties* when they are *used as intended or in a foreseeable way*”.⁹⁷

94 Case C-558/15 *Vieira de Azevedo and Others v. CED Portugal Unipessoal, Lda and Instituto de Seguros de Portugal – Fundo de Garantia Automóvel*, para. 19.

95 Case C-621/18 *Andy Wightman and Others v. Secretary of State for Exiting the European Union*, para 47, case 6/72 *Europemballage Corporation and Continental Can Company Inc. v. Commission of the European Communities*, para. 22: “one has to go back to the spirit, general scheme and wording [...], as well as to the system and objectives of the Treaty”. See Lenaerts and Gutiérrez-Fons 2013, p. 47.

96 RED Art. 3(1), emphasis added.

97 TSD Art. 10(2), emphasis added. TSD Annex I also sets out specific safety requirements as *lex specialis* to the general requirement.

Under the GPSD, producers can only place “safe products” on the market.⁹⁸ A product is “safe” when it, “under normal or reasonably foreseeable conditions of use [...] does not present any risk or only the minimum risks compatible with the product’s use, considered to be acceptable and consistent with a high level of protection for the safety and health of persons”.⁹⁹

3.1.1 Harm: Physical or Health Impacts

Security risks can produce different kinds of consequences (see Section 1.3). The directives focus on protection of persons’ safety and health, and to some extent property protection.

3.1.1.1 Protection of the Safety and Health of Persons

The GPSD and RED protection of the safety and health of “persons”,¹⁰⁰ and the TSD protection of “users and third parties”,¹⁰¹ include risks both to the child and others – “even complete outsiders”.¹⁰²

As for what kinds of impacts on persons are relevant, a product’s safety is determined by whether it entails “risks”.¹⁰³ Of the three directives, only the TSD defines this term. Assuming that “safety” and “risk” is similar across these instruments (Section 2.1.1), at least for protection of persons,¹⁰⁴ the TSD definitions are applied here.

The TSD bases both factors for “risk” – probability and severity – on the concept of “harm”¹⁰⁵ and defines “harm” as “*physical injury or any other damage to health*”.¹⁰⁶ All degrees of physical harm to persons are included,¹⁰⁷ and possibly

98 GPSD Art. 3(1), emphasis added.

99 GPSD Art. 2(b), emphasis added.

100 GPSD Art. 2(b), RED Art. 3(1)(a). An additional protection of property under the RED is discussed in Section 3.1.1.2.

101 TSD Art. 10(2).

102 For the TSD, see European Commission 2016 (*Guidance to the TSD*), p. 36.

103 See GPSD Art. 2(b).

104 The TSD definition of harm regards protection of persons and cannot necessarily be applied for the property protection set out in the RED.

105 TSD Art. 3, nr. 28, TSD Art. 3, nr. 27.

106 TSD Art. 3, nr. 26, emphasis added.

107 Cfr. “any” in TSD Art. 3, nr. 26, supported by “safety” being described as including “all minor and major injuries” in European Commission 2016 (*Guidance to the TSD*), p. 36). It depends instead on a risk assessment whether the potential harm is sufficiently severe to render a product “dangerous”.

also a wide range of health effects.¹⁰⁸ Both type 1 and 2 risks could fit under this phrasing, as they can ultimately induce harm to persons.

3.1.1.2 Protection of Property under RED Article 3(1)(a)

Connected toys and wearables may damage physical objects or other values. RED Article 3(1)(a) requires protection of “property” in addition to persons. The construction of “property” is decisive for whether risks impacting for example finances or data, hereunder economic loss due to fraud (see type 3 in Section 1.3), are relevant under RED Article 3(1)(a).

The legal wording provides little guidance. Although a broad legal definition could include “[a]nything that can be owned”, both tangibles and intangibles,¹⁰⁹ the RED term may also be narrower.

Looking to the internal structure of Article 3(3), both the current RED and its predecessor contain *litrae* referring to protection against personal data, privacy, and fraud.¹¹⁰ These provisions are dormant, but they can be activated by the Commission,¹¹¹ in which case they would apply in addition to the other Article 3 essential requirements.

Under the premise that the legislator is a “rational actor”, there should not be unnecessary overlaps of provisions.¹¹² It can be argued that RED Article 3(3)(e-f) would not have been included in the directive if the legislator considered their contents already encompassed under “property” in RED Article 3(1)(a). Admittedly, both “personal data and privacy” and “fraud” can encompass more than a wide “property” term (e.g., deception without loss of value). Those remaining aspects would, however, be relatively narrow compared to the *litrae*’s wide phrasings. This intimates that the legislator likely did not intend for “fraud” or “data protection” to be generally included under RED Article 3(1)(a). “Property” under RED Article 3(1)(a) therefore presumably focuses on tangibles (e.g., use of frequencies that negatively impact other equipment), not personal data or fraud.

108 The Commission has promoted the relevance of “mental safety”, including even mental well-being (COM(2020) 64 (*Report*), p. 8, COM(2020) 65 (*White Paper*), p. 15). Connected products can be used to harass, scare, or even abuse children, which could cause mental “damage to health”. Unfortunately, the lack of cases provides little basis to assess the relevance of mental health under these directives. Note also that if such risks are included, the lower limits of “damage to health” (see TSD Art. 3, nr. 26) for relevant mental impacts should be clarified.

109 Law 2018, p. 536. Compare also the Cybercrime Convention (CCC, Art. 8) which applies a “property” term related to digital fraud.

110 RED Art. 3(3)(e-f). Also, Directive 1999/5/EC on Radio Equipment and Telecommunications Terminal Equipment art. 3(3).

111 RED Art. 3(3)(2), see Art. 44. This is subject to an ongoing initiative (see Section 5.3).

112 Lenaerts and Gutiérrez-Fons 2013, p. 13.

3.1.1.3 Summary

Risks relevant under the RED, TSD and GPSD must hold potential for *physical injury or health damage consequences to persons*. The RED also requires *property* protection, although this appears focused on tangible objects, not including personal data or financial fraud.

3.1.2 Causality: The Relevance of Risks Involving Third-Party Interference

The directives require causality, as relevant risks must come from the product.¹¹³ Where third-party interference is necessary for a risk to catalyse, the harm's cause is twofold, relying on a combination of security weaknesses and their exploitation. For instance, if lax security enables a hacker to gain access and make a device overheat and burn, both product weaknesses and third-party actions are necessary causes to the fire. The directives' ability to address such exploitable weaknesses depends on risks with multiple causes fitting under their scopes.¹¹⁴

3.1.2.1 What It Entails that the “Product” Must Be Safe

The directives prescribe that the *products* must be safe.¹¹⁵ This requires a causal link between the device and the potential harm, so that relevant risks are traceable back to product properties.

There is, however, no indication in the wording of how big a part the product must play in the causal picture: whether it must simply be *a* cause, the main cause, or even the sole cause. Thus, as long as product properties contribute to physical harm, risks involving third-party exploitation might be relevant.

113 See “present” in GPSD Art. 2(b), TSD Art. 18, RED Art. 10(5)(2). It should be mentioned that the directives also require risks to be present “under normal or reasonably foreseeable use” (GPSD Art. 2(b), similarly RED Art. 17(1), rec 46, and TSD Art. 10(2)). This excludes purposeful misuse by legitimate users, hereunder the child (for whom “reasonably foreseeable use” may require a higher threshold). However, it does not seem to regard third parties’ digital access outside the consumer’s control and beyond what they can reasonably prevent (compare also with the Product Liability Directive (PLD), where damage caused by product defects combined with third-party actions are relevant, with a differentiation between interference which the injured person can be held responsible for (Art. 8(2)), and third parties acting outside the injured person’s control (Art. 8(1))). A hacker may realise product risks within the frames of – and despite – the child’s own reasonably foreseeable use. This criterion does not appear to hinder manufacturer responsibilities to implement measures against exploitable security weaknesses.

114 The relevance of purely *accidental* risks based on digital properties (type 0) is not disputed (DSB e-mail 26.5.2020. Compare Regulation 2019/1020 Art. 14(4)(a) where embedded software is relevant for MSAs). Associated services can be considered part of the devices (Section 1.2), so that their risks stem from the product.

115 GPSD Art. 3(1), see Art. 2(b). Although this may seem less clear from RED Art. 3(1) (“constructed so as to ensure”) and TSD Art. 10(2) (“not jeopardise” safety), the phrasings in RED Art. 10(5) (2) and TSD Art. 18 confirm that a causal link between the product and the potential harm is necessary.

The directives' internal contexts may provide further indications. Firstly, for the RED, "fraud" in Article 3(3)(f) would always involve third parties. This demonstrates that the legislator considered risks involving interference to fit under the directive and the product safety legal system.

Further, the TSD contains a specific requirement involving also "outside" factors as combined causes with product weaknesses.¹¹⁶ Although this regards more random influences than malicious actions, it demonstrates encompassment of risks *not solely* stemming from the product but requiring external influences to unfold. This could strengthen the possibility to include also risks relying on purposeful interference under the general safety requirements.

"Security-for-safety" risks seem to fit under the directives. Still, type 1 risks (where the product is made to cause harm) and type 2 risks (where the product is used as a tool for the hacker to cause harm) may have to be assessed differently under the causality requirement. Unfortunately, the provisions provide little guidance for the "directness" required, i.e., to what extent there can be intermediate links between product and harm.

Risks of third parties digitally affecting a product can be invisible and unintuitive to average consumers.¹¹⁷ They may expect any safety and security risks to have been minimised upon design. From a consumer protection perspective, it is unfortunate to place responsibility on consumers for risks largely (depending on the case) outside their control. Manufacturers, on the other hand, can often implement suitable safeguards independent of whether third-party actions are necessary for risks to unfold.

There may be little reason to separate between a product starting to burn on its own (type 0) and the same effect being provoked by a hacker (type 1). The same argument may be harder to apply for risks of "personal security" (type 2), where the harm often relies more on the hacker's own physical execution. The chains of events can then also be less foreseeable and less expected.

3.1.2.2 Summary

Risks involving product weaknesses *and* exploitation are not excluded by the wording, nor do they seem entirely misplaced under the legislation. Different types of interference may, however, have to be considered differently. While consumer protection considerations support inclusion of some security-related

¹¹⁶ TSD Annex II, IV, nr. 7.

¹¹⁷ "[R]easonable consumer expectations" can be relevant to consider (GPSD Art. 3(3)(f), rec. 16). See also "consumer protection" in TFEU Art. 114(3).

risks, if the product weakness is causally distant from the impact, risks may be less predictable for the manufacturer to safeguard against. As the wording provides no explicit guidance beyond requiring that the harm comes from the product, it may be stretching the provisions too far to include more than type 1 risks.¹¹⁸

3.1.3 Dynamic Interpretation and EU Law Objectives

The above discussions have demonstrated a flexibility in the legal wording for “security-for-safety” risks: hacking which induces physical harm may to some extent be encompassed.

Technological developments, hereunder increasing overlaps between safety and security, can affect the contents of legal provisions.¹¹⁹ Completely excluding “security-for-safety” scenarios may fail to achieve the directives’ main objective of “safety and health”,¹²⁰ as well as adequate consumer protection.¹²¹ This can support encompassing at least type 1 risks.

The desire for EU harmonisation encourages a sufficiently wide interpretation that MSs don’t feel the need to implement additional rules nationally.¹²² Concomitantly, MSs seem to have a relatively wide margin of appreciation when implementing the directives.¹²³ This creates a potential for highly varying interpretations (as found in Section 4), in practice generating the opposite of harmonisation.¹²⁴

At the same time, restrictions on the free movement of goods require proportionality and sufficient legal basis.¹²⁵ Including situations too far from the explicit legal wording may equal unjustified restrictions to products’ market access.

118 The wording must not be stretched too far (Joined Cases C-310/98 and C-406/98 *Hauptzollamt Neubrandenburg v. Leszek Labis* (C-310/98) and *Sagpol SC Transport Międzynarodowy i Spedycja* (C-406/98), para. 46).

119 GPSD Art. 3(3)(e), Regulation 2019/1020 rec. 30, TFEU Art. 114(3). The GPSD is “broad-based” (rec. 5), i.e. to facilitate adaption to the changing state of the art. Although encompassment of certain cybersecurity-related risks was foreseen in RED (and its 1999 predecessor) Art. 3, overlap situations necessitating consideration of security under the general safety requirements appear less anticipated.

120 GPSD Art. 2(b). Interpretation of EU law requires account of legal objectives (Lenaerts and Gutiérrez-Fons 2013, pp. 24-26).

121 TFEU Art. 114(3). Consumer protection was also mentioned as a reason for an “extended” safety concept in COM(2020) 64 (*Report*), p. 6.

122 TEU 105(1), see TSD rec. 48.

123 See TFEU Art. 288(3), EEA Agreement Art. 1(1).

124 See Vries 2010, p. 1.

125 See TFEU Arts. 34-36.

Applying a rule beyond its intended scope, even if the interpretation is textually possible and desirable based on technological developments, could also make it “applicable in situations it was not suited for, and thereby [] dangerous”.¹²⁶ The present risks differ from what the directives have traditionally dealt with, which calls for cautiousness. Type 2 risks, where higher reliance on the hacker to perform the harm weakens the causal link between product and impact, could be too removed from the provisions’ intended scopes.

Also, in light of ongoing initiatives to regulate product security (see Section 5), a careful approach may be sensible of not encompassing *too* much under current rules that cannot easily be read from their wording. It is preferable to rely on explicit provisions for intrusive measures like market access restrictions.

3.2 Summary

The RED, TSD and GPSD require impacts of physical or health harm to persons, and the RED also encompasses damage to a narrow category of property.

The causality requirement does not exclude risks involving third parties. The question is rather what “security-for-safety” risks are sufficiently directly caused by the product to be relevant. Balancing the need for dynamic interpretation to ensure adequate safety and consumer protection against risks of overstretching the provisions (particularly the causality requirement), it seems reasonable to consider type 1 risks (direct “security-for-safety”) encompassed, while excluding type 2 risks (“personal security”).

This entails an adjustment of the traditional, narrower safety term. Nevertheless, most security risks are still outside the current legal scope, hereunder “personal security”, fraud, and other cybersecurity risks beyond safety. Three possible approaches to remaining legal gaps are explored in Section 5.

126 Svantesson 2011, p. 261.

4 Administrative Practice on “Security-for-Safety”

Market surveillance is carried out by national authorities (MSAs). Different interpretations of product safety rules, here illustrated by Icelandic and Norwegian administrative decisions, demonstrate the practical significance of analysing the current legal scope.

4.1 Safety Gate Alerts

Through the Safety Gate rapid alert system (previously known as Rapex), European MSAs share information on products that pose “serious risks”.¹²⁷ Notifications rely on national assessments.¹²⁸

Only two Safety Gate alerts have involved exploitable cybersecurity weaknesses, concerning a Jeep and a smartwatch for children.¹²⁹ Both products had security flaws enabling unauthorised access to their systems, and both were considered by the alerting MSAs to breach safety requirements. The low number of notifications intimates that most authorities consider few – if any – exploitable weaknesses relevant under PSL.

While the smartwatch contained risks of “personal security” and fraud (types 2 and 3), the Jeep presented more direct “security-for-safety” risks (type 1): it had “software security gaps”¹³⁰ (particularly lax authentication) which allowed hackers to “disable the steering, abruptly engage the brakes, and even turn off the engine”.¹³¹ If exploited, a possible road accident with personal injuries would be directly caused by the vehicle, expedited by a hacker.¹³²

127 GPSD Art. 12(1), see Art. 2(d), Regulation 765/2008 Art. 20(2). See GPSD Art. 10, Annex II.

128 MSA practice is based on national laws transposing the directives. These may contain minor differences from the EU frameworks, accounted for here by consideration of the national provisions. Note that publication in Safety Gate does not imply Commission approval of the alerting authorities’ interpretation. It rather seems that the Commission regarded the Enox alert (A12/0157/19) as a “test-case” to observe other MSs’ reactions (TIE 2019).

129 Safety Gate alerts A12/1671/15 (*Jeep*) and A12/0157/19 (*Enox Safe-Kid-One*).

130 Safety Gate alert A12/1671/15.

131 Fink et al. 2018, p. 9. Greenberg (2015) describes the hack of this Jeep in further detail.

132 Vehicle risks often entail potential for severe harm and may thus easily be considered “serious”. Note also that vehicles are subject to differently phrased product safety *lex specialis* requirements than children’s products (Regulation 2019/2144 Art. 4(4)).

The Jeep notification led to measures also in two other MSs,¹³³ which indicates a certain traction for including type 1 risks under vehicle safety legislation. No other MSAs took action based on the smartwatch alert. The assessment of the Icelandic MSA issuing this alert is explored in the following.

4.2 Icelandic Market Surveillance Authorities

Decisions from the Icelandic Consumer Agency (hereinafter “Neytendastofa”) from late 2018 apply an exceptionally broad “safety” scope on two smartwatches: Enox and Wonlex GW100.¹³⁴ Both were banned from sale, and the Enox watch was also withdrawn. A 2019 appeal decision on Enox confirmed the original conclusion,¹³⁵ and a Safety Gate alert was issued.¹³⁶

Both watches lacked encryption of data communications with the back-end server, enabling unauthorised access whereby a hacker could, *inter alia*, change data, listen in, or shut down the watch.¹³⁷ These risks affect “personal security” (type 2), as they can be exploited to harm the child. Fraud was also possible, as the watches could be made to call premium-rate numbers.¹³⁸

In Section 3, these risks were considered to fall outside the scope of the product safety directives. They nevertheless form the basis for Neytendastofa’s decisions.

4.2.1 Legal Basis for the Decisions

Neytendastofa found the watches not to be safe under the Icelandic Act on Product Safety and Official Market Control (law 134/1995, transposing the GPSD) §§8-9.¹³⁹ This was the only formal basis for the decisions,¹⁴⁰ although other acts were considered (including the Electronic Communications Act (law 81/2003, transposing the RED)).¹⁴¹

133 Safety Gate alert A12/1671/15.

134 Neytendastofa decisions 42/2018 and 46/2018. Wonlex GW100 was also assessed by the Norwegian Communications Authority (Nkom). Both Neytendastofa and Nkom found it to lack CE marks and have unsatisfactory conformity declarations (Nkom case 2017/4446-22, p. 1, Neytendastofa decision 46/2018, p. 8). Nkom alerted the supplier who stopped selling the watches in Norway (Nkom case 2017/4446-22, p. 2). Different laws and reasons underlie Nkom’s and Neytendastofa’s decisions.

135 Áfrýjunarnefnda (the Icelandic Consumer Appeals Committee) decision 1/2019.

136 Safety Gate alert A12/0157/19 (*Enox Safe-Kid-One*).

137 Neytendastofa decision 42/2018, p. 3.

138 Ibid.

139 “geti ekki talist örugg vara” (Neytendastofa decisions 42/2018, p. 8 and 46/2018, p. 8).

140 Áfrýjunarnefnda decision 1/2019(65).

141 Icelandic law 81/2003 transposes the RED after a 2018 amendment (Icelandic law 41/2018).

According to Neytendastofa, the Enox decision and the later appeal decision confirm that “safe product” (“örugg vara”) can include cybersecurity risks.¹⁴² However, the decisions fail to discuss the remit of the safety term. As Neytendastofa seems to consider their applied wide scope of “safety” to be in accordance with the GPSD (which does not include property protection),¹⁴³ and not just a particularity of Icelandic law, the decisions appear concentrated on risks affecting “personal security” (type 2). These risks rely on exploitation of security weaknesses. Including them under law 134/1995 must mean that Neytendastofa does not consider the causality requirement to exclude risks involving third-party actions (see Section 3.1.2). They don’t even seem to require a particularly direct link between product and harm.

4.2.2 Choice of Law: *Lex Generalis* vs. *Lex Specialis*

Neytendastofa has a coordinating role when cases fall under several authorities.¹⁴⁴ This is a particularity of Icelandic law, aiming to promote cooperation and coherent assessments.¹⁴⁵ The Icelandic Post and Telecom Administration (Póst- og Fjarðskiptastofnun, hereinafter PFS) therefore made an advisory assessment based on the Electronic Communications Act (law 81/2003) §§61(1-2) and 65(1), where they found the CE marking and documentation inadequate. This would make grounds for market restrictions. Instead of leaving the decisions to the PFS on this basis, Neytendastofa made decisions on both watches and based them on cybersecurity risks under law 134/1995, formally independent of law 81/2003.¹⁴⁶ This despite that their coordinating role only provides for coordination, not decision making (i.e., *lex specialis* still applies).

The applicability of the sector specific law 81/2003 was undisputed.¹⁴⁷ The use of law 134/1995 therefore raises questions on the scope and applicability of *lex gen-*

¹⁴² Neytendastofa e-mail 27.5.2020.

¹⁴³ The GPSD applies for the “safety and health of persons” (GPSD Art. 2(b)), which can hardly be extended to include fraud (e.g., the possibility to make the Enox watch call premium-rate phone numbers, see Neytendastofa decision 42/2018, p. 3). Although law 134/1995 §8(1) (which is mainly equivalent to GPSD Art. 2(b)) also protects property (“eignir”) (similarly to RED Art. 3(1)(a)), Neytendastofa (e-mail 27.2.2020) refers to the Safety Gate alert as based on the GPSD.

¹⁴⁴ Icelandic law 134/1995 §14(1)(4).

¹⁴⁵ According to the DSB (e-mail 20.5.2020), no similar coordinating role exists in Norway, neither based on the Product Control Act (produktkontrollloven) nor in practice. NOU 2018:14 (Chapter 18) has pointed to a need both for clearer division of tasks between relevant authorities and for improved cooperation.

¹⁴⁶ Áfrýjunarnefnda decision 1/2019(65) on Enox.

¹⁴⁷ Ibid. (56), see Neytendastofa decision 42/2018, p. 7 that the radio equipment properties of the watches fall under Icelandic law 81/2003.

eralis relative to the sector-specific legislation.¹⁴⁸ When *lex specialis* applies to the product type, *lex generalis* should only be used if the risks in question are not covered by the sector-specific law.

In the PFS's opinion, the "word öryggi does not represent cyberrisks or any kind of data" under the sector-specific law 81/2003 but is limited to the "safety" of persons.¹⁴⁹ The only way to address the smartwatches under that legislation would be through formal non-compliance (which the PFS had uncovered). To instead apply law 134/1995 based on cybersecurity risks requires this legislation to cover a wider remit of risks than law 81/2003.¹⁵⁰ Neytendastofa's choice of law thus implies a view that the *lex generalis* law 134/1995 has a wider risk scope, *inter alia* for risks affecting "personal security". The extent of this scope is not specified.¹⁵¹

4.3 Norwegian Market Surveillance Authorities

Norwegian authorities apply a much narrower interpretation of the product safety rules than Neytendastofa.¹⁵² Considering the toys Cayla and i-Que, the Norwegian Directorate for Civil Protection (DSB) concluded that risks of third parties connecting, listening in, and communicating with the child – i.e., risks affecting "personal security" – were not covered by existing toy safety requirements.¹⁵³ They still stand by this being outside their authority.¹⁵⁴

The DSB considers the safety requirements to concern only "direct physical health damage" (type 0).¹⁵⁵ These risks are *accidental*, based for example on small parts, sharp edges, or even software errors. As the risks of Cayla and i-Que

148 Áfrýjunarnefnda decision 1/2019(60-61) pointed (for Enox) to arguments of the telecommunication properties' conventionality and visibility as reasons for applying law 134/1995. However, if the products use radio waves, the conventionality of their functionalities is no condition for applying the RED (or law 81/2003). Neither does its applicability rely on the radio properties' visibility. Watches that transmit radio waves are subject to radio equipment *lex specialis*.

149 PFS e-mail 10.6.2020.

150 Recall that Section 2.1.1.1 argued that the EU directives GPSD and RED have overlapping risk scopes. Like the GPSD, law 134/1995 §1(4) explicitly states that it should only be applied when it covers risks that are inadequately addressed by the sectorial legislation.

151 It would also rely on a case-by-case assessment (Neytendastofa e-mail 27.5.2020).

152 The Norwegian Communications Authority (Nkom) have assessed several smartwatches under the Norwegian Radio Equipment Regulation (radioutstyrsforskriften), but they have not considered cybersecurity properties. The focus herein is therefore on the DSB's assessment.

153 DSB case 2016/11181-19, p. 1, based on the Norwegian Toy Safety Regulation (leketøyforskriften), transposing the TSD.

154 Per DSB e-mail 24.8.2020.

155 DSB e-mails 7.4.2020 (attachment) and 24.8.2020.

relied on *intentional* hacking, they considered them outside the legal scope.¹⁵⁶ In other words, they interpret the causality requirement (see Section 3.1.2) narrowly, excluding all exploitable security weaknesses (hereunder types 1, 2 and 3). The DSB therefore lacked legal basis to intervene.¹⁵⁷

4.4 Summary

Neytendastofa and the DSB represent two interpretational extremities of possible PSL safety scopes. The DSB limits it to physical life and health consequences without third-party intentional interference (type 0 only).¹⁵⁸ In contrast, Neytendastofa includes more indirect possibilities of harm based on exploitation of cyber weaknesses,¹⁵⁹ encompassing at least some risks affecting “personal security” (type 2). However, their choice of law is questionable, and it is not clear exactly how wide-reaching they consider the legislative scope, as they provide no explicit legal reasoning on the limits of “safety”.

BEUC nevertheless agrees with Neytendastofa’s approach and encourages its further uptake.¹⁶⁰ They consider Neytendastofa’s argument to be “security-for-safety”, in the sense that product safety legislation is relevant when security weaknesses present any risk of physical harm, however indirect.¹⁶¹

Still, most MSAs seem to consider risks of “personal security” and fraud outside the scope of product safety law. For toy safety, both stakeholders and the Commission agreed on this relating to privacy in 2017,¹⁶² and similar views have been expressed by the Commission more recently.¹⁶³

¹⁵⁶ DSB e-mails 25.5.2020 and 24.8.2020.

¹⁵⁷ DSB case 2016/11181-19, p. 1.

¹⁵⁸ DSB e-mails 7.4.2020 (attachment) and 25.5.2020.

¹⁵⁹ Neytendastofa decisions 42/2018 and 46/2018.

¹⁶⁰ ANEC and BEUC 2019, p. 21.

¹⁶¹ Ibid.

¹⁶² Expert Group on Toy Safety 2018, pp. 5-6 (*Minutes from meeting 22.6.2017*). Discussed risks included the possibility to listen in on Cayla (type 2). More direct “security-for-safety” scenarios (type 1) were seemingly not considered. Although expert group meetings are non-binding and not decisive for the interpretation of EU legislation (Andersen 2011, p. 16), they “may nonetheless have a significant impact on how member states interpret and implement EU law” (ibid. p. 25). Accordingly, no MSAs applied PSL on Cayla or toys with similar risks (CSSES and Tech4i2 2020b, pp. 45-46). Neither did other MSAs react against Enox after the Safety Gate alert (A12/0157/19).

¹⁶³ SWD(2020) 287, p. 76.

It is also worth keeping in mind that MSs shall not impede the market access of products that conform to the directives' essential requirements.¹⁶⁴ *If* a decision stretches a provision's wording *too* far – for instance by applying a too wide risk scope – this could entail a non-legitimate restriction of products' market access. At the same time, the MSs likely have a considerable margin of appreciation for provisions on safety, particularly for vague requirements, which provides a high threshold for acceptable interpretations.¹⁶⁵

164 TFEU Arts. 28 and 34-35.

165 See TFEU Art. 36.

5 Possible Regulatory Approaches to Consumer Product Security

Section 3 argues that direct “security-for-safety” risks (type 1) are encompassed under the RED, TSD and GPSD. Several weaknesses are, however, left unregulated under these directives, including risks of “personal security”, fraud, and security risks without physical impacts. This section explores three proposed regulatory approaches to reduce lacunae: (i) amending existing product safety requirements; (ii) adopting delegated acts (DAs) under the RED; and (iii) developing a new framework. These can be implemented separately or jointly (or not at all).

5.1 Regulatory Needs

The suitability of a regulatory approach relies on its ability to address existing needs. Based on the previous discussions, together with stakeholder statements on current shortcomings and future legal desires, the following non-exhaustive needs can be set out:

- Minimum requirements for security assessments and basic safeguards.¹⁶⁶
- Market restrictive enforcement mechanisms.¹⁶⁷
- A more well-aligned approach to safety and security.¹⁶⁸
- Encompassment of all consumer connected products,¹⁶⁹ and all necessary risks.

166 Raised, e.g., by Forbrukerrådet 2019b, p. 3, ANEC and BEUC 2018, p. 6. This can be complemented with stricter requirements for higher-risk products (e.g., children’s devices). Minimum requirements can ensure higher security from the outset – “security-by-design” – rather than dealing with it ex post, which not only endangers consumers, but risks liability, GDPR fines, and loss of reputation for EOs. Standards and softer instruments can specify technical (e.g., encryption and authentication) and organisational measures.

167 See Section 2.

168 See Sections 1.2-1.3.

169 Several challenges discussed herein are similar regardless of, i.a., the user group or whether the products are wired. Divergent rules for wired and non-wired products may then undermine fair competition (as mentioned in CSES and Tech4i2 2020a (*Impact Assessment*), p. 115). Possible inclusion of more services may also require consideration (Orgalim 2020, p. 4).

- Measures taken at the design stage, but also as risks emerge throughout product lifecycles.¹⁷⁰
- Clear and predictable rules, both for EO compliance and authority enforcement.¹⁷¹
- Minimised fragmentation between frameworks and avoiding duplication of costs.¹⁷²
- Expedient organisation of enforcement between relevant authorities.¹⁷³
- Consumer trust and improved security consciousness.¹⁷⁴
- Quick adoption and implementation.¹⁷⁵

Requirements should ensure adequate security and consumer protection, balanced against other interests. Too strict criteria for testing or demonstration of compliance could push small and specialised producers off the market,¹⁷⁶ as they may struggle to adapt. This could stifle innovation and competition. Considering the EU law objective of a well-functioning internal market,¹⁷⁷ EOs ability to comply – hereunder by ensuring coherent frameworks – is central. The mentioned needs provide a starting point for analysing the three regulatory approaches.

5.2 An Extended Safety Scope under EU Product Safety Legislation

The discussions in Sections 3 and 4 demonstrate a need for explicit clarifications on the current scope of product safety legislation, particularly if a wide category of emerging threats are encompassed. Although the Commission previously appeared to lean towards a narrow interpretation of “safety”,¹⁷⁸ their opinion seems to be evolving. In 2020 they intimated that several security risks must be considered already encompassed:

“The safety concept in the *current* Union product safety legislation is in line with an *extended concept of safety* in order to protect consumers and users. Thus, the concept

170 ANEC and BEUC 2019, p. 2, Orgalim 2020, p. 4. “Security-by-design” includes designing for security to be maintained over time (NOU 2018:14 Chapter 18).

171 As opposed to current uncertainties (see Sections 3-4).

172 Raised, e.g., by DigitalEurope 2019, p. 7-8, Orgalim 2020, p. 2.

173 E.g., NOU 2018:14 Chapter 18.

174 E.g., UK Department for Digital, Culture, Media and Sport 2018, p. 25. Increased consumer consciousness could also make high cybersecurity reputations more beneficial and thereby motivate EOs to implement safeguards.

175 ANEC and BEUC (2018, p. 14) describe current risks as “urgent”.

176 CSES and Tech4i2 2020a (*Impact Assessment*), p. 133.

177 TFEU Art. 26.

178 Expert Group on Toy Safety 2018 (*Minutes from meeting 22.6.2017*), p. 6.

of product safety encompasses protection against *all kinds of risks arising from the product*, including not only mechanical, chemical, electrical risks, but *also cyber risks and risks related to the loss of connectivity of devices*".¹⁷⁹

Although presented as the "current" legal scope, the statements are vague (as discussed below) and make weak grounds for intervention in a product's market access. It therefore seems more appropriate to read them as aimed towards regulatory updates. Whether this would entail changing the current legal scope (which would be the case based on the Section 3 conclusion) or just codify it (as appears to be BEUC's view)¹⁸⁰ is not clear.

A revision of the GPSD is ongoing, *inter alia* to facilitate more explicit provisions for "product risks linked to new technologies".¹⁸¹ Clarifications and changes in GPSD *lex generalis* requirements will affect all consumer products. Similar amendments can be made under *lex specialis* directives, for instance the TSD.¹⁸² The preference should then be to keep the extensions identical or similar, to maximise legal coherency and clarity. Concomitantly, placing cybersecurity under multiple PSL instruments can create fragmentation,¹⁸³ hereunder overlaps between MSA authorities which could impede effective enforcement. This increases the need for MSA cooperation mechanisms, as well as expanded competences to assess risks they traditionally have not.

The Commission does not specify their envisaged "extended" safety concept, hereunder what "cyber risks" contain. It could encompass "security-for-safety" in the broadest sense,¹⁸⁴ or it could be narrower (see Section 1.3). In any case, "security-for-safety" likely poses an upper limit under the product safety regulatory system. Where to draw the line between risks that can ultimately affect persons (or property) and those with purely digital effects, will then present a new challenge. For instance, risks of "personal security" can be very indirect and unforeseeable, making the "security-for-safety" concept potentially extensive. Future evolution of the overlaps between safety and security can augment this over time. Addressing cybersecurity through the existing directives could thus mend one legal uncertainty by creating another. There may not even be

179 COM(2020) 64 (*Report*), p. 6, emphasis added. See COM(2020) 65 (*White Paper*), p. 15.

180 ANEC and BEUC 2019, p. 21.

181 Ares(2020)3256809, pp. 2-3.

182 For the TSD, an evaluation was started in 2018 (Ares(2018)3667279). The feedback pointed to the lack of clear provisions to address non-secure toys (see SWD(2020) 287, pp. 76-77), and several stakeholders (e.g., BEUC 2018, VdTÜV 2018) claimed that security requirements – at least to some extent – should be encompassed under the TSD. The Commission seems to prefer a more horizontal approach (SWD(2020) 287, pp. 79-80).

183 SWD(2020) 287, p. 79.

184 COM(2020) 65 (*White Paper*) (p. 14) mentions, i.a., "personal security".

good reasons to legally distinguish between a wide “security-for-safety” concept and other forms of cybersecurity. This points towards regulatory approaches better able to address a wider category of risks.

Furthermore, simultaneously changing several product safety directives has been described as potentially opening a Pandora’s box.¹⁸⁵ Reopening discussions on existing frameworks can make it difficult to ensure changes are limited to what is necessary for dealing with the regulatory gaps one intended to mend. Since these instruments are based on MS compromises, such revisions could upset regulatory balances.¹⁸⁶

Revisions are also likely to take time, leaving non-secure products unsatisfactorily regulated until agreement, adoption, and implementation is achieved. A more rapid regulatory approach, like RED DAs (see Section 5.3), therefore holds an advantage. If DAs are adopted, the need to still extend the security scopes of multiple product safety instruments calls for reassessment.

In summary, although this approach can provide more explicit security-related minimum requirements, the regulatory needs listed in Section 5.1 would not be properly addressed.¹⁸⁷

5.3 Delegated Acts under RED Article 3(3)(e-f)

RED Article 3 allows for the Commission to adopt delegated acts (DAs) to activate additional essential requirements under the RED.¹⁸⁸ As the requirements are already in the directive, the adoption process can be relatively quick. Activated provisions become part of the basis for conformity declarations and CE marking, and harmonised standards can be adopted for presumption of conformity (see Section 2.1).

Initiatives to activate *litra e* on personal data and privacy safeguards, and *litra f* on fraud protection started in January 2019,¹⁸⁹ and they may be adopted shortly.

¹⁸⁵ Tosoni 2020c.

¹⁸⁶ *Ibid.*

¹⁸⁷ This should not be read as argumentation against revising the GPSD, which can, i.a., improve alignment with more recent regulation and facilitate effective enforcement. However, expanding the “safety” scope of the GPSD may not be an optimal approach to address cybersecurity risks.

¹⁸⁸ RED Art. 3(3)(2), see Art. 44. See TFEU Art. 290.

¹⁸⁹ Ares(2019)476926. Initiatives are also ongoing for RED Art. 3(3)(i) and Art. 4 (Ares(2019)476957) on software upgrades. *Litra d* on avoiding network harm or misuse of network resources may also become relevant.

Central for their ability to address current legal needs is what products and risks they will apply to.

The Commission should specify in the DA provisions what “categories or classes of radio equipment” they cover,¹⁹⁰ and a wide product coverage seems likely.¹⁹¹ Still, the widest scope possible is limited to RED products (i.e., all wirelessly connected devices). Wired products and standalone services cannot be contained.¹⁹²

Regarding the risk scope, the *litrae* do not focus directly on cybersecurity, but on personal data and privacy, and fraud.

Litra e could encompass any exploitable security weaknesses involving personal data or privacy infringements,¹⁹³ as well as less security-related aspects like service operators’ data sharing. Concomitantly, not all security risks are contained, since both data privacy and security have aspects not included under the other.¹⁹⁴

A *litra e* DA will likely look to GDPR provisions.¹⁹⁵ The potential overlap is still uncertain, hereunder how harmonised standards may be coordinated with codes of conduct under GDPR Article 40. The DA could complement the GDPR by making GDPR requirements applicable to EOs and enforceable with market restrictive mechanisms. Concomitantly, a DA based on GDPR requirements will create overlaps between RED MSAs and data protection authorities. As double assessments should be avoided for efficient enforcement, cooperation mechanisms and clear definitions of roles will be needed.

Unlike for *litra e*, there is no EU legal definition on which a DA can base its “fraud” scope.¹⁹⁶ It may include any false representation to gain advantages or

190 RED Art. 3(3)(2), see Art. 2(1)(6).

191 See European Commission 2020c (*Updates on Articles 3(3)(e) and (f) of the RED*). The Inception Impact Assessment lays a foundation for a wide scope (Ares(2019)476926).

192 Although the Section 3 conclusion did not consider the LVD (covering wired products), it is not unlikely that a similar interpretation can be made for that directive, i.e., that it covers type 1 risks (the Section 2.1.1 discussion could make this systemically probable). However, RED DAs will never apply to wired products under the LVD, leaving them still subject to considerable legal gaps.

193 Privacy concerns the protection of integrity and private life, which can include both information control and a “right to be let alone” (Bygrave 2014, p. 24).

194 Bygrave 2014, p. 2, Tosoni 2020a, p. 192.

195 Particularly the definitions, principles, and Arts. 25 and 32 (see Section 2.2.1). See CSES and Tech4i2 2020a (*Impact Assessment*), p. 176.

196 CSES and Tech4i2 2020a (*Impact Assessment*), p. 9.

cause loss.¹⁹⁷ Connected devices can be fraudulently misused in a variety of ways, from gaining financial information or instructing devices to perform expensive tasks, to manipulation of information or identity theft. Children can also, for instance, be manipulated to share their parents' credit card information or unlock the front door. A wide legal definition seems envisaged for *litra f*, hereunder considering data "a type of currency",¹⁹⁸ thereby potentially labelling as fraudulent anything that involves misuse of data. Unauthorised access to personal information could then both infringe privacy and entail fraud.

Litrae e-f DAs will likely contain both "personal security" (type 2) and fraud (type 3). Assuming the conclusion in Section 3 that types 0 and 1 are encompassed under current PSL, DAs would ensure that all "security-for-safety" related risks mentioned in Section 1.3 are covered for wireless devices. However, if the Section 3 conclusion is disputed, some type 1 "security-for-safety" risks may remain unaddressed despite adoption of DAs (e.g., the water boiler mentioned in Section 2.2.1).

The discussions in Section 3 and Section 5.2 were limited to "security-for-safety" due to the wording in Article 3(1)(a) (and similar provisions in the other directives). Since RED DAs are subject to a different RED Article 3 paragraph, they can encompass also risks without physical impacts. This avoids the difficulties of deciding the "upper limit" of, for instance, "personal security". Furthermore, any doubts on the inclusion of third-party interference are erased by this being a precondition for fraud.

Nevertheless, not all cybersecurity risks are contained, particularly for "products processing non-personal data".¹⁹⁹ The span and implications of such gaps are hard to predict,²⁰⁰ but if cybersecurity is the aim, it seems unfortunate to address it through other, partly overlapping risk aspects. The DAs cannot cover more than the *litrae's* wording,²⁰¹ making legal lacunae unavoidable.²⁰² A patchy approach to cybersecurity may prove vulnerable over time, as technological developments can create new or enlarged gaps of unaddressed risks.

197 Law 2018, p. 299. See CSES and Tech4i2 2020a (*Impact Assessment*), p. 112.

198 CSES and Tech4i2 2020a (*Impact Assessment*), p. 112.

199 See European Commission 2020c (*Updates on Articles 3(3)(e) and (f) of the RED*).

200 Mind that, e.g., misuse of networks can be addressed under RED Art. 3(3)(d), narrowing the gap further.

201 Tosoni 2020b, p. 1269, see TFEU Art. 209.

202 For this reason, DigitalEurope (2020, p. 2) "are surprised why the solution for cybersecurity issues is sought via the detour of data protection, privacy and protection against fraud".

The final Impact Assessment recommends adoption of DAs for litrae e and f “to close regulatory loopholes, and mak[e] an explicit link between product safety and security”.²⁰³ However, the above discussions show that RED DAs have shortcomings compared to the regulatory needs set out in Section 5.1. They also provide no guarantees for imminent legal certainty: although the DAs themselves can be adopted quickly, no standards are ready to be harmonised for presumption of conformity. Awaiting this, DAs will apply without such specifications, creating a challenging period of uncertainty for manufacturer compliance. The time needed to develop harmonised standards thus diminishes the advantages of quick adoption processes. Seen together with limitations of what products and risks can be addressed, it may be preferable to consider alternative approaches.

5.4 A New Cybersecurity Law

An alternative to the approaches discussed above is to develop new legislation.²⁰⁴ This can take a horizontal approach as *lex generalis*,²⁰⁵ and the risk scope can be based on cybersecurity without having to define difficult (and possibly unfortunate) limitations based on personal data and privacy, fraud, or safety impacts. At the same time, a broader product scope can be addressed (e.g., both wired and wireless devices) to improve legal coherence. Furthermore, responsibility could be distributed between more actors and beyond the time of placement on the market.²⁰⁶ New legislation provides flexibility to tailor the law to the regulatory needs, thereby changing the perspective from fitting security risks into the product safety directives, to making the law fit the relevant challenges.

Depending on how new legislation is designed, this approach holds potential to address most of the needs presented in Section 5.1. The exception is the time required.²⁰⁷ Still, it is promising that the Commission appears to be examining

203 CSES and Tech4i2 2020a (*Impact Assessment*), p. 181.

204 As proposed by stakeholders (e.g., ANEC and BEUC 2019, pp. 12-13) and assessed in the Impact Assessment (“Option 5” in CSES and Tech4i2 2020a (*Impact Assessment*), pp. 115-116).

205 ANEC and BEUC 2019, p. 12.

206 Raised, e.g., by Orgalim 2020, p. 4, also for better distribution of obligations between other EOs than manufacturers. Note, however, that while it is desirable that manufacturers by design facilitate updates after placement on the market, responsibilities to provide security patches may be better placed on those running the services (e.g., data controllers and processors – where personal data is involved – under the GDPR).

207 Predicting the time perspective is difficult where complex challenges and different interests are involved. CSES and Tech4i2 (2020a, p. 108) have indicated that developing new legislation might take 5-10 years. DigitalEurope (2020, p. 3) has intimated this to be an overestimation.

this possibility, intimating presentation of a proposal towards the end of 2021.²⁰⁸ The idea is to encompass a new cybersecurity framework under the NLF system, with market-restrictive enforcement, Safety Gate alerts, CE marks, and so on.²⁰⁹

Development of new cybersecurity legislation entails a high likelihood of extensive overlaps with other PSL (e.g., RED DAs), GDPR, CSA, and a possible NIS2. This highlights a need for harmonising measures, such as common standards. To this end, the longer timeframe for implementation can be an advantage. Certification schemes and codes of practice under the CSA and GDPR may then first be implemented and their efficiency better assessed, before new legislation is finalised. Concomitantly, there would be time to develop standards to be ready for adoption as harmonised standards when the new law enters into force, thereby providing better legal certainty from the outset.

The content of new cybersecurity legislation is still open. The main aim is to establish mandatory “security-by-design” requirements for market access. Although adoption is some way into the future, new legislation holds potential for addressing regulatory needs in a more holistic and well-planned manner.

5.5 Summary and *De Lege Ferenda*

Three possible regulatory approaches to product security have been examined against their abilities to meet regulatory needs.

Extending current directives addresses emergent challenges but is restricted to a “security-for-safety” scope. This may set an unnatural limit between indirect safety impacts and purely digital security risks. Such a differentiation could also prove difficult to define; the current vague and limited scope of the directives may simply be replaced with another (although wider) unclear limitation, still rendering significant regulatory gaps. Amending existing instruments also risks upsetting the careful balances and compromises on which they are based.

The second approach – to adopt RED DAs – holds the advantage of quick implementation. However, DAs can deal with cybersecurity only through security-related aspects (privacy, data protection, fraud). Although they would address several pertinent challenges also beyond “security-for-safety”, gaps may remain and even increase over time as technology evolves. In addition, RED DAs’ inability to encompass wired equipment creates fragmentation. Minimising over-

208 European Commission 2020c (*Updates on Articles 3(3)(e) and (f) of the RED*).

209 DigitalEurope 2020, p. 4, Orgalim 2020, pp. 3-5.

laps with existing and future instruments, hereunder reducing legal uncertainties and duplication of costs, will be central challenges if DAs are adopted. Furthermore, although DAs can be adopted quickly, manufacturers rely on specifications to comply. Until harmonised standards are in place, DAs may therefore struggle to achieve their purposes in practice.²¹⁰

The approach of an entirely new cybersecurity law can potentially address most of the needs set out in Section 5.1. A more complete set of risks and products can be encompassed under one instrument, promoting a more coherent legal landscape. It may even contribute better distribution of responsibilities between relevant actors. The main disadvantage is the longer time perspective. This can, however, also facilitate development of standards in advance and planning for consistency with other instruments to achieve a more coherent product security legal landscape.²¹¹

It is possible to pursue one, more, or none of these regulatory paths. The Commission seems to aim for all of them. This strategy of multiple overlapping solutions maximises the risks of regulatory overlaps and fragmentation.²¹² If a holistic approach is necessary in the long term anyway, adoption of RED DAs can be perceived primarily as a “quick *intermediary* solution to fix *some* of the problems with connected devices”.²¹³ Later adoption of a new cybersecurity framework can render the DAs redundant, or they may then unduly complicate the legal picture. Implementing various approaches can also cause repeated transitional costs for EOs. Perhaps too many instruments are trying to address the same and similar issues, adopting new requirements before sufficient time has passed to assess the actual effects of existing rules (e.g., under the CSA and GDPR).²¹⁴ It is indeed important to react quickly to emerging challenges, but a balance must be struck between this urgency and the need to ensure coherent legislation in the long term. If one aims for a new framework, intermediary solutions should perhaps be sought through less permanent measures, and specifications to a larger extent developed beforehand. This could contribute to a more coherent response to product security risks.

210 Raised, e.g., by DigitalEurope 2020, p. 4.

211 The same standards may be linked to multiple frameworks to decrease fragmentation (CSES and Tech4i2 2020a (*Impact Assessment*), p. 110), but variations in risk scopes and objectives can prevent them from fitting under multiple different instruments to the desired extent.

212 See, e.g., Orgalim 2020, p. 2.

213 ANEC and BEUC 2019, p. 10, emphasis added.

214 Specifications are expected both under GDPR Arts. 40 and 42, and under CSA Art. 46. Although they lack PSL market restrictive mechanisms, both instruments can be important to ensure product security while awaiting new cybersecurity rules.

6 Summary and the Way Forward

This paper has focused on market restrictive requirements for product security risks. The *de lege lata* analyses found that the applicability of the RED, TSD and GPSD on “security-for-safety” risks relies heavily on two legal criteria: harm impacts and causality. Firstly, the directives only cover risks affecting the health or physical safety of persons, in addition to a narrow category of property under the RED. Secondly, the causal requirement appears not to exclude risks relying on third-party interference. It was concluded that the directives likely encompass direct “security-for-safety” (type 1), while security risks beyond this represent legal lacunae.

In considering possible regulatory approaches against legal gaps and needs, significant shortcomings were found both for amending current directives and for adopting delegated acts (DAs) under the RED. The limitations of these frameworks prevent them from addressing product security in a holistic and coherent manner.

New cybersecurity legislation holds potential to address more regulatory needs. Development and implementation would admittedly require time, leaving product security challenges inadequately regulated for longer. Concomitantly, this extended time perspective would facilitate preparation of more adequate standards in advance and planning for consistency with other frameworks. Although the efficiency of voluntary measures (like CSA schemes) has been questioned,²¹⁵ such mechanisms can promote implementation of “security-by-design” until new legislation is ready. In the interest of legal coherence, the recommendation would then be to minimise adoption of other hard law instruments which only partially address present challenges.

Whatever regulatory approaches are taken, the underlying interests and considerations remain the same. This includes striking a balance between facilitating compliance and ensuring adequate security and safety for consumers.

The challenges discussed herein emerged from technological advancements, causing a need to fit legal instruments to matters for which they were not initially meant. New challenges – pertaining to the safety-security overlap, but also yet unforeseen risks – may arise. A well-suited framework must be prepared for

215 E.g., ANEC and BEUC 2019, p. 9.

further developments, both by providing technology-neutral and flexible provisions, but also by not setting unfortunate limits which may later generate new legal gaps. The fact that not everything can be foreseen and encompassed makes it imperative to address at least current obvious needs in the most holistic and coherent way possible, to prepare the law for the future.

Table of references

Conventions and Treaties:

EEA Agreement *Agreement on the European Economic Area*. 2.5.1992.

CCC *Convention on Cybercrime*, ETS No. 185, Budapest 23 November 2001.

TEU *Treaty on European Union* (TEU). Consolidated version (EUT 2016/C 202/01).

TFEU *Treaty on the Functioning of the European Union* (TFEU). 23.3.1957. Consolidated version (EUT 2016/C 202/01).

EU Legislation:

Reg. 2019/2144 Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166.

Reg. 2019/1020 Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) 305/2011.

Reg. 2019/881	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).
Dir. 2016/1148	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 (NIS Directive).
Reg. 2016/679	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).
Dir. 2014/53/EU	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).
Dir. 2014/35/EU	Directive 2014/35/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits (Low Voltage Directive)
Reg. 1025/2012	Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardization, amending Council Directives 89/686/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC,)(34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council Text with EEA relevance.

- Dir. 2009/48/EC Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys (Toy Safety Directive).
- Reg. 765/2008 Regulation (EU) 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93.
- Dec. 768/2008/EC Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/46. OJ L 2018/82.
- Dir. 2002/58/EC Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications, ePrivacy Directive).
- Dir. 2001/95/EC Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (General Product Safety Directive).
- Dir. 1999/5/EC Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity (Radio Equipment and Telecommunications Terminal Equipment Directive). (No longer in force).
- Dir. 85/374/EEC Council Directive of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (Product Liability Directive).

CJEU Case Law and Advocate General Opinions:

Opinion of Advocate General Hogan in Case C-523/18 *Engie Cartagena S.L. v. Ministerio para la Transición Ecológica*. Opinion delivered on 19 September 2019.

Case C-621/18. *Andy Wightman and Others v. Secretary of State for Exiting the European Union*. Judgement of 10 December 2018. ECLI:EU:C:2018:999.

Case C-434/16. *Peter Nowak v. Data Protection Commissioner*. Judgement of 20 December 2017. ECLI:EU:C:2017:994.

Case C-558/15. *Vieira de Azevedo and Others v. CED Portugal Unipessoal, Lda and Instituto de Seguros de Portugal – Fundo de Garantia Automóvel*. Judgement of 15 December 2016. ECLI:EU:C:2016:957.

Case C-136/04. *Deutsches Milch-Kontor GmbH v. Hauptzollamt Hamburg-Jonas*. Judgement of 24 November 2005. ECLI:EU:C:2005:716.

Joined Cases C-310/98 and C-406/98. *Hauptzollamt Neubrandenburg v. Leszek Labis (C-310/98) and Sagpol SC Transport Miedzynarodowy i Spedycja (C-406/98)*. Judgement of 23 March 2000. ECLI:EU:C:2000:154.

Case 6/72. *Europemballage Corporation and Continental Can Company Inc. v. Commission of the European Communities*. Judgement of 21 February 1973. ECLI:EU:C:1973:22.

EU Preparatory Works and Other Official Journal Documents:

SWD(2020) 287 Commission Staff Working Document Evaluation of Directive 2009/48/EC of the European Parliament and of the Council on the Safety of Toys. Brussels 19.11.2020.

COM(2020) 823 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) 65 White Paper on Artificial Intelligence – A European Approach to Excellence and Trust. Brussels, 19.2.2020.

- COM(2020) 64 Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics. Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee. Brussels, 19.2.2020.
- Ares(2020)3256809 Revision of Directive 2001/95/EC of the European Parliament and of the Council on General Product Safety. Combined Evaluation Roadmap/Inception Impact Assessment. 23.6.2020.
- Ares(2019)476926 Commission Delegated Regulation on Internet-Connected Radio Equipment. Inception Impact Assessment on Delegated Acts on RED Article 3(3) Litra e and f. 28.1.2019.
- Ares(2019)476957 Commission Delegated Regulation on Reconfigurable Radio Systems. Inception Impact Assessment on Delegated Acts on RED Article 3(3) Litra i and Article 4. 28.1.2019.
- Ares(2018)3667279 Toy Safety Directive – Evaluation. Evaluation Roadmap. 10.7.2018.
- COM(2017) 787 Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee. The Goods Package: Reinforcing Trust in the Single Market. Brussels, 19.12.2017.
- COM(2017) 795 Proposal for a Regulation of the European Parliament and of the Council Laying Down Rules and Procedures for Compliance with and Enforcement of Union Harmonisation Legislation on Products and Amending Regulations (EU) No 305/2011, (EU) No 528/2012, (EU) 2016/424, (EU) 2016/425, (EU) 2016/426 and (EU) 2017/1369 of the European Parliament and of the Council, and Directives 2004/42/EC, 2009/48/EC, 2010/35/EU, 2013/29/EU, 2013/53/EU, 2014/28/EU, 2014/29/EU, 2014/30/EU, 2014/31/EU, 2014/32/EU, 2014/33/EU, 2014/34/EU, 2014/35/EU, 2014/53/EU, 2014/68/EU and 2014/90/EU of the European Parliament and of the Council. Brussels, 19.12.2017.

- COM(2017) 10 Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). Brussels, 10.1.2017.
- OJ C 272/1 2016 European Commission. *The 'Blue Guide' on the Implementation of EU Products Rules* 2016. Official Journal of the European Union, C 272/01, Volume 59, 26.7.2016.

Other European Commission and Expert Group Documents:

- European Commission. *Updates on Articles 3(3)(e) and (f) of the RED*. EG RE (06)08. Presentation at the meeting of the Commission Expert Group on Radio Equipment 6.7.2020. (2020c). <https://circabc.europa.eu/ui/group/43315f45-aaa7-44dc-9405-a86f639003fe/library/489ca583-f94d-4c40-8cc1-539b3c7d71ff/details> [retrieved 30.8.2020]
- European Commission. *Summary of References of European Standards Published in the Official Journal – 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*. Brussels, 22.4.2020. (2020b). <https://ec.europa.eu/docsroom/documents/40881/attachments/1/translations/en/renditions/native> [retrieved 30.8.2020]
- European Commission. *First Meeting of the “Sub-Group on Artificial Intelligence (AI), Connected Products and Other New Challenges in Product Safety” to the Consumer Safety Network. Background Document*. Working Document, 29.1.2020. (2020a). <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=40730> [retrieved 30.8.2020]
- European Commission. *Guide to the Radio Equipment Directive 2014/53/EU*, 19.12.2019. (2019c). <https://ec.europa.eu/docsroom/documents/33162/attachments/1/translations/en/renditions/native> [retrieved 30.8.2020]
- European Commission. *Summary of References of European Standards Published in the Official Journal – Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys*. Brussels,

17.10.2019. (2019b). <https://ec.europa.eu/docsroom/documents/37686/attachments/1/translations/en/renditions/native> [retrieved 30.8.2020]

European Commission. *Delegated Acts under the Radio Equipment Directive. Comparison/Differences between RED and Some Other Related EU Acts.* EG RE (03)12. Brussels, 1.8.2019. (2019a). <https://circabc.europa.eu/ui/group/43315f45-aaa7-44dc-9405-a86f639003fe/library/0044c582-e555-44bc-a143-7e483034dc40/details> [retrieved 30.8.2020]

European Commission. *Toy Safety Directive 2009/48/EC. An Explanatory Guidance Document.* Rev. 1.9, 10.2.2016. <https://ec.europa.eu/docsroom/documents/16183/attachments/1/translations/en/renditions/native> [retrieved 30.8.2020]

Expert Group on Toy Safety, European Commission. *Approved Minutes of the Expert Group Meeting 22 June 2017.* EXP/2017/021/rev1, 3.1.2018. <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.group-DetailDoc&id=36484&no=1> [retrieved 30.8.2020]

Standards:

ETSI EN 303 645. *Cyber Security for Consumer Internet of Things.* V2.1.1 (2020-06). https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf [retrieved 30.8.2020]

National Legislation and Preparatory Works:

Icelandic Legislation:

2018 *Act on Changes to the Electronic Communications Act.* Lög 41/2018 um breytingu á lögum um fjarskipti, nr. 81/2003, með síðari breytingum (EES-reglur, nethlutleysi, CE-merkingar á fjarskiptabunaði).

2003 *The Electronic Communications Act.* Lög 81/2003 um fjarskipti (fjarskiptalög).

1995 *Act on Product Safety and Official Market Control.* Lög 134/1995 um öryggi vöru og opinbera markaðsgæslu.

Norwegian Legislation and Regulations:

2016 *Regulation on EEA Requirements for Radio Equipment*. Forskrift 15. april 2016 nr. 377 om EØS-krav til radioutstyr (radioutstyrsforskriften).

2013 *Regulation on Toy Safety*. Forskrift 18. november 2013 nr. 1403 om sikkerhet ved leketøy (leketøyforskriften).

1988 *The Sale of Goods Act*. Lov 13. mai 1988 nr. 27 om kjøp (kjøpsloven).

1976 *The Product Control Act*. Lov 11. juni 1976 nr. 79 om kontroll med produkter og forbrukertjenester (produktkontrollloven).

Norwegian Preparatory Works:

NOU 2018:14. *IKT-sikkerhet i alle ledd – Organisering og regulering av nasjonal IKT-sikkerhet*.

National Administrative Cases and Safety Gate Alerts:

Safety Gate Alerts:

Alert A12/0157/19 (Enox Safe-Kid-One).

https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/?event=viewProduct&reference=A12/0157/19&lng=en
[retrieved 30.8.2020]

Alert A12/1671/15 (Jeep).

https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/?event=viewProduct&reference=A12/1671/15&lng=en
[retrieved 30.8.2020]

Alert A12/00154/20 (Passenger car).

https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/?event=viewProduct&reference=A12/00154/20&lng=en
[retrieved 30.8.2020]

Norwegian Administrative Decisions:

DSB case 2016/11181 *Cayla and i-Que*. 2016/11181-19: *Orientering om avslutning av sak – markedstilsyn – leketøy*. Letter to Top-Toy AS 4.5.17. (On file with author).

Nkom case 2017/4446 Wonlex GW100. 2017/4446-22: *Markedskontrollresultater*. 8.5.2018. (On file with author).

Icelandic Administrative Decisions:

Áfrýjunarnefnda. *Úrskurður Áfrýjunarnefndar Neytendamála. Mál Nr. 1/2019*. Appeal decision on Enox Safe-Kid-One. 2019. <https://www.neytendastofa.is/library/Files/oryggissvid/akvardanir/%C3%9Arstur%C3%B0ur2019-01.pdf> [retrieved 30.8.2020]

Neytendastofa. *Sölubann á Wonlex krakka snjallúrum*. Ákvörðun nr. 46/2018. Decision on Wonlex GW100. 2018. [https://www.neytendastofa.is/library/Files/oryggissvid/akvardanir/%c3%81kv46_2018%20-%20Copy%20\(1\).pdf](https://www.neytendastofa.is/library/Files/oryggissvid/akvardanir/%c3%81kv46_2018%20-%20Copy%20(1).pdf) [retrieved 30.8.2020]

Neytendastofa. *Afturköllun og sölubann á Enox Safe-Kid-One krakka snjallúrum*. Ákvörðun nr. 42/2018. Decision on Enox Safe-Kid-One. 2018. <https://www.neytendastofa.is/library/Files/oryggissvid/akvardanir/H%c3%b3pkaup%20%c3%a1kv%c3%b6r%c3%b0un%2042-2018%20Sk%c3%b6nnu%c3%b0inn%20%c3%a1kv%c3%b6r%c3%b0un.pdf> [retrieved 30.8.2020]

Books and Journal Articles

Andersen, Stine. *Non-Binding Enforcement of EU Law: Interpretation or Centralization and Norm Assimilation?* Paper to be presented at EUSA Twelfth Biennial International Conference, Boston, Massachusetts, March 3-5, 2011. <http://aei.pitt.edu/52089/1/ANDERSEN.pdf> [retrieved 30.8.2020]

Burton, Cédric. *Article 32. Security of Processing*. In: Kuner, Christopher et al. (eds.). *The EU General Data Protection Regulation. A Commentary*. Oxford University Press, 2020, pp. 630-639.

Bygrave, Lee A. *Article 25. Data Protection by Design and by Default*. In: Kuner, Christopher et al. (eds.). *The EU General Data Protection Regulation. A Commentary*. Oxford University Press, 2020, pp. 571-581.

Bygrave, Lee A. *Data Privacy Law. An International Perspective*. Oxford University Press, 2014.

- Bygrave, Lee A. and Tosoni, Luca. *Article 4(1)*. In: Kuner, Christopher et al. (eds.). *The EU General Data Protection Regulation. A Commentary*. Oxford University Press 2020, pp. 103-115.
- Calo, Ryan. *Robotics and the Lessons of Cyberlaw*. In: *California Law Review*, Volume 103, 2015, pp. 513-563.
- Chu, Gordon et al. *Security and Privacy Analyses of Internet of Things Children's Toys*. In: *IEEE Internet of Things Journal*, Volume 6, Issue 1, 2018, pp. 978-985.
- Eckhoff, T. *Rettskildelære*. 5th Edition by Jan E. Helgesen, Oslo: Universitetsforlaget, 2001.
- Eliantonio, Mariolina and Stefan, Oana. *Soft Law Before the European Courts. Discovering a 'Common Pattern'?* In: *Yearbook of European Law*, Volume 37, 2018, pp. 457-469.
- Fink, Glenn et al. *Overview of Security and Privacy in Cyber-Physical Systems*. In: Song, Houbing et al. (eds.). *Security and Privacy in Cyber-Physical Systems. Foundations, Principles, and Applications*. IEEE Press, John Wiley & Sons Ltd., 2018, pp. 1-23.
- Karanikas, Nektarios. *Revisiting the Relationship Between Safety and Security*. In: *International Journal of Safety and Security Engineering*, Volume 8, Number 4, 2018, pp. 547-551.
- Lenaerts, Koen and Gutiérrez-Fons, José A. *To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice*. EUI Working Paper AEL 2013/9, European University Institute, Academy of European Law. https://cadmus.eui.eu/bitstream/handle/1814/28339/AEL_2013_09_DL.pdf [retrieved 30.8.2020]
- Ponsard, Christophe, et al. *Assessment of Emerging Standards for Safety and Security Co-Design on a Railway Case Study*. In: Abdelwahed E., et al. (eds.). *New Trends in Model and Data Engineering*, MEDI 2018, Communications in Computer and Information Science, Volume 929, Springer, 2018.

- Shasha, Sharon, et al. *Playing with Danger: A Taxonomy and Evaluation of Threats to Smart Toys*. In: *IEEE Internet of Things Journal*, Volume 6, Issue 2, April 2019, pp. 2986-3002.
- Svantesson, Dan. *A Legal Method for Solving Issues of Internet Regulation*. In: *International Journal of Law and Information Technology*, Volume 19, Number 3, 2011, pp. 243-263.
- Tamò-Larrieux, Aurelia. *Designing for Privacy and Its Legal Framework*. *Data Protection by Design and Default for the Internet of Things*. Law, Governance and Technology Series, Issues in Privacy and Data Protection, Volume 40, Springer, 2018.
- Tosoni, Luca. *Article 4(12). Personal Data Breach*. In: Kuner, Christopher et al. (eds.). *The EU General Data Protection Regulation. A Commentary*. Oxford University Press, 2020, pp. 188-195. (2020a).
- Tosoni, Luca. *Article 92. Exercise of the Delegation*. In: Kuner, Christopher et al. (eds.). *The EU General Data Protection Regulation. A Commentary*. Oxford University Press, 2020, pp. 1268-1277. (2020b).
- Valente, Junia and Cardenas, Alvaro A. *Security & Privacy in Smart Toys*. Proceedings of 1st ACM Workshop on Internet of Things Security & Privacy (IoT S&P'17) in conjunction with CCS'17, Dallas, USA, 2017. <https://dl.acm.org/doi/pdf/10.1145/3139937.3139947> [retrieved 30.8.2020].
- de Vries, Anne. *Maximum Harmonisation and General Clauses – Two Conflicting Concepts?* 2010. <https://dx.doi.org/10.2139/ssrn.1703078> [retrieved 30.8.2020]

Reports, Positions, and Industry Guidelines

- ANEC and BEUC. *Keeping Consumers Secure. How To Tackle Cybersecurity Threats Through EU Law*. 2019. https://www.beuc.eu/publications/beuc-x-2019-066_keeping_consumers_secure_-_how_to_tackle_cybersecurity_threats_through_eu_law.pdf [retrieved 30.8.2020]
- ANEC and BEUC. *Cybersecurity for Connected Products. Position Paper*. 2018. <http://www.anec.eu/images/Publications/position-papers/Digital/ANEC-DIGITAL-2018-G-001final.pdf> [retrieved 30.8.2020]

BEUC (The European Consumer Organisation). *Feedback from: BEUC – The European Consumer Organisation*. Feedback on Internet-connected radio equipment and wearable radio equipment, delegated acts for RED Article 3(3)(e-f), 4.3.2019. <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/2018-Internet-connected-radio-equipment-and-wearable-radio-equipment/F239298> [retrieved 30.8.2020]

BEUC (The European Consumer Organisation). *Feedback from: BEUC – The European Consumer Organisation*. Feedback to the Evaluation of the Toy Safety Directive, 8.8.2018. <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/1852-Evaluation-of-the-Toy-Safety-Directive/F13693> [retrieved 30.8.2020]

Bouvet. *Report. Investigation of Privacy and Security Issues with Smart Toys*. 2016. <https://fil.forbrukerradet.no/wp-content/uploads/2016/12/2016-11-technical-analysis-of-the-dolls-bouvet.pdf> [retrieved 30.8.2020]

CSES (Centre for Strategy & Evaluation Services) and Tech4i2. *Final Report. Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment*. Report for the European Commission, April 2020. (2020a). <https://ec.europa.eu/docsroom/documents/40763/attachments/2/translations/en/renditions/native> [retrieved 30.8.2020]

CSES (Centre for Strategy & Evaluation Services) and Tech4i2. *Product-Based Case Studies. Annex 8. Annex to: Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment*, for the European Commission, 7.4.2020. (2020b). <https://ec.europa.eu/docsroom/documents/40763/attachments/6/translations/en/renditions/native> [retrieved 30.8.2020]

Department for Digital, Culture, Media & Sport (UK). *Secure by Design: Improving the Cyber Security on Consumer Internet of Things Report*. March 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/775559/Secure_by_Design_Report_.pdf [retrieved 30.8.2020]

DigitalEurope. *Defining the Way Forward for IoT Security and Certification Schemes*. Position Paper, 24.10.2019. <https://www.digitaleurope.org/wp/wp-content/uploads/2019/10/Position-on-IoT-security-and-certification-schemes-FINAL-FOR-APPROVAL.pdf> [retrieved 30.8.2020]

- DigitalEurope. *Comments on the “Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment”*. 2.7.2020. <https://circabc.europa.eu/ui/group/43315f45-aaa7-44dc-9405-a86f639003fe/library/3be3b119-9731-49e3-bab6-24a858477307/details> [retrieved 30.8.2020]
- Eurostat. *NACE Rev. 2. Statistical classification of economic activities in the European Community*. 2008. <https://ec.europa.eu/eurostat/documents/3859598/5902521/KS-RA-07-015-EN.PDF> [retrieved 9.2.2021]
- Forbrukerrådet. *Innspill til Ny Regulering om Datasikkerhet og Personvern for Radioutstyr og Krav om Felles Ladere*. Addressed to Nasjonal kommunikasjonsmyndighet, 17.6.2019. (2019a). <https://fil.forbrukerradet.no/wp-content/uploads/2019/06/innspill-til-ny-regulering-om-datasikkerhet-og-personvern-for-radioutstyr-og-krav-om-felles-ladere-l2640282.pdf> [retrieved 30.8.2020]
- Forbrukerrådet. *NOU 2018:14 – IKT-Sikkerhetsutvalget – Høringsuttalelse*. Response to NOU 2018:14, 18.3.2019. (2019b). <https://fil.forbrukerradet.no/wp-content/uploads/2019/04/nou-201814-ikt-sikkerhetsutvalget-horingsuttalelse.pdf> [retrieved 30.8.2020]
- Forbrukerrådet. *#WatchOut. Analysis of Smartwatches for Children*. 2017. (2017b). <https://fil.forbrukerradet.no/wp-content/uploads/2018/03/watchout-rapport-october-2017.pdf> [retrieved 30.8.2020]
- Forbrukerrådet. *#Toyfail. An Analysis of Consumer and Privacy Issues in Three Internet-Connected Toys*. 2016. <https://fil.forbrukerradet.no/wp-content/uploads/2016/12/toyfail-report-desember2016.pdf> [retrieved 30.8.2020]
- Mnemonic. *GPS Watches for Children*. Security Assessment Report, the Norwegian Consumer Council, 18.10.2017.
- Orgalim. *Proposal for a Horizontal Legislation on Cybersecurity for Networkable Products within the New Legislative Framework*. Position Paper, 9.11.2020, https://orgalim.eu/sites/default/files/attachment/Final%20position%20on%20CS_2020-11-09.pdf [retrieved 13.2.2021]
- Strict. *Report on IoT Device Security*. 16.9.2019, <https://www.privacy-web.nl/cms/files/2019-09/report-on-iot-device-security.pdf> [retrieved 30.8.2020]

VdTÜV (Verband der TÜV e.V.). *Feedback from: Verband der TÜV (VdTÜV). Feedback to the Evaluation of the Toy Safety Directive*, 1.8.2018. <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/1852-Evaluation-of-the-Toy-Safety-Directive/F13556> [retrieved 30.8.2020]

News Articles, Blog Posts, and Press Releases

Forbrukerrådet. *Cayla Forbudt i Tyskland, på Salg i Norge*. 17.2.2017. (2017a). <https://www.forbrukerradet.no/siste-nytt/cayla-forbudt-i-tyskland-pa-salg-i-norge/> [retrieved 30.8.2020]

Fowler, Bree. *Parents Should Be Cautious with Connected Toys, CR Testing Shows*. Consumer Reports, 19.12.2018. <https://www.consumerreports.org/privacy/test-of-connected-toys-shows-parents-should-be-cautious/> [retrieved 30.8.2020]

Greenberg, Andy. *Hackers Remotely Kill a Jeep on the Highway – With Me in It*. Wired Magazine, 21.7.2015. <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/> [retrieved 30.8.2020]

Smithers, Rebecca. *Strangers Can Talk to Your Child Through ‘Connected’ Toys, Investigaton Finds*. The Guardian, 14.11.2017. <https://www.theguardian.com/technology/2017/nov/14/retailers-urged-to-withdraw-toys-that-allow-hackers-to-talk-to-children> [retrieved 30.8.2020]

Stykas, Vangelis. *GPS Watch Issues... AGAIN*. Pentest Partners, 29.1.2019. <https://www.pentestpartners.com/security-blog/gps-watch-issues-again/> [retrieved 30.8.2020]

TIE (Toy Industries of Europe). *Smartwatch Recall is ‘Test Case’ for New Delegated Act*. TIE Weekly Bulletin. 8.2.2019. <https://www.toyindustries.eu/resource/weekly-bulletin-08-02-19/> [retrieved 30.8.2020]

Tosoni, Luca. *Intelligenza Artificiale, Rischi Privacy con le Proposte della Commissione UE*. Agenda Digitale, 11.3.2020. (2020c). <https://www.agendadigitale.eu/sicurezza/privacy/intelligenza-artificiale-rischi-privacy-con-le-proposte-della-commissione-ue/> [retrieved 30.8.2020]

Westlund, Jacqueline M. Kory. *Robots for Kids: Designing Social Machines That Support Children's Learning*. IEEE Spectrum, 20.7.2017. <https://spectrum.ieee.org/automaton/robotics/robotics-hardware/designing-robots-for-kids> [retrieved 30.8.2020]

Dictionaries and Definitions:

Law, Jonathan (ed.). *A Dictionary of Law*, Ninth Edition, Oxford University Press, 2018.

Oxford University Press. *Shorter Oxford English Dictionary, Volume II*, 6th Edition, Oxford University Press, 2007.

Correspondence with Market Surveillance Authorities:

DSB E-mails from Astrid Lie Olsen, Senior Adviser in the Directorate for Civil Protection (Seksjon for produktsikkerhet, DSB), dated 7.4.2020 (*attachment*), 20.5.2020, 25.5.2020, 26.5.2020 and 24.8.2020. All on file with author. Stated opinions used herein are confirmed in e-mail 24.8.2020.

Neytendastofa E-mail from Svava G. Ingimundardóttir, Lawyer in the Icelandic Consumer Agency, dated 27.2.2020, and from Reynir Ingi Reinhardsson, Legal Officer, dated 27.5.2020. Both on file with author.

PFS E-mail from Hjalti Pálmason, Lawyer/Specialist, in the Technical Division of the Icelandic Post and Telecom Administration (PFS), dated 10.6.2020. On file with author.