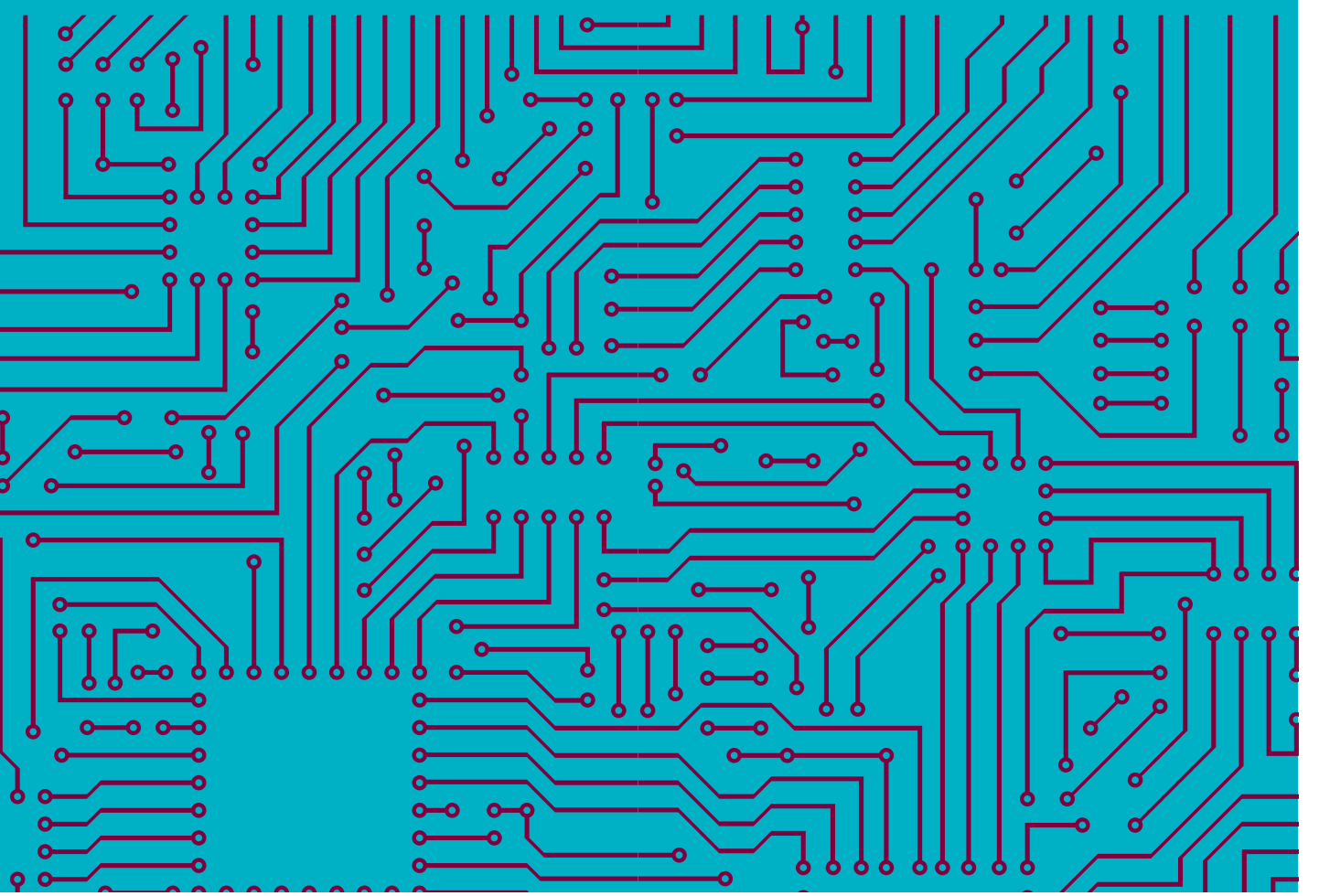
10 TOWARDS HARMONISED DUTIES OF CARE AND DILIGENCE IN CYBERSECURITY

Radboud University

By Dr. Paul Verbruggen*
Dr. Pieter Wolters*
Prof. dr. Mireille Hildebrandt**
Prof. dr. Carla Sieburgh*
Prof. dr. Corjo Jansen*

* Business and Law Research Centre (OO&R)
Radboud University, Nijmegen, the Netherlands
http://www.ru.nl/law/research/business-law/
** Institute for Computing and Information Sciences (iCIS)
Radboud University, Nijmegen, the Netherlands
http://www.ru.nl/icis



CONTENTS

PREFACE 80

EXECUTIVE SUMMARY 80

1. INTRODUCTION 82

2. PROBLEM ANALYSIS 83
- 2.1 Legal uncertainty as regards duties of care 83
- 2.2 Internet of Things 84
- 2.3 Exclusion of liabilities 85
- 2.4 Public enforcement action 87
- 2.5 Incentives to ensure cybersecurity 88

3. NEED FOR HARMONISATION 88

4. TOPICS FOR HARMONISATION 89
- 4.1 Pre-contractual information duties 89
- 4.2 Conformity 91
- 4.2.1 Conformity in present and future EU consumer law 92
- 4.2.2 Burden of proof 95
- 4.2.3 Relationship with data protection law 96
- 4.3 Unfair terms 97
- 4.4 Liability in the ICT supply chain 99
- 4.4.1 Product liability 99
- 4.4.2 Development risk defence 101
- 4.4.3 Product surveillance and recall 102
- 4.5 Enforcement 103

5. APPROACHES TO HARMONISATION 104

6. CONCLUSION 105

ANNEX: GLOSSARY OF TERMS 106

PREFACE

This White Paper was commissioned by the Dutch Cyber Security Council as part of the National Coordinator for Security and Counterterrorism, residing under the Ministry of Security and Justice. It provides a framework for discussion around the need to harmonise legal standards for duties of care and diligence in cybersecurity related to ICT goods and services, and offers proposals to better protect the interests of consumers of such goods and services.

The White Paper was drafted by dr. Paul Verbruggen, dr. Pieter Wolters, prof. dr. Mireille Hildebrandt, prof. dr. Carla Sieburgh, and prof. dr. Corjo Jansen.

We would like to acknowledge the comments and suggestions of the members of the supervising committee in preparing the White Paper: Liesbeth Holterman (Nederland ICT), Danny ter Laak (Parket-Generaal, Openbaar Ministerie), prof. dr. Lokke Moerel (Tilburg University, Morrison & Foerster LLP, member Cyber Security Council), Reinout Rinzema (Ventoux Law), Peter van Schelven (self-employed legal council), Ronald Verbeek (CIO Platform) and Maurice Wesseling (Consumentenbond).

The views expressed in this White Paper are those of the drafters only.

Nijmegen, May 2016.

EXECUTIVE SUMMARY

Information and communication technology (ICT) is ever more central to Europe's economic growth. However, as society becomes more and more dependent on ICT goods and services, the risks and costs of its disruption, failure or misuse increase. Consequently, **ensuring the confidentiality, integrity and availability of ICT (i.e. cybersecurity) constitutes a crucial pillar on which the use of ICT must be based in Europe and beyond**.

Yet, the question of who is responsible for ensuring cybersecurity is not easy to answer, in part due to the diversity among legal frameworks of EU Member States related to cybersecurity. **The Digital Single Market strategy launched by the European Commission in May 2015 offers a clear momentum to address, in a uniform and harmonised way, this legal fragmentation and resulting uncertainty.** This White Paper therefore offers a framework for discussion around the need to adopt harmonised duties of care and diligence for **cybersecurity in relation to ICT goods and services offered to consumers**. The paper does not address any sector-specific regulation adopted at EU or national level relating to cybersecurity, such as critical infrastructures, energy, health and finance. It further assumes the entry into force of the General Data Protection Regulation and the Network and Information Security Directive and does not offer suggestions on the topics covered by these legislative instruments.

The White Paper starts from the assumption that **any individual who has suffered a loss because of a lack of cybersecurity should have effective legal remedies against the actor responsible for providing such security.** In seeking to remedy these losses a consumer now encounters serious legal obstacles. It might first of all be difficult for a consumer to establish that the ICT provider owed a duty of care to him/her, what that duty implies given the circumstances, and whether the duty was in fact breached. While the fields of law applying to this context (sales, contract, unfair commercial practices, and tort law) offer various frameworks and concepts to provide answers to these pressing questions, they have so far only rarely been applied by courts in relation to cybersecurity issues. Consequently, there is **little legal certainty** as regards the question what actors in the ICT supply chain are required to do in terms of cybersecurity and, in turn, to what extent consumers can hold them to account for the lack of it. The question of who is responsible for the security of ICT goods and services is increasingly difficult to answer in the important development of the **Internet of Things** (IoT) as this development depends on the interconnection of multiple business actors in the provision of goods and services to consumers. Moreover, ICT providers typically use

extensive **exemption clauses** to limit or exclude their liability in contracts concluded with consumers. Enforcement by public enforcement authorities is typically not concerned with providing remedies to consumers who suffered damages because of a security breach.

Consequently, there are few regulatory incentives for business actors in the ICT supply chain to ensure the security of the ICT goods and services they provide to consumers. We contend that **a uniform legal benchmark requiring the use of appropriate technical and organisational measures (i.e. security by design)** by ICT providers when placing on the market goods or services will provide important new incentives for the ICT sector to ensure cybersecurity across the entire ICT supply chain and increase legal certainty for both business and consumers around duties of care and diligence in cybersecurity.

Below we identify a set of circumstances that must be considered significant when determining the relevant duty of care, after which we offer a number of recommendations. We use the term 'ICT goods and services' to collectively denote ICT systems, infrastructures, networks, hardware, firmware, software, applications and digital content. If more specific terminology applies, this will be specified. We kindly refer to the Glossary of terms annexed to this White Paper for the exact definitions used.

We recommend that **in assessing whether a duty of care and diligence has been breached in a specific case, the following circumstances should at least be taken into account**:

- The purposes for which similar ICT goods or services are normally used;
- The purpose for which the consumer requires the ICT goods and services, as communicated to the ICT provider;
- The legitimate expectations of the public at large;
- The presentation of or public statements about the goods and services by the ICT provider;
- Any foreseeable or irresponsible (mis)use by the consumer;
- The nature and severity of the risks poses by the ICT goods or services to consumers;
- The nature and severity of the damages involved;
- The state of scientific and technical knowledge at the time the ICT provider placed the ICT goods and services on the market;
- (Non-)compliance with accepted private industry standards.

This White Paper also offers the following **recommendations** concerning a specific set of topics **to harness the legal position of consumers** in the case of a lack of cybersecurity.

- ICT providers should be required to offer, in a clear and comprehensible way, information to consumers about their contractual obligations to ensure cybersecurity before they enter into a contract with consumers, including information about when, how, to what extent and for how long an ICT service provider or a producer or seller of goods with embedded ICT components, will provide updates or upgrades to consumers.
- Cybersecurity should be recognized as a main characteristic of ICT goods and services. As such, it should be part of a conformity assessment related to these goods and services.
- Sellers of consumer goods should not be able to contract out the confidentiality, integrity and availability of embedded ICT or digital content for the normal life-span of these goods. Also suppliers of digital content should not be able to contract out such matters in relation to this content for the duration of the related services contract.
- Consumers should have the right to be compensated for the damages they suffered due to any non-conformity with regard to the security of ICT goods and services. The recoverable damages should not be limited to material damages and should also include immaterial damages, in line with Article 77 of the General Data Protection Regulation.
- General terms and conditions related to consumer contracts of ICT goods and services must meet the requirements of fairness and transparency as laid down by the Unfair Contract Terms Directive. National courts, public enforcement authorities and consumer representative bodies should intervene proactively within the scope of their respective competences to better address the use of unfair terms by businesses in the ICT sector in consumer contracts.

- The material scope of the Product Liability Directive should be revised so as to include software. The 'development risk defence' as allowed under this Directive should not be interpreted extensively such as to exclude the liability of producers for the release, updating and upgrading of software that disregards known and knowable security vulnerabilities.
- Consumers should be able to recover from businesses liable under the Product Liability Directive damages to hardware devices or damage related to the loss of digital content. We propose to consider whether and to what extent consumers of software, whether or not embedded in a product, should have the right to claim material and immaterial damages from the producer based on the strict liability system as set out in this Directive.
- Businesses placing on the market ICT goods and services should be required to control, monitor and inspect these goods and services in terms of security vulnerabilities throughout the normal life-span of these products or for the duration of the related services contract.
- We recommend investigating whether and how existing EU legislative instruments intended to improve consumer access to justice (e.g. the Injunctions Directive, the ADR Directive and the ODR Regulation) may be applied effectively to provide consumer protection in relation to disputes with traders concerning cybersecurity.

1. INTRODUCTION

Information and communication technology (ICT) is ever more central to Europe's economic growth. It offers new opportunities to respond to business demands, consumer needs and pressing societal challenges. However, as society becomes more and more dependent on ICT goods and services (e.g. systems, infrastructures, networks, hardware, firmware, software and applications), the risks and costs of its disruption, failure or misuse increase. Consequently, ensuring the confidentiality, integrity and availability of ICT – discussed here as *cybersecurity* – constitutes a crucial pillar on which the use of ICT must be based in Europe and beyond.

The **aim** of this White Paper is to provide a *framework for discussion around the need to harmonise legal standards for duties of care and diligence concerning cybersecurity and offer proposals to better protect the interests of non-commercial end-users of ICT (i.e. consumers and data subjects) in terms of the confidentiality, integrity and availability of ICT goods and services, and data (including personal data) handled through them.* In practice, the costs of cyber *in*security are typically born by consumers and data subjects, rather than the business actors offering the ICT goods and services (i.e. *ICT providers*), including hardware producers, software and application developers, Internet service providers, telecom operators, digital content suppliers and retailers. Regardless of any responsibilities on the part of individual users, these users face numerous **hurdles to ensure effective remedies** against disruption, failure or misuse of ICT, including the compensation of damages sustained as a result thereof. This is in part due to legal uncertainty, as well as limited and diverse legal frameworks of the Member States.[1]

There is a clear **momentum** to address, in a uniform and harmonised way, this legal uncertainty and fragmentation. In May 2015, the European Commission launched an ambitious strategy for a *Digital Single Market*, which also fundamentally concerns cybersecurity.[2] Important new legislation is on its way in the areas of data protection and network and information security,[3] and new proposals have recently been submitted as part of this strategy to strengthen the protection of consumers of digital content (including

1 E. Tjong Tjin Tai e.a., 'Duties of Care and Diligence against Cybercrime', report for the Dutch National Coordinator for Security and Counterterrorism (March 2015), https://www.gccs2015.com/sites/default/files/documents/Bijlage%202%20-%20Duties%20of%20care%20and%20diligence%20against%20cybercrime%20(1).pdf (accessed 1 May 2016).

2 European Commission, 'A Digital Single Market Strategy for Europe' COM(2015) 192 final, p. 13.

3 European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final, Brussels, 25.1.2012 (latest version as adopted by the European Parliament 15 December 2015) and the Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union COM (2013) 48 final, Brussels, 7.2.2013.

software) and in online sales contracts.[4] It is therefore timely to also **critically discuss the general legal framework in the European Union (EU) applying to the sale of goods and services by ICT providers to consumers**. This White Paper offers suggestions on how this framework can be amended to further harness the legal position of consumers in remedying a lack of cybersecurity, including the right to compensation of damages for the disruption, failure or misuse of ICT goods and services, including the personal data handled through them. The White Paper will not address any sector-specific regulation adopted at EU or national level relating to cybersecurity, such as critical infrastructures, energy, health and finance. The paper further assumes the entry into force of the General Data Protection Regulation and Network and Information Security Directive.[5] It therefore does not offer new suggestions on the topics covered by these legislative instruments.

2. PROBLEM ANALYSIS

The increasing dependence on ICT goods and services in today's society highlights the need to ensure their security. A lack of confidentiality, integrity and availability of ICT is likely to translate into direct or indirect, material or immaterial damages for businesses, consumers and data subjects concerned. **Any individual** who has suffered a loss because of the failure to deliver cybersecurity should have effective remedies against the responsible actor.

2.1 Legal uncertainty as regards duties of care

However, when seeking to remedy cyber insecurity, individual users frequently find themselves confronted with serious legal obstacles that prevent them from actually bringing a claim against the ICT provider in court. It might first of all be **difficult to establish whether a duty of care owed to the user, what the duty may imply given the context, and whether that duty was in fact breached**. An illustration is provided by a recent case in the Netherlands, which has received much attention from abroad.

Stagefright: Consumentenbond v. Samsung Electronics Benelux B.V.[6]

In July 2015 it was announced that Google's Android system was vulnerable to the so-called 'stagefright' bug, as a result of which smart phones operating on this system could be remotely accessed, allowing the attacker to read and delete data, and to spy on the user through operating the smart phone camera and microphone. In October 2015 a new version of the bug, stagefright 2.0, was publically announced.[7] Samsung's smart phones operate on the Android system and as a result some of the older models of its phones proved vulnerable. However, Samsung did not warn users of its smart phones about the bug, nor did it patch the security threat by providing updates or upgrades for its older models.

Therefore the Consumer Association in the Netherlands – *Consumentenbond* – decided to bring legal proceedings against Samsung requesting the court to provide interim injunctive relief. More specifically, Consumentenbond petitioned the court, amongst others, to require Samsung to (i) provide to the users of its vulnerable mobile phones information about the bug, (ii) provide security updates for Android bugs considered critical by Google for all smart phone models having this bug, and (iii) provide security updates for all smart phone models introduced in the Netherlands within the last two years and in the future. It based these claims on requirements under national laws of unfair commercial practices, sales, tort and data protection, which are all (some more than others) harmonised by EU law. According to Consumentenbond Samsung holds a

4 European Commission, Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contract for the supply of digital content, COM(2015) 634 final, Brussels, 9.12.2015, and the Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sale of goods, COM(2015) 635 final, Brussels, 9.12.2015.

5 See at note 3.

6 District Court of Amsterdam (President), Case C/13/600958 / KG ZA 16/51.

7 https://www.theguardian.com/technology/2015/jul/28/stagefright-android-vulnerability-heartbleed-mobile (accessed 1 May 2016).

market share of some 40% in the Dutch smart phone market, while over 80% of its smart phones are vulnerable to the stagefright bug.

The judge hearing the application for interim relief did not grant injunctive relief. The main reason for this decision was the finding that Consumentenbond had not provided sufficient evidence showing the urgency required for interim relief. Expert witnesses of Samsung testified that the stagefright bug does not constitute a security breach, but merely a weakness in Google's Android software. Misuse of that vulnerability would prove to be very complex, expensive and time consuming. As a result, a successful use of this weakness would be extremely limited. Documentary evidence provided by Consumentenbond did not disconfirm this, and neither could Consumentenbond furnish proof that a Samsung smart phone was hacked outside the testing environment. Furthermore, the interim relief requested was not considered appropriate as this would have considerable technical implications and costs for Samsung, whereas for the updating of their smart phones they would be dependent on Google's collaboration for they operate the Android system. With regard to the request to grant an order to provide information to smart phone users about the stagefright bug, the judge held that Samsung had already provided additional information on its website and that the question whether this information would be sufficient could not be answered based on the evidence provided by Consumentenbond.

Consumentenbond failed in its claims because it could not satisfy the specific requirements under national procedural law for summary proceedings. As a result, the judge did not consider the case in substance. Nevertheless, the case raises a number of very fundamental questions concerning the debate on duties of care and diligence in cybersecurity, including:

- Can a producer of smart devices be required to offer updates or upgrades for the software embedded in the device if that software proves to be vulnerable in terms of cybersecurity?
- Does such a duty exist independently of the fact that the vulnerable software is provided by a third party?
- In what time frame would such a duty to offer updates or upgrades exist? Would the producer be required to continue to provide updates or upgrades only shortly after the product is sold, for the normal life span of a product, or during its entire life cycle?
- Should the producer inform a consumer about what he/she can expect in terms of cybersecurity before a contract is concluded?
- Is the potential risk of disruption, failure or misuse of ICT sufficient to constitute a breach of contract even if the risk has not materialized in reality?

So far, questions such as these have hardly been addressed by courts in the Member States. While **the law as it stands offers various frameworks and concepts to provide answers to these questions, in particular in the fields of sales, contract, unfair commercial practices, and tort law**, few cases have come to the courts in which these frameworks and concepts could be applied and interpreted extensively to allow for remedies against insecure ICT goods or services. Consequently, there is little legal certainty as regards the question what actors in the ICT supply chain are required to do in terms of cybersecurity. This begs the political question of whether legislative intervention is needed at the European level in order to a lay down a clear and uniform legal framework regarding these duties of care and diligence.

2.2 Internet of Things

The discussion around the existence and scope of duties of care and diligence in cybersecurity is likely to gain further prominence in the light of the development of the Internet of Things (IoT). In this development, which has been recognized by the European Commission as a major catalyst for economic growth, innovation and digitalization in Europe,[8] **the question of who is responsible for the security of ICT goods and services is increasingly difficult to answer in the IoT** as it presupposes the interconnection of multiple business

8 COM(2015) 192 final, p. 14. See more generally, European Commission, Communication on 'Internet of Things – An action plan for Europe', COM(2009) 278 final, Brussels, 18.6.2009.

actors in the provision of goods and services to users. The functionality of the products or devices connected through the IoT is no longer determined by the hardware itself, but increasingly dependent on multiple service providers.[9] As the **complexity of the ICT supply chain** increases, also responsibilities for cybersecurity become more and more blurred and intransparent. Who can be held responsible for what exactly?

To answer this question one should look at the contracts that provide the legal infrastructure for the dense network of actors in the IoT. These contracts, which may be explicitly or implicitly linked, each involve their own set of rules and procedures determining the respective rights and obligations of the contracting parties. It is very difficult for consumers to understand the contracts they conclude, the documentation related to them (e.g. terms of service, privacy policies, etc), and the contracts between the business actors to which the consumer contracts are linked.[10] Moreover, the consumer contracts are typically **contracts of adhesion** ('take it or leave it'), locking users into long-term relationships with ICT providers through simple click wrap agreements. Users are bound by the services, their terms of service (and to some extent the privacy policies) by simply clicking an 'OK' or 'agree' button.

Cybersecurity is of eminent importance to the IoT since this novel ICT development does not only enable the collection of much more personal data, but also more intimate data in both intrusive and dynamic ways.[11] These data are no longer simply a by-product generated by the use of the device, but feed into the device and related services provided by and through it in order to, so it is claimed, enhance their functionality. We may expect that the business models in businesses in the IoT will be personal data-driven, as with current search engines, social media, advertising networks and data brokers. In the event of unwarranted disclosure of personal data (data breaches) we can thus expect a privacy and data protection impact. However, even without such breaches harm may be caused where the data are combined across different context and allowing for prohibited or undesirable discriminatory practices (e.g. regarding insurance pricing, credit rating or employability).[12] Furthermore, some of the devices in the IoT are designed with safety purposes in mind, such as door locks, smoke alarms and self-driving vehicles. Vulnerabilities in the cybersecurity of the ICT systems underpinning these devices may not just lead to the loss and misuse of personal data, but also to physical harm.[13] Thus, **cyber insecurity may translate into physical insecurity**. This, again, underlines the acute need to ensure cybersecurity in our society, now and in the future.

2.3 Exclusion of liabilities

Another important legal obstacle for consumers to obtain effective remedies against the failure to provide cybersecurity concerns the use of general terms and conditions through

9 This is already the case now for an ordinary smart phones, where security problems can relate to the hardware providers, the provider of the operating system, the firmware, various types of integrated software, telecom providers, and the providers of a plethora of apps (which may be part of the smartphone by default or downloaded by the end-user), while these phones can be bought from various types of (online) retailers or be part of a service contract with a telecom provider.

10 In assessing the contractual regime underpinning the use of the Nest thermostat, one of the popular home devices with Internet connectivity, Noto La Diega and Walden content that Nest users need to at least read thirteen different documents to have a full overview of their rights and obligations vis-à-vis sellers, services providers, licensors and other third parties concerned with the operation of the thermostat and related services. See: G. Noto La Diega and I. Walden, 'Contracting for the 'Internet of Things': Looking into the Nest', Queen Mary University of London, School of Law, Legal Studies Research Paper No. 219/2016, p. 3-4, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2725913 (accessed 1 May 2016).

11 Consider the smart watch that collects data about the physical condition of its wearer (pulse, body temperature, physical exercise through GPS, etc.) throughout the day, on the workplace and even in bed.

12 For example, the US-based insurance company Oscar uses personal data generated by insurance takers to set insurance premiums. See https://www.hioscar.com/about/ (accessed 1 May 2016).

13 There are various reports of smart devices of which the security was compromised and could result in extensive physical harm for users and third parties. For example, iOS software in cars was reported to be hacked, making it possible for a hacker to have control over certain aspects of a car, including the possibility to start it remotely. See: http://blog.caranddriver.com/researcherbmw-mercedes-vulnerable-to-remote-unlocking-hack/ (accessed 1 May 2016). Another example is provided by the smoke alarms of Nest, the company that also produces smart thermostats, included the feature 'Wave', whereby one could switch the alarm off by waving the hands. This feature has been disabled since April 2013, since 'movements near Nest Protect that are not intended as a wave can be misinterpreted by the Nest Wave algorithm. If this occurs during a fire, this could delay the alarm going of'. See https://nest.com/support/article/Nest-Protect-Safety (accessed 1 May 2016).

which business actors impose far-reaching duties on consumers and make extensive restrictions as regards their liability. The **use of exemption clauses in contractual arrangements is widespread**.[14] Through these clauses businesses seek to exempt or severely limit their liability in relation to cybersecurity issues. One extreme example of this strategy is provided by the toy manufacturer Vtech in the aftermath of a hack which left millions of user accounts of children exposed.

VTech

In November 2015, the online Learning Lodge Portal of the Hong Kong based toy manufacturer VTech was hacked, leaving some 4.8 million unique email addresses and personal data relating to hundreds of thousands of children (names, genders, birthdates, postal addresses, user names, passwords, etc) exposed.15 According to one influential observer, VTech 'allowed itself to be hacked' because it 'continued to run a service with such egregious security flaws (...)'.[16]

In response to this major security breach, VTech amended its Terms & Conditions of the Learning Lodge Portal. It now includes an extensive exemption clause that reads:

'YOU ACKNOWLEDGE AND AGREE THAT YOU ASSUME FULL RESPONSIBILITY FOR YOUR USE OF THE SITE AND ANY SOFTWARE OR FIRMWARE DOWNLOADED THEREFROM. YOU ACKNOWLEDGE AND AGREE THAT ANY INFORMATION YOU SEND OR RECEIVE DURING YOUR USE OF THE SITE MAY NOT BE SECURE AND MAY BE INTERCEPTED OR LATER ACQUIRED BY UNAUTHORIZED PARTIES (emphasis added).'[17]

This clause implies a full disclaimer as to the duty to provide cybersecurity on the part of VTech. It is highly doubtful whether this clause will hold in court proceedings.[18] While this is an extreme example, many actors in the ICT sector use such extensive exemption clauses for direct or indirect, material or immaterial damages caused by their devices and services. Rather common is the use of a clause phrased along the lines of 'any exclusions, disclaimers or limitation of liability provisions will apply to the extent permitted by local laws'. In the United Kingdom, however, the Competition and Markets Authority, which is the national public enforcement authority in the field of consumer protection, has stated that such wide exclusion clauses are both unfair and lack transparency.[19] This would entail that such clauses are inapplicable, meaning that companies relying on these clauses can be held liable for damages caused. The problem is that **consumers are frequently not aware of their rights** and we do not expect the liable parties to remind them of their rights.

14 The European Commission recognizes the widespread use of exemption clauses in cloud services: '(...) contracts often exclude, or severely limit, the contractual liability of the cloud provider if the data is no longer available or is unusable, or they make it difficult to terminate the contract. This means that that data is effectively not portable.' Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'A Digital Single Market Strategy for Europe' COM(2015) 192 final, Brussels, 6 May 2015, p. 14.

15 http://motherboard.vice.com/read/one-of-the-largest-hacks-yet-exposes-data-on-hundreds-of-thousands-of-kids (accessed 1 May 2016).

16 http://www.troyhunt.com/2016/02/no-vtech-cannot-simply-absolve-itself.html (accessed 1 May 2016).

17 VTech Electronics Europe plc, 'Terms and Conditions' Learning Lodge Support (update 24 December 2015), http://contentcdn.vtechda.com/data/console/GB/1668/SystemUpgrade/FirmwareUpdateTnC_GBeng_V2_20160120-170000.txt (accessed 1 May 2016).

18 In December 2015 a class-action lawsuit was filed against VTech Electronics North America and VTech Holdings Limited before the U.S. District Court for the Northern District of Illinois. See: https://www.bigclassaction.com/lawsuit/vtech-data-breach-class-action-lawsuit.php (accessed 1 May 2016).

19 Competition and Markets Authority, 'Unfair contract terms guidance. Guidance on the unfair terms provisions in the Consumer Rights Act 2015',31 July 2015 (CMA37), at para. 2.54-2.55, available at: https://www.gov.uk/government/ uploads/system/uploads/attachment_data/file/450440/Unfair_Terms_Main_Guidance.pdf (accessed 1 May 2016).

More generally, there is a **tendency in the private sector to deny any responsibility** whenever a weakness in the security of their network, infrastructure or services is exposed. Companies tend to freeze and entrench themselves in legal discourses on liability, rather than assuming responsibility (*not* liability) to improve and remedy the signalled shortcomings. A typical response by industry is provided by the example of the Volkswagen Group, whose encrypted electronic car keys proved rather easy to crack.

Volkswagen Group

In 2013, a research team of Radboud University (Nijmegen, the Netherlands) and the University of Birmingham (UK) publicly announced that they had dismantled the so-called 'Megamos Crypto transponder'.[20] This type of transponder is a passive RFID tag which is embedded in the key of the cars and is widely used in the automotive industry as an electronic vehicle immobilizer. The 'obvious' security gaps uncovered by the researchers could lead the dark minded to wirelessly lock pick cars.

In response the Volkswagen Group, who had used the specific transponder in millions of its cars, brought interim proceedings against the research team before the High Court of Justice in London, requesting a prohibitive injunction preventing the authors, their institutions, and anyone who assisted them, from publishing key sections of the paper. The High Court allowed the injunction for it found that the researchers had misused confidential information in software similar to that used by Volkswagen for its car keys (i.e. the Megamos Crypto algorithm), while Volkswagen cars depend on the secrecy of that information. As a result, the study could not be published containing the disputed algorithm.

Accordingly, rather than acknowledging the weaknesses exposed by researchers and improving electronic car key safety, the hardware producer's knee-jerk response was to file interim proceedings against them. Car owners with these specific keys are left to wonder about the security of their car locks, while the producer does not initiate any action (e.g. a product recall) to resolve the security issue. The spokesperson of the Dutch automotive industry suggested car owners to get a steering-column lock.[21] Similar responses to deny all responsibility to provide better solutions to security threats have been observed in relation to home wireless routers, which prove to be vulnerable for hackers by simply trying the default login password of the routers.[22] Importantly, the example of Volkswagen also shows that **manufacturers of products with significant embedded ICT components deny responsibility for failures of this software as if it is not an inherent part of the product they produced**. Instead, they point to the developer of the ICT involved. With modern products becoming more and more software-driven, it should be questioned whether this position is tenable under the law and whether producers can be held liable for damages caused by insecure ICT integrated in their products.

2.4 Public enforcement action

Enforcement by public authorities is typically not concerned with providing remedies to consumers who have suffered damages because of a security breach. These authorities have powers to impose penalties, but not to compensate damages suffered. These need to be compensated through civil court proceedings. More generally, **few public authorities in the field of competition, trade and consumer law have developed a mature policy strategy concerning cybersecurity.** Enforcement action is either pursued through individual court proceedings or, more likely, collective actions. Public enforcement action is principally concerned with the managing, monitoring and controlling of security breaches concerning personal data, typically in response to notifications by targeted data controllers and processors. Data protection authorities and supervisory bodies in the field of telecom are the

20 R. Verdult, F.D. Garcia & B. Ege, 'Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer', in: USENIX, *Supplement to the Proceedings of the 22nd USENIX Security Symposium*, Washington, DC: USENIX 2013, https://www.usenix.org/sites/default/files/sec15_supplement.pdf (accessed 1 May 2016).

21 Harald Bresser, spokesperson RAI Automobielindustrie, http://nos.nl/nieuwsuur/artikel/2051484-miljoenen-auto-s-te-hacken-door-gebrekkige-beveiliging-chip-autosleutel.html (accessed 1 May 2016).

22 A. Greenberg, '"Millions" of Home Routers Vulnerable to Web Hack', 3 July 2010, http://www.forbes.com/sites/firewall/2010/07/13/millions-of-home-routers-vulnerable-to-web-hack/#43ca6249a68c (accessed 1 May 2016).

central public actors here.[23] Budgetary restraints require these authorities to take focused action only, at times leading to sub-optimal outcomes in terms of protection. 'Rogue traders' and 'cowboys' may take advantage of the absence of any market access controls, and may offer digital services (applications) with very few security measures in place, or worse, with no security at all. As long as public authorities cannot keep these players from offering their services on the digital market place (e.g. through the introduction of approval or licensing systems), individual rights to ensure compensation for damages caused by insecure ICT must be available to complement public enforcement action.

2.5 Incentives to ensure cybersecurity

Combined with factors such as the **high costs of litigation** and the applicability of **foreign systems of law** under the rules of private international law, these circumstances are likely to lead end-users of ICT goods and services, in particular consumers, to abstain from pursuing their claims. Consequently, there are very few legal incentives for the private sector to ensure the security of the ICT goods and services they provide to users, both businesses and consumers. Economic incentives tend to be lacking as well, due to the **absence of information about and transparency of** cybersecurity issues at the consumer's end, limiting their ability to choose between different service providers based on how they provide the appropriate cybersecurity. The **costs of switching** to another service provider may also be high given the long-term service agreements into which consumers are enrolled through click-wrap contracts, thus limiting the ability of consumers to respond to cyber insecurity by choosing another provider.[24] As there are **few regulatory and market incentives** for actors in the ICT supply chain to ensure cybersecurity, legislative intervention by the EU is desirable.

3. NEED FOR HARMONISATION

Cybersecurity constitutes a crucial pillar on which the responsible use of ICT must be based. Users of ICT systems depend on the security of these systems to engage in economic transactions (online sale of goods and services), politics (voting machines, e-voting) and social life (social media). **A lack of cybersecurity will translate into distrust** of important aspects of daily life.

The European Commission recognizes the salience of cybersecurity for economic growth in Europe in its Digital Single Market strategy adopted in 2015. In its strategy it places great emphasis on the security in digital services and in the handling of personal data for public trust in online activities and the digital economy in general. More specifically, it holds:

> "Specific gaps still exist in the fast moving area of technologies and solutions for online network security. A more joined-up approach is therefore needed to step up the supply of more secure solutions by EU industry and to stimulate their take-up by enterprises, public authorities, and citizens."[25]

Harmonising legal duties of care and diligence in cybersecurity will help to further strengthen public trust in ICT goods and services. Harmonisation will also address important aspects of the problems highlighted above. It will first of all increase **legal certainty** for both consumers and businesses. All actors will be able to rely on a uniform legal framework based on clearly defined legal concepts regulating central aspects of cybersecurity across the EU. The laws stipulating duties of care and diligence in cybersecurity are currently only in part harmonised. While the General Data Protection Regulation will provide a new uniform standard for data protection in Europe,[26] including rules for the recovery of damages by individuals suffering damages because of a violation of the Regulation, the general legal

23 Tjong Tjin Tai e.a. 2015 (note 1), p. 141-142, 144.

24 See in the domain of cloud computing the discussion paper by Expert Group on Cloud Computing Contracts, 'Switching – Data portability upon switching' (January 2014) http://ec.europa.eu/justice/contract/files/expert_groups/discussion_paper_topic_4_switching_en.pdf (accessed 1 May 2016).

25 European Commission, 'A Digital Single Market Strategy for Europe' COM(2015) 192 final, p. 13.

26 See note 3.

framework concerned with the compensation of damages caused by a lack of cybersecurity beyond data protection differs strongly among Member States. A **uniform legal benchmark requiring the use of appropriate technical and organisational measures (i.e. security by design) proportionate to the cybersecurity risks posed by goods or services sold by ICT providers to consumers** will further the free movement of these goods and services in the EU internal market, reduce unfair competition between businesses based in different jurisdictions, and may help to protect users against the loss of personal data, digital content, and even physical health.

We anticipate that removing the current barriers stemming from the fragmentation of the legal framework discussed above, will strengthen the legal position of consumers to recover damages, thus stimulating the private sector to ensure higher levels of confidentiality, integrity and availability of ICT. A demand for a high level of cybersecurity will also foster technological development and innovation in that field, offering industry the chance to roll out effective security solutions worldwide. Increased cybersecurity will bolster Europe's economic growth, whilst also providing secure ways to collect and process personal data to help address pressing societal challenges, including aging, environmental degradation and organised crime.

4. TOPICS FOR HARMONISATION

This White Paper presents a specified set of topics suitable for harmonisation with a view to harness the legal position of consumers in recovering damages sustained due to a lack of cybersecurity. The topics have been selected upon thorough analysis of the existing legal framework, its application in practice, and through repeated engagement with the ICT sector, concerned NGOs and government authorities.

The measures proposed here extend beyond national approaches to market economies and related public and private ordering. In general, complex policy objectives require the capacities of both public and private actors to address challenges in delivering these objectives. Also for the policy area of cybersecurity, it has been stressed on several occasions that such security can only be attained by a combination of public and private law measures.[27]

4.1 Pre-contractual information duties

Consumers need reliable and comprehensible information to make a well-informed decision when entering into a contract for the provision of ICT goods and services. Such **transparency enables efficient economic transactions.** There are several instruments of secondary EU legislation in which businesses are required to disclosure the main characteristics of ICT goods or services before a contract is enter into by the consumer,[28] yet cybersecurity has not been identified as such a main characteristic.

It is suggested that where ICT goods and services are concerned these legislative measures should be read as including the obligation for businesses to inform consumers in a clear, meaningful and comprehensive way about their obligations under the contract to ensure the confidentiality, integrity and availability of the ICT involved. **Information about when,**

27 OECD, '*Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies* (OECD, Paris 2012), available at: http://oe.cd/cybersecurity-strategies (accessed 1 May 2016), p. 13, 15, 31 and 32, the EU Cybersecurity strategy JOIN(2013) 1 final, Directive 2013/40/EU (Recital 23), and the White House Summit on Cybersecurity and Consumer Protection, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/summit (accessed 1 May 2016).

28 Generally these pre-contractual information duties concern the main characteristics of the service, identity of the trader, price, arrangements for payment, delivery, and performance, right to withdrawal, duration of the contract, and out-of-court complaint and redress mechanisms. See for example Articles 5 and 6 Directive 2000/31/EC **of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market** (E-commerce Directive), OJ L 178, 17.07.2000, p. 1-16, Article 22 Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, OJ L 376, 27.12.2006, p. 36-68 and Article 5 and 6 Directive 2011/83/EC of the European Parliament and of the Council on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, OJ *L* 304, 22.11.2011, p. 64-88 (Consumer Rights Directive).

how, to what extent and for how long a business will provide the consumer with updates or upgrades of the ICT goods or services must be offered. Cybersecurity should be regarded as a key characteristic of these goods and services and, accordingly, accurate information about it should be provided to consumers. If the updates or upgrades are only available upon additional payment or via **additional service contracts** (including maintenance or end-user license agreements - EULAs), this should also be disclosed. Accordingly, consumers are enabled to make a more informed and efficient transactional decision.

Furthermore, the Unfair Commercial Practices Directive lays down rules for businesses when engaging in commercial practices vis-à-vis consumers.[29] It prohibits commercial communications, including advertising and marketing, by a business (the 'trader') related to the promotion, sale or supply of a product to consumers that are unfair. The Directive holds that a commercial practice is unfair if it is contrary to requirements of professional diligence and it materially distorts or is likely to materially distort the ability of the average consumer to make an informed decision, thereby causing the consumer to take a transactional decision that he would not have taken otherwise.[30]

We need to investigate **to what extent the omission of information about the obligations of the business under the contract as regards the provision of updates or upgrades can be considered an unfair commercial practice**, in particular in case of an invitation from the business to purchase ICT goods or services. Such information should be regarded as material for consumers to make an efficient transnational decision, for example, in relation to software that has proven vulnerable to specific cybersecurity risks but is still offered to consumers. According to Article 7(1) of the Directive a commercial practice shall be regarded as misleading and unfair if it does not provide the substantive information that an average consumer requires to take an informed transactional decision, thus potentially causing the consumer to conclude a contract it would not have concluded otherwise. Following Article 7(2), the same is true where the trader provides the required information in an unclear, unintelligible, ambiguous or untimely manner. Where the trader invites the consumer to purchase its ICT goods or services the duty to provide such information is even more stringent, arguably including the duty to disclose information regarding cybersecurity.

Having regard to the complexity of the ICT supply chain, in particular in the IoT, we also suggest studying in further detail in what way and to what extent accurate **information about who is responsible for ensuring cybersecurity for each of the relevant parts of this supply chain** can be provided to the consumer in a clear, meaningful and comprehensible way. From a consumer law perspective knowing who is responsible for the security of ICT goods or services is necessary for consumers to know who to hold liability in case of a security breach. From the perspective of data protection law, controllers have a duty to inform individuals about who is the processor or sub-processor of the personal data processed by such goods and services.[31]

29 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), OJ L 149, 11.6.2005, p. 22-39.

30 Article 5(1) read in conjunction with 5(2) and 2(2) Directive 2005/29/EC.

31 Articles 28-30 General Data Protection Regulation. See more generally: Article 29 Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"', 264/10/EN, WP 169, Opinion of 16 February 2010.

RECOMMENDATION 1 – ICT providers should be required to offer consumers, in a clear and comprehensible way, information about their contractual obligations to ensure cybersecurity before they enter into a contract with consumers, including information about when, how, to what extent and for how long a business will provide updates or upgrades of ICT goods and services to consumers.

4.2 Conformity

Conformity in sales law traditionally concerns the question of whether supplied goods (i.e. tangible products) comply with the quantity, quality and description required by the contract.[32] Conformity is typically presumed if the goods are fit for the purposes for which goods of the same description would ordinarily be used, possess the qualities of goods which the seller has held out to the buyer as a sample or model, or are fit for any particular purpose for which the buyer requires the goods and which he had made known to the seller at the time of the conclusion of the contract.[33] General contract law and services law similarly require ICT service providers to provide services in accordance with the conditions stipulated by contract and in a way that can reasonably be expected of them.[34]

Cybersecurity (including security of personal data) is only rarely stipulated as one of the qualities of supplied ICT goods and services. Contracts related to the sale of 'smart' goods (i.e. goods embedded with ICT, software and/or network connectivity) or the provision of ICT services do not generally include obligations about the security of the networks and infrastructures used or the personal data collected through them. As the example of VTech discussed above showed, contracts are used to play down user expectations as to the security of the product and to limited or exclude any liability for damages caused by security breaches. Here, mandatory rules from the fields of telecommunications law and data protection law do not seem to be integrated (sufficiently) in the contracts underpinning the supply ICT goods and services. Given the forthcoming General Data Protection Regulation we may expect data protection by design to become a legal duty whenever goods or services are sold that involve the processing of personal data. **Integration of for example obligations of security by design into contracts could provide important additional incentives for compliance**, in particular in business-to-business relationships. Public enforcement authorities may also help to ensure such integration in contracts.

In the Digital Single Market as envisaged by the European Commission, a central role has been given to trust and security in ICT goods and services and in the handling of personal data. In line with this, **cybersecurity should be recognized as a principle quality attribute of ICT goods and services.** Such recognition should not be limited to business-to-consumer relationships, but also extend to business-to-business relationships in order to ensure that duties of care in cybersecurity translate into legal duties throughout the entire ICT supply chain.

32 In the Netherlands the rules governing the sale of tangible goods has recently also been applied (by analogy) to standard software provided upon payment through a tangible medium or downloaded from the internet and of which the use is not limited in time. Cf. Supreme Court, 27 April 2012, *NJ* 2012/293 (*Beeldbrigade*). This implies that Dutch sales law, including the rules on conformity, burden of proof and prescription, also apply to such standard software. This position is exceptional in the EU, however. Member States typically define the provision of standard software as a service or licence contract. The leading case under English law is *St Albans City and District Council v. International Computers Ltd* [1997] FSR 251, which still requires software to be transferred through a tangible medium in order to fall within the scope of sales law.

33 See for example Article 35 United Nations Convention on Contracts for the International Sale of Goods and Article 2 Directive 1999/44/EC of the European Parliament and of the Council on certain aspects of the sale of consumer goods and associated guarantees, OJ L 171, 7.7.1999, p. 12-16.

34 Importantly, articles 12-15 of the E-commerce Directive (Directive 2000/31/EC) exempt ISPs from liability with regard to data stored or transmitted by them on the condition that they did not have knowledge of or control over such data. They are not liable to the extent that their conduct is 'of a mere technical, automatic and passive nature' (cf. CJEU Joined Cases C-236/08 to C-238/08, *Google v Louis Vuitton* [2010] ECR I-02417, para. 120). This exemption is remains in place after the entry in force of the General Data Protection Regulation (see Article 2(4)). However, if ISPs are controllers or processors of personal data, the rules of this Regulation do apply, including the right to compensation of data subjects.

4.2.1 Conformity in present and future EU consumer law

The understanding of cybersecurity as a fundamental quality of ICT goods only in part resonates in the current EU legal framework on sales law. The principle legislative instrument applying here, the Consumer Sales Directive, does not mention the issue of cybersecurity in the sale of consumer goods.[35]

In December 2015 two legislative proposals were presented by the European Commission as part of its Digital Single Market Strategy to further harmonise the field of sales law: (i) a proposal for a Directive on certain aspects concerning contract for the supply of digital content (**Digital Content Directive**),[36] and (ii) a proposal for a Directive on certain aspects concerning contracts for the online and other distance sale of goods (**Online Sales Directive**).[37] Both proposals introduce fully harmonised rules that aim to ensure a high and uniform level of consumer protection across the EU. Importantly, the Digital Content Directive currently explicitly excludes the IoT from its scope of application.[38] It is suggested that **these proposals do not sufficiently take into consideration the importance of cybersecurity**, now and in the future, in the provision of ICT goods and services, and more generally, the Digital Single Market.

There are several reasons to argue for this. When exploring the contents of the Digital Content Directive, it should first be welcomed that the proposed regime on conformity of digital content involves the matter of security of related ICT services. Article 6, paragraph 2 of the proposal reads:

> (...) the digital content shall be fit for the purposes for which digital content of the same description would normally be used including its functionality, interoperability and other performance features such as accessibility, continuity and security, taking into account:
>
> (a) whether the digital content is supplied in exchange for a price or other counter-performance than money;
>
> (b) where relevant, any existing international technical standards or, in the absence of such technical standards, applicable industry codes of conduct and good practices; and
>
> (c) any public statement made by or on behalf of the supplier or other persons in earlier links of the chain of transactions unless the supplier shows that
>
> (i) he was not, and could not reasonably have been, aware of the statement in question;
>
> (ii) by the time of conclusion of the contract the statement had been corrected;
>
> (iii) the decision to acquire the digital content could not have been influenced by the statement.

35 Article 2 Directive 1999/44/EC.

36 European Commission, Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contract for the supply of digital content, COM(2015) 634 final, Brussels, 9.12.2015. Article 2 defines digital content as 'data which are produced and supplied in digital form, including computer software, applications, games, music, videos or texts, irrespective of whether they are accessed through downloading or streaming, from a tangible medium or by other means. It also includes services allowing for the creation, processing and storage of data in digital form (e.g. cloud computing) and for the sharing of such data with other users of the service.

37 European Commission, Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sale of goods, COM(2015) 635 final, Brussels, 9.12.2015.

38 Recital 17 Digital Content Directive.

However, this objective approach to conformity is disowned by the Directive as it allows the digital content provider under Article 6, paragraph 1 to define in the contract – and more likely in the general terms and conditions under it – what the consumer may expect in terms of the quantity, quality, duration and version of the content, as well as its functionality, interoperability, accessibility, continuity and security. Also the extent to which the consumer may expect updating of the digital content – presumably including patches and upgrades in the light of discovered software bugs and security breaches – can be defined in the contract. Accordingly, **digital content providers can subjectively determine by contractual arrangements what conformity means** and thus what expectations consumers may have in terms of the security of the digital content provided to them. As Beale notes, this phrasing is 'quite unnecessary' and 'potentially dangerous to consumers'.[39]

The Online Sales Directive, in contrast, does not allow for such a subjective approach to conformity. Much like the Consumer Sales Directive, it defines conformity of goods in Article 5 in objective terms, namely as being fit for all the purposes for which goods of the same description would ordinarily be used, including all accessories and instructions the consumer may expect to receive, and possessing the qualities and performance capabilities which are normal in goods of the same type and which the consumer may expect given the nature of the goods and taking into account any public statement made by or on behalf of the seller.

The **lack of consideration of cybersecurity as a matter of conformity of sales is problematic**, not only for sales falling within the scope of the Online Sales Directive, but also for the face-to-face sales contracts concluded between traders and consumers in physical establishments (e.g. in shops) as covered now by the Consumer Sales Directive. This is so because now already and even more so in the near future a substantial part of sales will concern goods with significant ICT components. In the case of smart goods and connected devices in the IoT the functionality of these tangible goods is substantially (if not predominantly) defined by related and linked service contracts. More specifically, the use of smart or connected devices typically involves the following contracts:

- A sales contract through which ownership of a tangible good (incl. hardware) is acquired;
- An end user license agreement (EULA) to use the software embedded in the device;
- Service contracts for software maintenance;
- Service contracts for the provision of digital infrastructure, content or services;
- Service contracts (user agreements) for the processing or exploitation of user data.[40]

This underlines that smart goods and connected devices being sold in stores, online or through other distance means will generally bring with them the provision of ICT services as an inherent part of their functionality. Due to this **hybrid character of smart products**, security of integrated and related digital content (e.g. data, software, applications) should be part of any applicable conformity assessment. From the perspective of the promotion of a Digital Single Market in which European businesses and consumers can trust on the accessibility, continuity and security of ICT services, the absence of these matters in rules determining the conformity assessment is an undesirable flaw. The proposals for the Digital Content Directive and Online Sales Directive offer an excellent opportunity to also review the Consumer Sales Directive and explicitly include cyber security in the requirements of conformity.

Furthermore, as the two proposals now stand, there is a very **static separation between the material scope of both Directives**. The purchase of smart goods and connected devices online or by other distance means falls within the ambit of the Online Sales Directive only,

39 H. Beale, 'Scope of application and general approach of the new rules for contracts in the digital environment', briefing paper for the European Parliament, PE 536.493 (February 2016), p. 21, http://www.europarl.europa.eu/committees/nl/ events-workshops.html?id=20160217CHE00181 (accessed 1 May 2016).

40 This list is likely to be extended in the context of devices used in the Internet of Things. In assessing the contractual regime underpinning the use of the Nest thermostat, Noto La Diega and Walden (note 10) content that Nest users need to at least read thirteen different documents to have a full overview of their rights and obligations vis-à-vis sellers, services providers, licensors and other third parties concerned with the operation of the thermostat and related services.

as if they were 'traditional' tangible goods. Where digital content is *embedded* in these products, it would seem to follow from Recital 13 of the proposed Directive that it applies 'where the digital content is embedded in such a way that its functions are subordinate to the main functionalities of the goods and it operates as an integral part of the goods.' Recital 11 of the Digital Content Directive reads the exact opposite and excludes digital content embedded in goods from its material scope. If consumers download new digital content onto these goods, however, the Digital Content Directive does seem to apply.

This static separation is not **tenable in practice**, in particular in the light of the hybrid character of smart goods and connected devices in the IoT. For example, if the digital content (e.g. software or applications) embedded in a smart phone sold online proves vulnerable for security breaches, but the content in this phone was in part updated under a service contract the owner signed with a third party, which Directive would apply? As Wendehorst has aptly noted, it is '**hardly possible to draw a clear line** between the supply of goods *with embedded* digital content and the supply of goods *and* of digital content'.[41]

Furthermore, it is debatable what is meant by 'the main functionalities of the goods' under Recital 11 of the Digital Content Directive and Recital 13 of the Online Sales Directive. Consider the example of smart thermostats, of which the key functionality can be said to be the control of household heating systems. However, through in-build sensors, related software and applications for remote control (e.g. through smart phones, tablets, and smart watches), and interconnections with other household devices (such as door locks, lights, electricity sockets, sprinklers, fire alarms and home security systems) their function changes into something much wider, namely a control system for energy use and home security that might autonomously control the functionality of household appliances based on user-generated data. Knowing which Directive applies in the event of a security breach in this complex, yet increasingly real-life situation is important since the current proposals provide different rules on conformity, remedies against non-conformity and termination of contracts. To overcome potential difficulties in determining the scope of application it has already been suggested to adopt a single piece of secondary EU legislation covering all types of online and digital content contracts.[42]

What appears crucial in a review of the scope of the Digital Content Directive, the Online Sales Directive, and even the existing Consumer Sales Directive, is the **need to better integrate features of accessibility, continuity and security in the conformity assessment**. This could be done by including the principles of **privacy by design and privacy by default** as laid down in Article 23 of the General Data Protection Regulation as additional criteria for establishing conformity.[43] To define conformity in this context, regard may also be had to **accepted industry standards** laying down best practices among commercial entities, including ISO 27000-series on information security management.[44]

It is also recommended that this **conformity assessment is extended to devices operating in the IoT and the digital content provided through them**. As noted, the Digital Content Directive explicitly excludes the IoT from its scope of application, but this exclusion carries with it the danger that it would leave a potentially huge market largely unregulated in such a way that the full harmonisation objective of the current proposal would be undermined. In its Digital Single Market strategy the European Commission contends that:

41 Ch. Wendehorst, 'Sales of goods and supply of digital content – Two worlds apart? Why the law on sale of goods needs to respond better to the challenges of the digital age', briefing paper for the European Parliament, PE 556.928 (February 2016), p. 8, http://www.europarl.europa.eu/committees/nl/events-workshops.html?id=20160217CHE00181 (accessed 1 May 2016). See in the same vein, V. Mak, 'The new proposal for harmonised rules on certain aspects concerning contracts for the supply of digital content' briefing paper for the European Parliament, PE 536.494 (February 2016), p. 8-9, http://www.europarl.europa.eu/ committees/nl/events-workshops.html?id=20160217CHE00181 (accessed 1 May 2016).

42 Mak 2016 (note 41), p. 9-10.

43 Wendehorst (note 41), p. 14-15.

44 ISO, 'ISO/IEC 27001 – Information security management', http://www.iso.org/iso/home/standards/management-standards/iso27001.htm (accessed 1 May 2016).

'A fragmented market does not provide sufficient scale for cloud computing, Big Data, data-driven science and the Internet of Things to reach their full potential in Europe. To benefit fully from the potential of digital and data technologies, we will need to remove a series of technical and legislative barriers. (...) Legal certainty as to the allocation of liability (other than personal data related) is important for the roll-out of the Internet of Things.'[45]

A security breach in the IoT context may enable the unwanted access to all parts of the network. The Article 29 Working Party also notes that devices operating in the IoT are also difficult to secure, both for technical and commercial reasons.[46] Therefore, the current proposals should be revised taking into close consideration the development of the IoT and the cybersecurity issues triggered by it.

RECOMMENDATION 2 – Cybersecurity should be recognized as a main characteristic of ICT goods and services. As such, it should be part of a conformity assessment related to these goods and services. To determine the conformity of these goods and the appropriate level of security for them, regard must at least be had to the purposes for which goods and services of the same description would ordinarily be used, the particular purpose for which the goods and services are required by consumers and the security risks these goods and services pose to consumers.

RECOMMENDATION 3 – Sellers of consumer goods should not be able to contract out the confidentiality, integrity and availability of related ICT for the normal life-span of these goods. Similarly, suppliers of digital content should not be able to contract out such matters of cybersecurity for the content supplied for the duration of the related services contract.

4.2.2 Burden of proof

To further strengthen the position of consumers in relation to providers of ICT goods and services, the two proposed Directives includes rules on the **burden of proof** as regards conformity with the underlying contracts. Article 9(1) of the Digital Content Directive places the burden on the supplier, requiring it to show that the content was in conformity at the time of supply. This would also imply that the supplier carries the burden to prove that a security problem (e.g. exploits, malware, attacks, ID theft or fraud) was caused by the own fault of the consumer, e.g. irresponsible password use. In any event, the consumer does not carry the burden to prove that the digital content supplied to him/her was already non-conforming at the time of supply. The Online Sales Directive also suggests a reversal of the burden of proof with respect to conformity. Article 8(3) of the proposal holds that any lack of conformity with the contract is presumed to have existed at the time of acquiring the goods or the dispatch to a carrier chosen by the consumer. This reversal is limited to a period of two year, however. The Digital Content Directive, in contrast, does not place a time limit on its reversal of the burden of proof.

The suggested reversals of the burden of proof with respect to conformity **strengthen the legal position of consumers in important ways**. Provided that cyber security becomes an inherent part of the conformity assessment related to ICT goods and services the proposals should be welcomed. This is particularly so for reasons of cybersecurity since a security vulnerability may be

45 COM(2015) 192 final, p. 14.

46 It holds that: 'As their components use wireless communications infrastructures and are characterised by limited resources in terms of energy and computing power, devices are vulnerable to physical attacks, eavesdropping or proxy attacks. Most common technologies currently in use – i.e. KPI infrastructures – are not easily ported on IoT devices since most of the devices do not have the computing power needed to cope with the required processing tasks. Article 29 Working Party, 'Opinion 8/2014 on the recent developments on the Internet of Things' 14/EN, WP 223, Opinion of 16 September 2014.

difficult for individual consumers to discover given the potentially secretive and hidden nature of such vulnerabilities, let alone attacks or breaches. In that regard, it might be considered to extend the time limit under the Online Sales Directive for goods with embedded ICT components that were not in conformity with accepted principles of cybersecurity. This may already be read into the exception Article 8(3) of the Directive provides.[47]

RECOMMENDATION 4 – It should be considered whether time limits as regards the reversal of the burden of proof for conformity could be extended where it is difficult for individual consumers to discover security vulnerabilities.

4.2.3 Relationship with data protection law, including the right to damages

It also needs consideration that the **two proposed Directives do not provide for an explicit link with data protection law**. As noted, the Directives do not consider basic principles of data protection law, including privacy by design and default as criteria for conformity of supplied digital content and goods sold online or by other distance means. More generally, data protection laws grant rights to consumers with the view to protect their personal data and privacy (e.g. rights to withdraw consent, to information and access to data, rectification and erasure of data, data portability) and impose duties of care on controllers and processors of personal data in the handling of these data. These rights and obligations may directly affect contractual relationships between consumers and businesses.[48] For example, the exercise by a consumer of his/her right to withdraw consent to the processing of personal data under Article 7(3) General Data Protection Regulation may impact on the provision of services under a service contract for the supply of digital content. Similarly, termination of a contract for the supply of digital content would seem to imply the deletion of personal data collected under that contract. These are important questions that need to be addressed, also from the perspective of cybersecurity. The Digital Content Directive and Online Sales Directives do not provide any answers, however.

The lack of coordination between consumer sales law and data protection law also emerges in relation to the **right to damages**. Article 77 of the General Data Protection Regulation provides consumers (data subjects) with a right to compensation from the controller or processor for the material and immaterial damages they have suffered as a result of an infringement of the rules laid down by the Regulation.[49] The Online Sales Directive does not provide for a right to damages. Article 14 of the Digital Content Directive gives consumers the right to compensation of 'any economic damage to the digital environment of the consumer caused by a lack of conformity with the contract or a failure to supply digital content'.

However, this article limits the right to compensation for non-conformity to economic damages to the digital environment of the consumer. Damage to the digital content itself (e.g. unavailability, disruption or the loss of data) is not compensated under this provision and neither are consequential losses other than damage to the consumer's digital environment. Accordingly, damages suffered because of bugs in the digital content that enabled hackers to access the consumer's computer, steal (personal) data, access his/her bank account, and fully clear it, are not recoverable under the proposed Directive.[50] Even if the stolen data do not represent any economic value (e.g. family pictures, personal notes), its unavailability, disruption or loss should be compensated by allowing claims for immaterial damages congruent with the sentimental and moral value of the data, or the degree of distress and anxiety caused by the security breach, as already recognized in certain Member States and the forthcoming General Data Protection Regulation. As noted, the insecurity of software might

47 Article 8(3) Online Sales Directive provides that the two limit of two year does not apply if it 'is incompatible with the nature of the lack of conformity'.

48 Mak 2016 (note 41), p. 9.

49 Under English law, it was recently recognized that the immaterial (non-pecuniary) damages suffered by individuals as a result of the collection of personal data contrary to privacy laws can be recovered under tort law. See Vidal-Hall v. Google, [2014] EWHC 13 (QB) as upheld by Google v. Vidal-Hall [2015] EWCA Civ 311.

50 Cf Mak 2016 (note 41), p. 27.

in some instances even lead to physical insecurity and physical harm (and potentially death). Damages related to physical harm and death also seem to be excluded, however.

What is more, Article 14(2) Digital Content Directive enables Member States to lay down detailed rules on the exercise of the right to damages. The discretion provided to Member States when designing a regime for compensation might effectively undermine the objective of the Directive to provide full harmonisation measures as regards the supply of digital content to consumers.[51] In the light of the full harmonisation aim, one may also wonder whether Member States are at all allowed to provide for the right to be compensated for additional damages, as this would certainly provide more protection to consumers than the level of protection offered by the Directive itself. In line with this, some authors have noted that the removal of the consumer's right to seek compensation for other damages is to be considered wrong.[52]

Accordingly, there seems to be an **apparent mismatch between the Digital Content Directive, Online Sales Directive and General Data Protection Regulation** with regard to the scope of the right to damages. Given that many types of damages fall outside the scope of the right to damages as warranted by the Directive, the recovery of these damages is governed by non-mandatory national private laws. Consequently, it is likely that businesses will seek to exclude liability for these damage types through contractual arrangements with consumers. To the extent that suppliers of digital content can be seen as controller or processors of personal data, this would be manifestly contrary to the directly binding provisions of Article 77 GDPR. Accordingly, it is suggested that the rights to damages for consumers under the Digital Content Directive is amended along the lines of Article 77 GDPR to provide the consumer a stronger legal position to recover the damages suffered as a result of insecure digital content. Enabling the compensation of the full amount of damages suffered, strengthens the motivation for consumers to seek compensation from businesses, which may in turn **incentivize individual business and the industry at large to enhance their efforts to ensure cybersecurity**.

RECOMMENDATION 5 – Consumers should have the right to be compensated for the damages they suffered due to an established non-conformity with regard to cyber-security of ICT goods and services.

RECOMMENDATION 6 – The recoverable damages caused by such a non-conformity should not be limited to material damages only and should also include immaterial damages, in line with Article 77 of the General Data Protection Regulation.

4.3 Unfair terms

Upon concluding contracts related to ICT goods and services, consumers typically agree to the general terms and conditions of business as part of a contract. Frequently, these terms and conditions include far reaching duties and restrictions for consumers. Empirical research shows that standard form contracts and related terms and conditions are hardly ever read, in particular in online environments.[53] This creates the risk that businesses use these general terms to minimize expectations regarding cybersecurity and write off any corresponding liability. Recent studies on standard contract terms used by major online service providers and mobile applications such as Dropbox, Google, Facebook, LinkedIn, Instagram, Snapchat and Twitter demonstrate that these providers use terms that would not meet the fairness test under the Unfair Contract Terms Directive.[54] These terms include:

51 Mak 2016 (note 41), p. 27.

52 Beale 2016 (note 39), p. 24.

53 In a study by researchers at New York University the Internet browsing behaviour of 48,154 monthly visitors to the websites of 90 online software companies was tracked to study the extent to which potential buyers accessed the end-user license agreement linked to the software. The study found only one or two consumers out of every 1000 accessed the agreement. Those who did access the agreement do not read more than only a small portion. See: Y. Bakos, F. Marotta-Wurgler and D. Trossen, 'Does anyone read the fine print? Consumer Attention to Standard-Form Contracts' *Journal of Legal Studies* (2014) 43(1), p. 1-35.

54 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, *OJ* 1993 L 95, p. 29.

- The unilateral change of contractual obligations and the services that are provided under a contract with the user;
- The unilateral termination of the contract by the service provider;
- The exclusion or limitation of liability; and
- The choice of jurisdiction, including arbitration clauses.[55]

It must be recognized that **general terms and conditions related to consumer contracts for ICT goods and services should meet the fairness and transparency tests** laid down by the Unfair Contract Terms Directive. Unilateral changes as regards the level of cybersecurity provided under the contract should not be allowed without reasonable notice to the consumer. Liability exemption clauses should be closely scrutinize d as regards unfairness within the meaning of this Directive if they effectively bar consumers from obtaining compensation for the damages they suffered because of a lack of security.[56] Clauses phrased along the lines of 'any exclusions, disclaimers or limitation of liability provisions will apply to the extent permitted by local laws' may be considered to lack transparency (and thus be unfair), as the Competition and Markets Authority in the United Kingdom currently does.[57] Also clauses excluding the jurisdiction of the courts in which the consumer resides and imposing mandatory arbitration should be examined as regards their fairness. The Unfair Contract Terms Directive creates the presumption that arbitration clauses in consumer contracts are unfair and, therefore, invalid.[58] Case law of the Court of Justice of the European Union has consistently held that such clauses are to the detriment of consumers and should be considered unfair.[59]

Finally, it is well recognized that litigation by individual consumers against users of general terms and conditions is underdeveloped. In response to this stance and to ensure a high level of consumer protection across Europe, the Court of Justice has on the national courts of the Member States the obligation to apply the unfairness test under the Unfair Contract Terms Directive *ex officio*. This obligation involves the **duty of a national court to assess of its own motion whether a contractual term falling within the scope of the Directive is unfair**, thus compensating for the imbalance which exists between the consumer and the seller or supplier in drafting and negotiating the contract.[60] In the event that claims are brought to court, either by individual consumers or their representative organisations through collective action, these courts should investigate the fairness of the general contract terms used in the related consumer contracts.

Public enforcement authorities in the field of consumer protection and consumer representative bodies also have a role to play here. It is suggested that they **should proactively address the use of unfair terms** by businesses in consumer contracts relating to ICT goods and services. While public authorities may develop enforcement strategies to target such usage in the ICT sector, consumer representative bodies may initiate complementary collective action against businesses before a court to require the cessation or prohibition of the use of unfair terms.

55 See: M. Loos and J. Luziak, 'Wanted: a Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers', *Journal on Consumer Policy* (2016) 39(1), 63-90 and Forbrukerrådet (Norwegian Consumer Association), 'Appfail. Threats to Consumers in Mobile Apps' (March 2016), http://fbrno.climg.no/wp-content/uploads/2016/03/Appfail-Report-2016.pdf (accessed 1 May 2016).

56 The Annex to Directive 93/13/EEC contains an indicative and non-exhaustive list of the terms which may be regarded as unfair. Point 1(b) relates to exemption clauses as it concerns terms that have the objective of 'inappropriately excluding or limiting the legal rights of the consumer vis-à-vis the seller or supplier or another party in the event of total or partial non-performance or inadequate performance by the seller or supplier of any of the contractual obligations'.

57 Competition and Markets Authority 2015 (n 19), at para. 2.54-2.55.

58 Point 1(q) of the Annex to Directive 93/13/EEC.

59 See for example CJEU Case C-168/07, *Mostaza Claro v. Centro Movil Milenium SL* [2006] ECR I-10421 and Case C-40/08, CJEU *Asturcom Telecomunicaciones SL v. Rodriguez Nogueira* [2009] ERC I-9579.

60 See most recently CJEU Case C-377/14, Radlinger v. Finway, ECLI:EU:C:2016:283 (decision of 21 April 2016), paras. 52-53.

RECOMMENDATION 7 – General terms and conditions related to consumer contracts of ICT goods and services must meet the requirements of fairness and transparency as laid down by the Unfair Contract Terms Directive. National courts, public enforcement authorities and consumer representative bodies should intervene proactively within the scope of their respective competences to better address the use of unfair terms by businesses in the ICT sector in consumer contracts.

4.4 Liability in the ICT supply chain

So far this White Paper has addressed the duties of care and diligence as regards cybersecurity arising under contractual arrangements between businesses and consumers relating the ICT goods and services. However, the ICT supply chain involves a much **wider range of actors concerned with the delivery of secure ICT**. To give an example, the seller of smart goods with embedded software is to some extent dependent on the care taken by the software developer for the security of that software. There might be good reasons why consumers suffering damages because of a lack of cybersecurity would want to hold liable these third parties for damages rather than their respective contracting parties.[61]

However, the current legal framework applying to the extra-contractual liability of third parties for damages caused by a lack of cybersecurity fails to provide sufficient incentives for the ICT sector to secure higher levels of cybersecurity.[62] More specifically, **the conditions governing the extra-contractual liability of these actors (including tort, laws of delict or unlawful act, and product liability) have proven difficult to satisfy** for consumers in order to compensate the damages caused by a security breach. Under these liability regimes the burden of proof concerning the existence of a duty of care, the breach of that duty, and the causal link between that breach and damages suffered typically lies with the claimant. Furthermore, the widespread use of liability exemption clauses may also limit the extent to which damages can be claimed. Whereas the Product Liability Directive has established a fully harmonised strict liability regime for producers as regards damages caused by defective products,[63] it is unclear to what extent this regime applies to faulty software as such, or to software embedded in products.[64]

4.4.1 Product liability

To further strengthen the duty of care as regards cybersecurity in the ICT sector, and provide better possibilities for end-users sustaining damages because of a lack of such security, it is suggested to **extend the strict liability regime for damages caused by defective products laid down by the Product Liability Directive to software**. Such extension appears to be in line with the position of the European Commission in the late 1980s.[65] Accordingly, the concept of 'product' as set out in Article 2 of this Directive should be read to include software, irrespective of whether it is provided by downloading or streaming, or on a tangible medium or by other means.[66] Updates and upgrades of software should also considered part of the definition of product. Products with embedded software would logically qualify under this definition as well if that software proves vulnerable in terms of cybersecurity.

61 These reasons involve practical reasons (e.g. if the contracting parties turn out to provide fewer possibilities to recover all damages, for example because of a lack of financial means or insolvency), but also legal concerns (e.g. the applicability of liability exemption clauses).

62 Tjong Tjin Tai e.a. 2015 (note 1), p 135-136.

63 Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (OJ L 210, 7.8.1985, p. 29), last amended by Directive 1999/34/EC of the European Parliament and of the Council (OJ L 141, 4 Jun. 1999, p 20).

64 Tjong Tjin Tai e.a. 2015 (note 1), p. 54 and 84.

65 Lord Arthur Cockfield, then vice-President of the European Commission and Commissioner for Internal Market, Taxes and Customs, noted in his written response on behalf of the Commission to question raised by Mr. Gijs de Vries (LDR-NL) whether the Product Liability Directive also covers computer software that the Directive indeed 'applies to software in the same way (...) that it applies to handicraft and artistic products'. Response to written question No. 706/88, *OJ* C 114, 8.5.1989, p. 42. The Court of Justice of the EU has not had the opportunity to rule on the matter as a case concerning insecurity digital content or products with embedded digital content has not been presented to it so far.

66 Cf. Article 2(1) Digital Content Directive.

The inclusion of software within the material scope of the Product Liability Directive offers **important advantages to consumers who want to obtain compensation for damages caused by insecure software.** The Product Liability Directive establishes a regime of strict liability for specific damages caused by a defect in a product that was placed on the market by the producer. Article 4 of the Directive requires a claimant to prove the damage, the defect and the causal relationship between defect and damage. Fault on the part of the producer does not need to be established. With the extended scope of the Directive as proposed here, the developer of software or applications that place these 'products' on the market can also be held liable as a 'producer'. Furthermore, Article 3(1) may also provide that where a business only supplies a specific part of the software (e.g. the source code of software, which is then moderated by another actor), it can nonetheless be held liable as a producer of a 'component part' of the product.[67] Article 3(2) may enable that if the software developer cannot be identified, which might be a real risk for consumers in IoT environments, the supplier of the software shall be treated as its producer, unless he informs the consumer, within a reasonable time, of the identity of the software developer or of the person who supplied him with the software. Accordingly, **the multi-layered concept of producer as presented by the Directive would closely fit with characteristics of the ICT supply chain,** in which almost all goods and services are composite 'products'.[68] The Directive notes that if two or more producers are liable under its regime, they are jointly and severally liable.[69]

Article 6 of the Product Liability Directive holds that a product is defective when it does not provide the safety which a person is entitled to expect, taking all circumstances into account. **Software with security vulnerabilities should be considered defective**.[70] Producers should take into account any foreseeable irresponsible use of software, for example by implementing smart solutions as regards cybersecurity based on security by design (e.g. no default passwords and the automated implementation of crucial security updates or upgrades). The defect does not need to materialise in reality: **the risk of a defect or 'potential for failure' has been considered sufficient to prove the defectiveness of the product**.[71] In the case of a security vulnerability this implies that potential attacks causing damages to the consumer are not required to establish liability on the part of the producer. The costs 'necessary to overcome the defect in the product in question' may in that case be compensated to the extent that they fall within the scope of Directive.[72]

Article 9 of the Product Liability Directive stipulates that damages caused by death or by personal injury can be compensated, as well as damage to, or destruction of any item of property other than the defective product itself and used by the injured person for private use and consumption, with a lower threshold of € 500. This concept of damages is rather restricted and consequential losses other than medical costs (e.g. pure economic losses, loss of income, and damage to the product itself) cannot be compensated. This significantly limits the potential for consumers to recover their damages from producers and, in turn, the practical importance of the Product Liability Directive.[73]

67 This implies that only those actors putting into circulation software, applications or components thereof can be held liable under the regime. Individual developers working under the supervision of these actors (e.g. employees) will not be liable vis-à-vis consumers. Also component producers will be able to escape liability where they show that the defect is attributable to the design of the product in which the component has been fitted or to the instructions given by the final producer of the product (cf. Article 7(f) Product Liability Directive).

68 Noto La Diega and Walden (note 10), p. 23.

69 Article 5 Product Liability Directive.

70 This is in line with what has been argued above (paragraph 4.2.1) in relation to conformity in sales law.

71 CJEU Joined Cases C-503/13 and C-504/13, *Boston Scientific Medizintechnik GmbH* v. *AOK Sachsen-Anhalt and Betriebskrankenkasse RWE*, ECLI:EU:C:2015:148 (decision of 5 March 2015), paras. 40-42.

72 Ibid., para. 54.

73 See in general B. van Leeuwen and P. Verbruggen, 'Resuscitating EU Product Liability Law? Contemplating the Effects of Boston Scientific Medizintechnik (Joined Cases C-503 and 504/13)', 23(5) *European Review of Private Law* **2015, 899-915.**

To further enhance the legal position of consumers of software it may **be considered whether these end-users should be allowed to claim a broader set of damages from the producer based on the strict liability system as set out in the Product Liability Directive** in case of a lack of cybersecurity. Introducing a right for consumers to recover both material and immaterial damages under this Directive would be congruent with developments in the field of data protection law, in which Article 77 of the forthcoming General Data Protection Regulation will allow data subject to claim from controllers or processors such damages.

Article 9 of the Directive already enables compensation of damages caused by personal injury. Where software insecurity translates into physical insecurity and thus causes harm, which is more likely to occur where household appliances are connected in the IoT,[74] that harm may be compensated under the Directive. **Damages to items of property should be read to include also damage to hardware devices or damage or loss of digital content stored** on the consumer's devices or via cloud computing services. Damages should also include the necessary costs incurred by a consumer to prevent the risk caused by the defective product (e.g. a potential intrusion in the consumer's digital environment) from happening. These costs might include the price of related to necessary updates or upgrades to patch the security vulnerability and the costs related to restoring and retrieving any lost data.

Another additional advantage of bringing software within the scope of the Directive is that **producers are prohibited to limit or exempt their liability arising from the Directive to consumers**.[75] Currently, producers frequently exclude their liability for damages caused by the software embedded in their products.[76] Such limitations or exemptions would no longer be allowed in relation to the liability for damages sustained by consumers and covered by the Directive.

We anticipated that the inclusion of software in the material scope of the Product Liability Directive creates spin-off effects for more general regimes governing extra-contractual liability (tort and delict law) such that concepts developed under the Directive translate into and influence concepts used to establish liability under these regimes (e.g. the concept of product, the duty of care of producers, and burden of proof for *culpa*), as it has done in the past.[77]

RECOMMENDATION 8 – The material scope of the Product Liability Directive should be revised so as to include software.

RECOMMENDATION 9 – Damages to items of property for personal use should be interpreted to include also damage to hardware devices or damage to or loss of digital content. It may be considered whether and to what extent consumers of software, regardless of whether it is embedded in a product, may be enabled to claim both material and immaterial damages from the producer based on the strict liability system as set out in this Directive.

4.4.2 Development risk defence

Importantly, the producer escapes all liability arising from the Product Liability Directive if he proves that 'the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered.'[78] This so-called **development risk defence offers businesses in the ICT sector**,

74 See note 11.

75 Article 12 Product Liability Directive.

76 Noto La Diega and Walden cite a 'limited warranty' clause used by Nest Labs Europe Ltd in relation to Nest products, which states that the warranty 'does not cover consumable parts, including batteries, unless damage is due to defects in materials or workmanship of the Product, or software (even if packaged or sold with the Product)'. See Noto La Diega and Walden (note 10), p. 23.

77 See in general Van Leeuwen & Verbruggen 2015 (note 76).

78 Article 7(e) Product Liability Directive.

in which technologic knowledge is highly fluid and rapidly evolving, **a very significant instrument to fend off liability claims** related to insecure software. As the ICT industry would typically contend, there is no such thing as 'bug free' software. Accordingly, it might argue that software developers who did not discover any serious vulnerability at the time of the release of its product would be able to take advantage of the defence.

While Member States are allowed to exclude the development risk defence under the Directive, only Luxembourg and Finland have used this possibility.[79] To strengthen the position of consumers in recovering damages sustained due to a lack of cybersecurity, **the European legislature and the individual Member States should critically consider the application of this defence in relation to defective software**. While it should be acknowledged technological development in the ICT sector is fast, the release of software that disregards known and knowable vulnerabilities in terms of cybersecurity should preclude the producer from relying on the development risk defence. This should also apply to updates and upgrades of software which do not sufficiently take into account observed security threats. The defence should be interpreted restrictively.[80] Allowing for an extensive interpretation of the defence would not seem to be in line with the high level of protection offered in the domain of data protection law through the forthcoming General Data Protection Regulation, which requires controllers and processors of personal data to implement appropriate technical and organisational measures to secure personal data.

RECOMMENDATION 10 – To the extent that software falls within the material scope of the Product Liability Directive, the development risk defence allowed under the Directive should not be interpreted extensively such to exclude the liability of producers for a release of software (including updates or upgrades of it) that disregards known and knowable security vulnerabilities.

4.4.3 Product surveillance and recall

Product safety laws impose duties on producers to control, inspect and monitor the quality of the products they place on the market. In general, they need to be informed of the risks these products might pose to consumers and must be able to take appropriate action necessary to avoid these risks, including the communication of adequate and effective warnings and the organisation of product recall from distributors and consumers. Also distributors of products are obliged to act with due care to help to ensure compliance with the safety requirements, in particular by not supplying products which they know or should have presumed, on the basis of the information in their possession and as professionals, do not comply with those requirements.[81]

Where producers place on the market ICT goods and services, it should be considered whether general duties of product safety law concerning product surveillance may also apply to these goods and services. This could imply that producers of such goods and services are required to monitor these products in terms of security vulnerabilities through surveillance and testing mechanisms during normal life-span of these products. **Where vulnerabilities are discovered, they could be required to issue notifications and warnings to consumers, and in cases of high risk, a product recall.** If this concerns products with network connectivity, a notice, warning or recall could effectively and efficiently be organised through pop-up messages or screen alerts. Furthermore, they could be blocked or frozen in order to patch the vulnerabilities and restore the security of the goods and services. The risk of incurring liability for damages arising under the Product Liability Directive may provide additional incentives to issue effective warnings and organise recalls.

79 Article 15(1)(b) Product Liability Directive.

80 See also Case C-300/95, *Commission v. United Kingdom* [1997] ECR 1997, p. I-02649, paras. 26-29.

81 Article 5(1) and (2) Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (OJ L 11, 15.1.2002, p. 4). Article 17 Directive 2001/95/EC notes that it shall be without prejudice to the Product Liability Directive.

RECOMMENDATION 11 – Businesses placing on the market ICT goods and services should be required to control, monitor and inspect these goods and services in terms of security vulnerabilities throughout the normal life-span of these products or for the duration of the related services contract.

4.5 Enforcement

It has been noted above that individuals typically lack the information, legal expertise and financial resources necessary to initiate proceedings against actors in the ICT supply chain and be successful. Courts, public enforcement authorities and consumer representatives can complement the actions of individual consumers to enforce their rights in important ways, as already observed in the case of unfair contract terms. Collective action by consumers or their representative bodies would appear more effective than individual action,[82] although its success is not guaranteed.[83] Some ICT providers have been noted to develop strategies to forestall class actions.[84]

Collective action has only in part been harmonised in the EU. The Injunctions Directive provides rules for consumer representative bodies and public enforcement authorities to bring collective actions against traders for the cessation or prohibition of infringements of consumer rights.[85] The Directive does not provide for harmonisation as regards the collective recovery of mass damages. It should be investigated whether and how the Injunctions Directive can assist consumer representative bodies and public enforcement authorities in the protection of consumer interests related to cybersecurity.

We suggest conducting a similar investigation for the recently adopted Alternative Dispute Resolution (ADR) Directive and the Online Dispute Resolution (ODR) Regulation.[86] These legislative instruments both aim to provide to consumers easy and low-cost dispute resolution in order to find out-of-court solutions to their disputes with traders arising from cross-border (online) transactions. In the absence of these solutions, such disputes currently are often left unresolved.

Public enforcement authorities in the fields of data protection law and telecommunications law have developed national and cross-border policies relating to cybersecurity. It is suggested that also national public authorities in the **field of competition, trade and consumer law need to (further) develop policies on cybersecurity, preferably in coordination with other competent national authorities.** Campaigns to raise awareness amongst consumers as regards risks of cybersecurity may already address a number of important issues and have been applied

82 Tjong Tjin Tai e.a. 2015 (note 1), p. 139-155.

83 In the US, a number of class actions involving security breaches have been filed. See for a list of these class actions: www.lawyersandsettlements.com/lawsuits-filed/internet-technology-lawsuits/ (accessed 1 May 2016). It is unclear how successful these class actions are in providing consumers with remedies. There are few final court decisions and the settlements themselves are not disclosed. Moreover, Settlements may not necessarily resolve security threats, as the settlement in the class action brought against Sony for the major security breach of its Playstation Network in 2011 shows (see: https://www.bigclassaction.com/lawsuit/sony-employee-data-breach-class-action-lawsuit.php, accessed 1 May 2016).

84 In response to a class action filed against Dropbox for its authentication bug before the US District Court, Northern District of California (*Christina Wong, et al. v. DropBox, Inc.*, Case. No. CV-11-3092), the California-based company amended its Terms of Services requiring users in the US to sign up to mandatory arbitration and a prohibiting them to initiate class actions. See: http://www.computerworld.com/article/2487987/cloud-computing/update--dropbox-changes-its-terms-of-service-to-stop-class-action-lawsuits.html and Dropbox Inc., 'Dropbox Terms of Service' (Version of November 4, 2015) https://www.dropbox.com/terms?view_en#terms (both accessed 1 May 2016).

85 Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests (Codified version), *OJ* L 110, 1.5.2009, p. 30-36. The consumer rights that can be protected through the harmonised collective action concern the rights granted under the Directives on consumer rights, consumer credit, package travel, unfair commercial practices, unfair terms in consumer contracts and consumer sales.

86 Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes (Directive on consumer ADR) OJ L 165, 18.6.2013, p. 63-79 and Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR), OJ L 165, 18.6.2013, p. 1-12.

successfully in the past.[87] Such campaigns may be organised together with relevant business organisations and consumer representative bodies to strengthen their legitimacy base and effectiveness.[88]

RECOMMENDATION 12 – It should be investigated whether and how existing EU legislative instruments intended to improve consumer access to justice might be applied effectively to provide consumer protection in relation to disputes with traders concerning cybersecurity.

RECOMMENDATION 13 – Public enforcement authorities should complement enforcement activities taken by individual consumers and consumer representative bodies, for example by developing awareness raising campaigns as regards cybersecurity risks.

5. APPROACHES TO HARMONISATION

There is a wide array of techniques to achieve harmonisation as regards duties of care and diligence in cybersecurity, ranging from bottom-up 'spontaneous' harmonisation at the national levels to top-down legislative intervention through Regulations adopted by the EU legislature. Each of these approaches has its relative advantages and disadvantages. Generally, the harmonisation of consumer rights in the EU is orchestrated through the adoption of Directives, aiming to establish a minimum or maximum harmonised level of protection by the laws of the Member States. Regulations are not typically used as legislative instruments if consumer rights are established or harmonised. However, where harmonisation specifically concerns procedures for the enforcement of consumer rights, Regulations might be used as legislative instruments.

Having regard to the topics discussed in this White Paper, however, **it is unrealistic to expect that all these topics can be harmonised by adopting one single legislative measure with a single approach to harmonisation for cybersecurity.** In fact, several recommendations offered here do not require any legislative action at the EU or national level, but simply different action under the existing legal framework. It is therefore proposed that, to the extent possible, **the amendments suggested here should be incorporated in the existing legislative frameworks or proposals for legislation**, each having its own approach to harmonisation.

It must be noted, however, that in these legislative frameworks and proposals due regard must be had to private, **industry standards for cyber security**. These rules might be technical standards or industry codes of conduct and good practices, concerning technical aspects of cybersecurity, but also organisational (or management) requirements to ensure the confidentiality, integrity and availability of ICT goods and services. **If adopted at the international level, such as the ISO 27000-series, and widely implemented in the entire ICT supply chain through the use of contractual arrangements or procurement policies, these private standards may offer additional harmonisation effects in the ICT sector.** Such effects might further be bolstered by incorporating such standards in relevant legal frameworks concerning the assessment of the existence, scope and violation of duties of care and diligence in cyber security.

87 See for example the campaign 'Updates in, hackers out' organised by the Dutch Authority for Consumers and Markets in 2014 to raise awareness amongst Dutch consumers about the importance of up-to-date software. See https://www.consuwijzer.nl/thema/veilig-internetten-updates-binnen-hackers-buiten (accessed 1 May 2016).

88 See for example the campaign 'Alert Online' supported by government bodies and representatives from business and society in the Netherlands. The campaign sets the goal 'to encourage greater awareness of cyber security in government and the business community, as well as among consumers in general.' See on this background of this campaign: https://www.alertonline.nl/over_alert_online/About-Alert-Online/ (accessed 1 May 2016).

6. CONCLUSION

This White Paper has sought to provide a framework for discussion around the need to harmonise legal standards for duties of care and diligence concerning cybersecurity and offer proposals to better protect the interests of consumers and data subjects in terms of the confidentiality, integrity and availability of ICT goods and services. Acknowledging that the policy field of cyber security is wide, diverse and only in part regulated and harmonised, the White Paper has focused on the general EU legal framework applying to commercial transactions between ICT providers and consumers with respect to ICT goods and services. Various elements of this legal framework have been critically discussed as regards the scope of protection offered by them to consumers and, accordingly, suggestions were offered for improvement.

It needs to be stressed once more that **the exact scope of the duty of care and diligence that an ICT provider owes to a consumer as regards cybersecurity of ICT goods or services, if any, ultimately depends on the set of circumstances of a particular case.** It is not possible (or desirable) to define in detail the duties of care and diligence ICT providers owe to consumers in their commercial dealings. Such specified rules do not match with the wide diversity of cybersecurity threats (e.g. vulnerabilities, exploits, malware, attacks, ID theft and fraud), or with the constitutive elements of cybersecurity (i.e. confidentiality, integrity and availability). Moreover, specified rules would run the risk of becoming impracticable and obsolete soon after their enactment given the rapid technological developments in the ICT sector.

Therefore, we suggest to rely on accepted and tested **open norms** in the domain of European private law (including the concepts of 'conformity', 'unfairness', 'defectiveness'), and to interpret these norms to accommodate concerns of cybersecurity in relation to ICT goods and services provided by businesses to consumers. In assessing whether a duty of care and diligence has been breached in a specific case, the following circumstances should at least be taken into account:

- The purposes for which goods or services of the same description as sold by the ICT provider to the consumer would ordinarily be used;
- The purpose for which the consumer requires the goods and services, as communicated to the ICT provider;
- The legitimate expectations of the public at large;
- The presentation of or public statements about the goods and services by the ICT provider;
- Any foreseeable irresponsible (mis)use by the consumer;
- The nature and severity of the risks poses by the ICT goods or services to consumers;
- The nature and severity of the damages involved;
- The state of scientific and technical knowledge at the time the ICT provider started to offer the goods or services to consumers;
- (Non-)compliance with accepted private industry standards.

Accordingly, duties of care and diligence in cybersecurity can be differentiated in relation to the type of cybersecurity threat, the ICT provider, and the goods or services involved. Such **a principle-based approach corresponds with the regulatory approach taken under the General Data Protection Regulation and the Network and Information Security Directive**, which require controllers and processors of personal data and operators of networks and information systems to have in place appropriate technical and organisational measures to manage the risks posed to the security of these data and networks and information systems.

ANNEX: GLOSSARY OF TERMS

Application – A specific form of software designed to run on hardware and perform tasks for the benefit of the user.

Consumer – Any natural person who is acting for purposes which are outside his trade, business, craft or profession.

Controller – The natural or legal person, public authority, agency or other body which, alone or jointly with others, who determines the purposes and means of the processing of personal data.

Cybersecurity – The situation in which ICT and all of its relevant components are safe from threats to its confidentiality, integrity or availability and to the data (including personal data) handled through it.

Data subject – A natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Digital content – Data which are produced and supplied in digital form (including computer software, applications, games, music, videos or texts), irrespective of whether they are accessed through downloading or streaming, from a tangible medium or by other means. Digital content also includes services allowing for the creation, processing and storage of data in digital form and for the sharing of such data with other users of the service.

Duty of care and diligence – The legal obligation to act with due care or use professional diligence towards the legitimate interests of others.

General contract terms – A contractual term which has not been individually negotiated and has been set by a trader with the view to be used in multiple contracts.

Hardware – The collection of physical elements that constitutes an ICT system.

Hacker – A persons who seeks and exploits vulnerabilities in ICT systems or services in a malicious manner or for personal gain.

Information and Communication Technologies (ICT) – Technologies that enable users to access, store, transmit, and change information.

ICT goods and services – Goods and services based on ICT, including systems, infrastructures, networks, hardware, firmware, software, applications and digital content.

ICT providers – Business actors offering on the market ICT goods and services.

Internet of Things – The infrastructure in which devices ('things') are designed to record, process, store and transfer data (including personal data) and interact with other devices or systems using network capabilities in order to deliver services or digital content based on the collection and further combination of these data.

Internet service providers (ISPs) – For-profit or not-for-profit actors that store and transmit Internet traffic, data and online content, including hosting providers, access providers and other content and service providers (including search engines, trading platforms, social media).

Personal data – Any information relating to an identified or identifiable natural person, that is, the data subject.

Personal data breach – A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Processing – Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor – A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Software – Set of information and instructions that enable the operation of hardware, including application software, system software, and malicious software (malware).

Security by design – The situation in which ICT goods and services have been designed to provide the appropriate technical and organisational measures to ensure cybersecurity, given the ordinary use of these systems and services and the foreseeable risks they pose to users.

Trader – Any natural person or any legal person who is acting for purposes relating to his trade, business, craft or profession and any other person acting in the name or on behalf of a trader.

Vulnerability – A characteristic of ICT goods or serviced that enable their unauthorized disruption, failure or misuse.