Centre for Strategy & Evaluation Services

Product-based case studies

Annex 8

Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment

716/PP/GRO/IMA/18/1133/10768 IMPLEMENTING FRAMEWORK CONTRACT 575/PP/2016/FC

April 7th 2020

Case study writers: Mark Whittle (CSES), Eugénie Lale-Demoz (CSES), James Eager (CSES), Richard Potter (Tech4i2) and Professor Paul Foley (Tech4i2).

QA review by: External expert, Dr. Marie-Helen Maras

Centre for Strategy & Evaluation Services LLP
Westering House
17 Coombe Road
Otford, Kent TN14 5RJ
United Kingdom
E: enquiries@cses.co.uk
T: +44 (0) 1959 525122

Contents

Tables

List of acronyms

Acronyms	Full meaning
AI	Artificial intelligence
AES	Advanced Encryption Standard
AMD	Advanced Micro Devices
B2B	Business-to-business
B2C	Business-to-consumer
BYOD	Bring Your Own Device
C2	Command-and-control servers
CAGR	Compound annual growth rate
CBA	Cost-Benefit Analysis
CCTV	Closed-circuit television
CISA	Cybersecurity and Infrastructure Security Agency (US)
CJEU	Court of Justice of the European Union
CLASP	Lightweight Application Security Process
CNIL	Commission Nationale de l'Informatique et des Libertés (French)
CoP	Code of Practice
COPPA	Children's Online Privacy Protection Rule (US)
CSA	Cybersecurity Act
CVE	Common Vulnerabilities and Exposure
DA(s)	Delegated Act(s)
DCMS	Department for Digital Culture, Media and Sport (UK)
DDoS	Distributed denial of service (attacks that can be mounted at the network level using networks of hacked individual IoT security devices)
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security (US)
DNS	Domain Name Server
DPbDD	Data protection by design and default
DPA	Data protection authorities
DPIA	Data Protection Impact Assessment (process that helps organisations identify and minimise risks that result from data processing. DPIAs are usually undertaken when introducing new data processing processes, systems or technologies)
DSM	Digital Single Market
EO	Economic operators
EDPB	European Data Protection Board
ENISA	European Network and Information Security Agency
EoL	Older End of Life
ePD	ePrivacy Directive (Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in Electronic Communications)
ePR	ePrivacy Regulation (Proposal for a Regulation of the EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications. COM/2017/010 final - 2017/03 (COD)
ESO	European Standardisation Organisations
ETSI	European Telecommunication Standards Institute

Acronyms	Full meaning
FCC	Federal Communications Commission (US)
GDPR	General Data Protection Regulation (EU) 2016/679 (GDPR)
GPR	Ground-penetrating radar
GPS	Global Positioning System
GVC	Global Value Chains
HTTPS	Hypertext Transfer Protocol Secure
IA	Impact Assessment
ICO	Information Commissioner's Office (UK)
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things. IoT system architecture is generally divided into three layers: the perception layer, the network layer and service layer (or application layer)
IoTSF	Internet of Things Security Foundation
IP	Internet Protocol address
IR	Infrared
ISE	Independent Security Evaluators
LAN	Local Area Network
LTE	Long-Term Evolution standard for wireless broadband communication for mobile devices and data terminals
MAC	Media access control address
MMS	Multimedia Messaging Service
MSA	Market Surveillance Authority
NACE	*Nomenclature des Activités Économiques dans la Communauté Européenne)* is a European industry standard classification system similar in function to Standard Industry Classification (SIC) and North American Industry Classification System (NAICS) for classifying business activities.
NAT	Network Address Translation
NCC	Norwegian Consumer Council
NCSC	National Cyber Security Centre (UK
NLF	New Legislative Framework
NFC	Near field communication
NGO	Non-Governmental organisation
NIST	National Institute of Standards and Technology (US)
NVR	Networked video recorder
ODM	Original Design Manufacturer
OEM	Original Equipment Manufacturer
ONVIF	Open Network Video Interface Forum
OPC	Open Public Consultation
OS	Operating System
PESEL	Personal Identification Number (Poland)
PO	Policy option(s)
RE	Radio Equipment
RE EG	Radio Equipment Expert Group
RED	Radio Equipment Directive (2014/53/EU)

Acronyms	Full meaning
RED ADCO	Radio Equipment Directive Administrative Cooperation Group
RFID	Radio-frequency identification
RSA	Rivest–Shamir–Adleman
SBS	Eurostat's Structural Business Statistics (SBS), which shed light on relevant classes of connected Radio Equipment and Wearables.
SCC	Surveillance Camera Commissioners (UK)
SDL	Security Development Lifecycle
SIM	Subscriber identity module
SMS	Short message service
SQUARE	Security Quality Requirements Engineering
SRE	Security Requirements Engineering
SSL	Secure Sockets Layer
T&C	Terms and conditions
TCP	Transmission Control Protocol
TEE	Trusted Execution Environment - a secure area of a main processor.
TLS	Transport Layer Security
TUIs	Trusted User Interfaces for securing critical mobile apps.
TS	Technical Standard
VMS	Video management system
VSS	Volume Shadow Copy Service
WAN	Wide area network
WEP	Wired Equivalent Privacy
Wi-FI	Wi-Fi a family of wireless networking technologies, based on the IEEE 802.11 family of standards, which are commonly used for local area networking of devices and Internet access
WLAN	Wireless local area network
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup
WTP	Willingness to Pay (concept in economics that can be applied to data protection and privacy i.e. how much do consumers and businesses value their data, and what types of personal data are they willing to share via their connected radio equipment products and devices?

1. Introduction

1.1 Introduction - Product-based case studies

This standalone annex contains product case studies carried out as part of the study assignment *Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment.*

1.1.1 Purpose of the case studies

The purpose of the case studies was, in summary, to:

- Identify and analyse the main security vulnerabilities of the RE product groups selected in relation to i) data protection and privacy and ii) protection from fraud;
- Identify the types of personal data being collected, as well as any data of a non-personal nature;
- Ascertain which is the applicable EU legislation currently (e.g. the GDPR, e-Privacy Directive) and assess how effective this has been in terms of providing adequate safeguards to ensure adequate levels of i) data protection and privacy and ii) protection from fraud;
- Assess the implications for the different policy options (regulatory, non-regulatory) identified for the impact assessment study for the product group concerned;
- Assess how far there are suitable technical solutions available already in the market that could help to address identified vulnerabilities e.g. encryption and authentication;
- Consider the extent to which the setting of minimum baseline security requirements through a regulatory approach could help to 1) address the identified risks and 2) support more effective implementation of data protection by design and default principles in the GDPR;
- Gather any feedback from producers and / or other stakeholders as to what would be the costs for industry in the product group concerned were the two Delegated Acts within scope to be activated.
- Check how far industry has already been taking steps to address identified vulnerabilities, and industry views on whether different types of non-regulatory approaches could be viable (e.g. industry codes of conduct, industry-led standards, joint certification schemes with the Commission through the Cybersecurity Act, etc.

1.1.2 Selection criteria and product groups selected for case studies

A number of selection criteria were applied for the product case studies, namely the need to achieve a balance between:

- Internet-connected radio equipment products by market segment e.g. sufficient representation of different sectors such as consumer electronics, household appliances, wearables;
- Internet-connected RE products with differing levels of risk from a cybersecurity vulnerability point of view;
- Products depending on the level of sales. It was important to include consumer IoT devices sold in high volume, which are ubiquitous in homes and offices, along with more specialist products.

An overview of the six product-based case studies – and the justification for their selection – is provided in the following table:

Table 1-1 - Product case studies

Product type	Risks	Justification for selection in longlist
Laptops	• Commonly used product for both personal and business purposes in Europe. • Some common risks such as the frequent connection of laptops to a wide range of internet-connected radio equipment through varied radio communication means (for example, wireless routers via WLAN or smart watches via Bluetooth), the risks highlighted through the other case studies are also relevant to laptops. • In addition, users often store significant amounts of personal and non-personal data on their laptops, which are vulnerable to a wide range of cyber-attacks.	• Laptops make an interesting case due to the complexity of their production, the combination of multiple hardware (including cameras and microphones) and software elements and their frequent connection to multiple internet-connected devices via varied means (e.g. WLAN, Bluetooth and more recently LTE). • Furthermore, laptops are regularly used by a significant proportion of EU citizens to store personal and non-personal data for both personal and business purposes.
Routers (wireless)	• Examples of security vulnerabilities relating to routers are: inadequate authentication, TCP injections and problems with the efficacy of some firewalls. • Weaknesses in how saved passwords in the browsers Google Chrome and Opera interact with Wi-Fi over unencrypted connections[1]. The hacker would be able to join the Wi-Fi network, access shared files, access IoT devices which trust the local network [and] view what websites everyone is visiting," If those websites are unencrypted, the hacker could attempt to implant malware onto the device to steal passwords. Routers can also be hacked by the use of a fake landing page[2]. • However, to compromise a home network, the criminal would need to be within Wi-Fi range of router. Additionally, the victim's device would need to be using the Chrome or Opera browsers that have the router's login credentials to an open network saved. • Nevertheless, to compromise a home network, the criminal would need to be	• Routers are both a RE piece of equipment in their own right, and a gateway to accessing a network of other internet-connected IoT devices and equipment. • Therefore, if a router is penetrated, personal data on the network could potentially be compromised if other devices are not secured. • NL study into cybersecurity risks identified routers as having some security vulnerabilities and presenting certain risks. • Chance to highlight differences in level of risk between consumer and enterprise grade products. • Useful to demonstrate the extent and nature of network-based rather than product-based risks. Some industry associations argue that routers are secure, therefore the devices within the network are secure, even if the devices themselves are not secure. This could prove otherwise.

[1] Murdock, J. (2018). Millions of Home Wi-Fi Networks at Risk of Hacking, Cybersecurity Firm Claims. Newsweek, September 5, 2018. https://www.newsweek.com/millions-home-wi-fi-networks-risk-hacking-cybersecurity-firm-claims-1105525

[2] Moore, M. (2018). Is your router a cybersecurity risk? *TechRadar*, August 20, 2018. https://www.techradar.com/news/is-your-router-a-cybersecurity-risk

Product type	Risks	Justification for selection in longlist
	within Wi-Fi range of router. • Chrome browsers save Wi-Fi router administration credentials and re-enter them automatically—an auto-fill process that is designed for convenience. The victim's device would need to be using the Chrome or Opera browsers that have the router's login credentials to an open network saved. • Router details obtained could be used to capture the Wi-Fi network password[3].	
(Connected) Security Cameras and Baby Monitors	• The technology behind CCTV cameras is widening to include personal identification through facial recognition. These raise important privacy and ethical considerations. • Video-surveillance footage often contains images of people. As this can be used to identify these people either directly or indirectly it qualifies as personal data[4]. • An increasing number of video surveillance systems can be run through mobile devices • There have been a number of scandals involving hacking of unsecured baby monitors and security cameras connected directly to the internet.	• Video surveillance systems of up to ten network cameras can be managed entirely via mobile devices, no longer requiring a desktop PC to run video management software. • Users are more open to using a smartphone app than having to use a comprehensive video management software on a desktop PC, whilst also reducing overall system and maintenance costs. • However, using such apps on a mobile phone may expose users to greater security vulnerabilities. • Advances in CCTV technologies – especially from analogue CCTV cameras to internet protocol (IP) ones increases information security and privacy concerns. • Manufacturing of CCTV cameras and facial recognition technologies is rapidly increasing: in the UK alone, there is one CCTV camera for every 11 people. All countries with a population of at least 250,000 are using some form of AI surveillance systems to monitor their citizens.[5]
Smart Toys	• There have been a number of high-profile cases in recent years involving internet-connected toys that have highlighted particular security vulnerabilities. • These relate to data protection and	• Whilst a small percentage of the global market and only an estimated 2-3% of the European market, smart toys are growing in popularity. • The advent of new technologies such as AI and increased desire to interact with toys means this trend may continue in

[3] An argument made against this was that *"the majority of Wi-Fi networks are encrypted in recent years, which means that this attack would not be viable. Even if you can find an unencrypted Wi-Fi network, you would still have to find a victim on said network who is actively using Chrome or Opera, and who had the administrator credentials for the network router saved in the browser".*

[4] https://edps.europa.eu/data-protection/data-protection/reference-library/video-surveillance_en

[5] https://www.bbc.co.uk/news/business-50348861

Product type	Risks	Justification for selection in longlist
	privacy, although there have also been examples of fraud attempts by ransoming user accounts of hacked smart toys (e.g. hack of database of smart Teddy Bear accounts). • There are examples of risks relating both to products directly and indirectly connected to the internet.	future. • There are concerns regarding safeguarding the privacy of children, including concerns regarding geo-locational data being collected. • There is also evidence that industry practices are already changing over the course of the development of successive generations of smart toys, which have relatively quick product development lead-times to tighten security (at least among the leading global manufacturers, in an industry in which the top 10 players account for as high as 80% of the market. • Also, interesting examples of how industry has changed the documentation of business processes due to the GDPR, but is also partly self-regulating, aware that the regulatory environment for smart toys is evolving.
Smart TVs	• Examples of security vulnerabilities have been identified such as: • Pre-product-placement – embedding of software able to track TV viewing usage. Risks to viewers – privacy could be compromised. • Post placement on the European market, lack of updating of software and firmware. • Whilst formally outside the RED's present scope if there are no regular software and firmware updates, then there could be security vulnerabilities for the rest of the IoT network. This might affect poorly protected or unprotected internet-connected RE products and devices.	• High volume product present in many European households. • Issues around securing consent to ensure that consumers' privacy is respected. • The need to consider the interaction between network and device-level vulnerabilities. • The challenge that firmware and software updates are often only updated for a maximum of 3-5 years post product-placement. Whilst such updates are presently outside the scope of the RED's existing essential requirements, they could potentially be covered through possible activation of Art. 3(3)(i).
Smart Watches	• Risks through smart watches come from the range of personal data collected, which increasingly includes health related information but is also expanding into financial transactions. These add to location and other data. • An example of potential risk comes through the European commission warning that the global positioning system (GPS) of Enox Safe-Kid-One, app could be easily hacked, allowing	• Smart watches form a significant element of wearable devices[8]. • The number of wearables devices in the EU are estimated as 21.75million in 2015, 116million in 2017 and forecast to rise to 260million in 2022[9] • Fraud has been defined as the "Intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right".

[8] https://www.statista.com/topics/4762/smartwatches/
[9] https://www.statista.com/statistics/490231/wearable-devices-worldwide-by-region/

Product type	Risks	Justification for selection in longlist
	strangers to track children or conceal the wearer's true location from their parents[6]. • The measures required to increase security can be classed as encryption, security updates, strong passwords, vulnerabilities management and privacy policy[7].	

In Sections 2-7, the five case studies are presented in alphabetical order i.e.

- Product case study 1 – Laptops
- Product case study 2 – Routers (wireless)
- Product case study 3 – Security Cameras (connected) and baby monitors
- Product case study 4 – Smart Toys
- Product case study 5 – Smart TVs
- Product case study 6 – Smart Watches

[6] https://www.theguardian.com/technology/2019/feb/05/eu-recalls-childrens-smartwatch-over-data-fears
[7] https://foundation.mozilla.org/en/privacynotincluded/

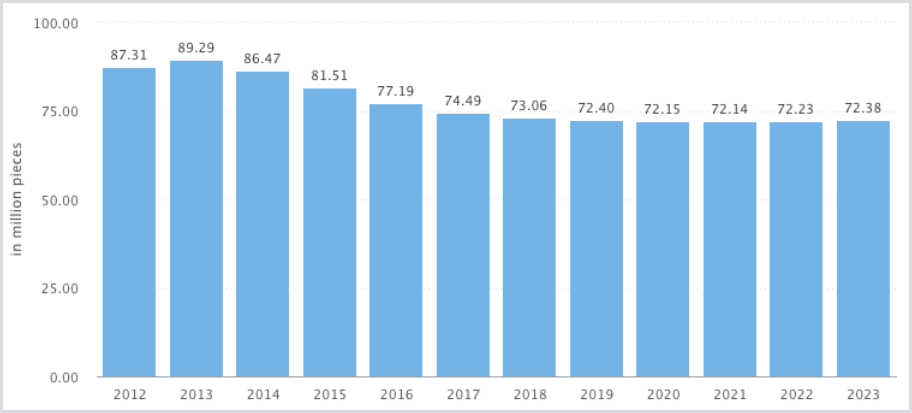
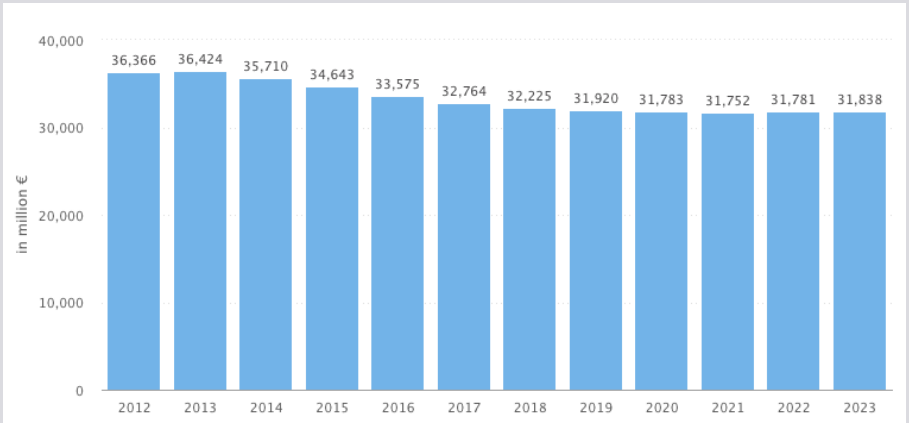
2. Product case study 1 - Laptops

This section sets out the first case study on laptops.

Case study title:	Assessment of security vulnerabilities in laptops
Product group and short definition:	Laptops are electronic devices used by consumers and businesses to store and process data according to a particular set of application programmes. In many cases, laptops are networked (i.e. connected to the internet and other RE devices). Laptops are comprised of a wide variety of hardware and software components.
Rationale for selection of product group:	There are many reasons why laptops make an interesting case. The complexity of their production, the combination of multiple hardware (including cameras and microphones) and software components and their frequent connection to the internet and multiple internet-connected devices via varied means (e.g. WLAN, Bluetooth and more recently LTE). Laptops are also regularly used by a significant proportion of EU citizens to access the internet, use various services and store personal and non-personal data. For instance, Eurostat has found that, in 2014, 78% of EU households access the internet via a desktop or portable computer, rising to 96% when considering only households with internet access.[10] Furthermore, pursuant to workplace policies concerning Bring Your Own Device (BYOD) trend, where employees are allowed to use their own devices (e.g. laptops etc.) in the workplace, including to access privileged company information and applications. This has brought many associated information security, data protection and fraud-related risks to the business environment.[11]
Case study overview and aims	The aims of this case are to: • **Highlight vulnerabilities in laptops**, and to consider the extent to which technical solutions are available to mitigate these vulnerabilities. • Consider the extent to which the vulnerabilities identified are **pervasive within the product group**, or specific to certain models and manufacturers. • **Review available technical solutions** on the market to address vulnerabilities, and the nature of these (e.g. general security by design and default principles, industry-led standards and technical standards developed by standards bodies etc.) • Shed light on the **costs and benefits of strengthening product security**, specifically from a data protection and privacy / protection from fraud perspective. • Consider the implications of having complex international value chains in complex products such as laptops, such as monitoring GDPR compliance when there are multiple data processors globally. The case draws on secondary research and interviews. The research study does not allow scope to test or comment on individual products. Rather, the aim is to identify the main types of vulnerabilities, to categorise the impact of these from a data protection and privacy and protection from fraud perspective.
Number of devices on European	According to data from Statista on the European laptops and tablets segment, there are **72.40 million laptops and tablets in Europe in 2019** (392.38 million globally, 2019).

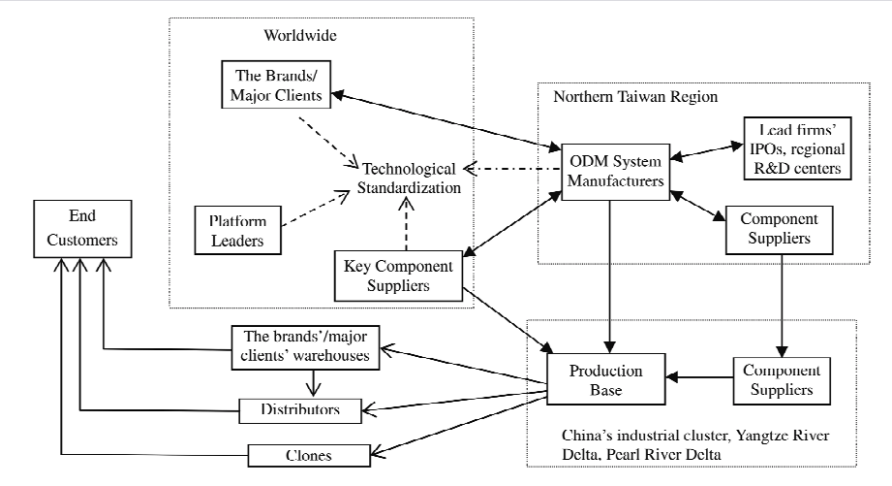
[10] Eurostat, Households – devices to access the internet [isoc_ci_id_h], https://ec.europa.eu/eurostat/web/products-datasets/product?code=isoc_ci_id_h

[11] Fraud Advisory Panel, Bring your own device (BYOD) policies, Fraud Facts, Information for organisations, Issue 23 June 2014, https://www.fraudadvisorypanel.org/wp-content/uploads/2015/04/Fraud-Facts-23B-Bring-Your-Own-Device-Policies-June14.pdf

Case study title:	Assessment of security vulnerabilities in laptops
market and growth rate:	This figure has steadily decreased since a peak of 89.29 million in 2013 (425.19 million globally, 2013) and forecasts predict limited change over the next five years, resulting in 72.38 million laptops and tablets in Europe in 2023 (411.89 million globally, 2023).[12] As such, Europe's share of global laptops and tablets has reduced from 21% (2013) to 18% (2019), where, looking at forecasts for 2023, it is predicted to stay. ***Figure: Number of devices – Laptops & Tablets, Europe, 2012-2023***  ***Source:*** *Statista, August 2019, Volume in million pieces in the European Laptops & Tablets segment* Data on revenue in the European laptops and tablets segment, according to the same data source, has followed and is predicted to continue following a similar pattern. **In 2019, revenues of €31,920 million** were achieved in Europe (€151,697 million globally, 2019), having decreased steadily since a peak of €36,424 million in 2013 (€155,749 million globally, 2013). Limited movement is predicted in the coming five years, with €31,838 in revenue predicted for 2023 (€155,628 million predicted globally, 2023).[13] As such, Europe's share of global revenue in laptops and tablets has reduced from 23% (2013) to 21% (2019). It is forecast to reduce to 20% by 2023. ***Figure: Revenue – Laptops & Tablets, Europe, 2012-2023***  ***Source:*** *Statista, August 2019, Revenue in million € in the European Laptops & Tablets segment*
Mapping of key stakeholders in product group:	Laptop manufacturing comprises a complex and global production network, requiring input from a wide range of stakeholders. The below figure illustrates the relationships

[12] Statista data on Laptops & Tablets segment, Europe: https://www.statista.com/outlook/15030100/102/laptops-tablets/europe?currency=eur

[13] Statista data on Laptops & Tablets segment, Europe: https://www.statista.com/outlook/15030100/102/laptops-tablets/europe?currency=eur

Case study title:	Assessment of security vulnerabilities in laptops
	between different stakeholders within the production network, as well as indicating common geographical associations for parts of the network. • Companies involved in the global laptop production network: ▪ Lead firms / brands (e.g. HP Inc., Dell, Apple, Lenovo, Asus, Acer etc.) ▪ Component and key component suppliers, e.g. – Central processing units (CPUs) – Intel, AMD – Hard disk drives (HDDs) – Seagate, Toshiba, Western Digital – Motherboards – ASRock, Asus, Biostar etc. – Etc. ▪ Original design manufacturers (ODMs) (e.g. Quanta, Compal, Wistron, Inventec etc.) • Industry Associations representing interests of computer manufacturers  ***Source:*** *Yang and Chen (2013)[14], adapted from Yang and Coe (2009)[15]* Beyond industry, relevant stakeholders include: data protection and privacy NGOs and civil society organisations; consumer associations; and international standardisation organisations.
Type of data being collected (e.g. personal data and non-personal data) **How transmitted to manufacturer, technology provider or service provider *(e.g. which type of connected network, internet, other***	Significant personal and non-personal data are collected, stored or processed by laptops, including by the operating system (OS) and many applications installed on the laptop or accessed via the internet. For example, Microsoft's Windows 10 OS essentially offers three levels of diagnostic data collection: • **Basic level** "gathers a limited set of information that is critical for understanding the device and its configuration including: basic device information, quality-related information, app compatibility and Microsoft Store."[16] It also gathers information on the security settings of the computer. • **Enhanced level** builds on the basic level by providing 'Windows Analytics Device Health' reports, which include crash reports and further OS diagnostic data events.[17]

[14] Yang, D.Y-R. and Chen, Y-C., The ODM Model and Co-Evolution in the Global Notebook PC Industry: Evidence from Taiwan, February 2013. https://pdfs.semanticscholar.org/89e5/73a785c2d917f9c89aa92ff75a6bfc2b9a02.pdf

[15] Yang, D.Y-R. and Coe, N., The Governance of Global Production Networks and Regional Development: A Case Study of Taiwanese PC Production Networks, February 2009. https://onlinelibrary.wiley.com/doi/full/10.1111/j.1468-2257.2008.00460.x

[16] Microsoft, Windows 10, version 1903 basic level Windows diagnostic events and fields, 23/04/2019. Last accessed on 21.11.2019 at: https://docs.microsoft.com/en-gb/windows/privacy/basic-level-windows-diagnostic-events-and-fields-1903

[17] Microsoft, Windows 10 enhanced diagnostic data events and fields used by Windows Analytics, 09/11/2018. Last accessed on 21.11.2019 at: https://docs.microsoft.com/en-gb/windows/privacy/enhanced-diagnostic-data-windows-analytics-events-and-fields

Case study title:	Assessment of security vulnerabilities in laptops
secure communications system)	• **Full level** comprises all diagnostic data "to keep Windows secure and up-to-date, troubleshoot problems and make product improvements"[18], including the option to have tailored experiences provided (e.g. personalised tips, ads and recommendations). These data include information on device characteristics, connectivity and configuration, product and service usage and performance data and data on browsing history. Furthermore, data collected by individual RE products may be transferred via the laptop. These data could include any data collected by RE products, for example activity data from wearables. In addition, users store significant amounts of personal and non-personal, commercial and private data on their laptops (e.g. this could include a company's financial data or an individual's private photos or videos etc.)
Security vulnerabilities in laptops ***(differentiate between latest generation products and older products on market)***	Given the complexity inherent in the production and operation of laptops, as well as their extensive connectivity potential, laptops face a significant range of potential hardware and software security vulnerabilities. These can include **technical, human and operational vulnerabilities**, including poor or default password selection, default security configurations and limited security engagement by users, and users not updating firmware and/or software potentially leaving technical vulnerabilities available for exploitation by attackers. This is without noting the network vulnerabilities related to the connectivity of laptops to the internet and other RE devices via WLAN, Bluetooth and, more recently, LTE. More specifically, from an information security perspective the following threats exist: • Related to **hardware**, the following threats are relevant: ▪ Theft of hardware ▪ Copying (disk imaging) of the hardware ▪ Malicious / accidental damage of the hardware ▪ Hardware failure • Considering **software**, the following general threat types exist: ▪ Theft of software ▪ Illegal copying of software ▪ Malicious / accidental deletion of software ▪ Malicious alteration of software ▪ Unauthorised running of software ▪ Running of unauthorised software ▪ Faulty software ▪ Unavailability of software • Related specifically to **data**, the following general threat types exist: ▪ Data theft ▪ Malicious / accidental deletion of data ▪ Corruption of data ▪ Unauthorised access to data ▪ Unauthorised modification of data ▪ Unavailability of data From the above, it is worth noting that hardware threats are often the least probable threats to be realised, as compared with software and data threats, and also the easiest to safeguard against.

[18] Microsoft, Windows 10, version 1709 and newer diagnostic data for the Full level, 15/04/2019. Last accessed on 21.11.2019 at: https://docs.microsoft.com/en-gb/windows/privacy/windows-diagnostic-data#device-connectivity-and-configuration-data

Case study title:	Assessment of security vulnerabilities in laptops
	These threats can be realised through the exploitation of a wide range of vulnerabilities, the most common of which include: • **Poor physical protection mechanisms**, for example leading to hardware theft or access to exploit other vulnerabilities and enact other threats; • **Poor (or no) password protection**, as evidenced by regular publications of the most common passwords, including 'qwerty', 'password' and '111111'. In addition, poor password policies exist that, for example, do not require complex enough passwords, have no periodic obligation to change passwords or do not reject the use of repeat passwords, implement no limit in password guess attempts, have limited restrictions on user types that can conduct password recovery; • **Use of default or poor security configurations**, in particular in relation to encryption of data, both in storage and in transit, user access controls and authentication; • Common technical software vulnerabilities, as listed by the US-government sponsored Common Weakness Enumeration community[19], including **memory safety violations**, such as buffer overflows[20], **input validation errors**, such as cross-site scripting[21], **privilege-related errors**, such as improper privilege management[22].
Nature and extent of threat, likelihood and impacts of security vulnerabilities occurring	Contained within the above box
Extent to which covered by existing legislation	In relation to the collection and processing of personal data, as well as protection against fraud, within the context described in this case study, there is significant coverage provided by the General Data Protection Regulation (GDPR). More specifically, the GDPR includes significant requirements on data controllers and processors (i.e. the legal entities collecting and processing the personal data) to ensure the protection of personal data. Key requirements include: • Respecting the principles relating to the processing of personal data - which include that personal data shall be processed in a manner that ensures appropriate security of the personal data using appropriate technical or organisational measures – and demonstrating compliance with the principles (Art. 5). • Only process data in line with one of the legal bases for processing (Art. 6), which include consent. Within the GDPR, data subjects are also provided a range of rights (see Chapter III, GDPR), to be respected by data controllers and processors, which include the requirement for data controllers to provide any information related to processing in a concise, transparent, intelligible and easily accessible form. As such, the GDPR stipulates comprehensive requirements to be met by data controllers for the protection of personal data. However, given the GDPR has only been in force since May 2018, no evaluation has been conducted and the effectiveness of the legislative mechanisms employed are as of yet unknown. In terms of enforcement, it is clear that some action is being taken, as evidenced by the fines and notices levied by Data Protection Authorities (DPA) across a number of

[19] https://cwe.mitre.org/about/index.html
[20] https://cwe.mitre.org/data/definitions/119.html
[21] https://cwe.mitre.org/data/definitions/79.html
[22] https://cwe.mitre.org/data/definitions/269.html

Case study title:	Assessment of security vulnerabilities in laptops
	Member States specifically for the implementation of insufficient information security practices by companies (although these cases do not have a laptop-specific focus). Specific examples of such fines include: • The €180,000 fine issued against Active Assurances by the French Commission Nationale de l'Informatique et des Libertés (CNIL) for the implementation of insufficient security measures to protect the personal data of users.[23] • The ca. €645,000 fine issued against Morele.net by the Polish DPA, Urząd Ochrony Danych Osobowych (UODO). The fine was imposed due to a lack of appropriate technical and organisational measures that led to the leakage of personal data, including personal ID numbers (PESEL number), and possible high risk of adverse effects.[24] Considering protection against fraud, the GDPR details in its recitals that fraud is a key potential impact of a personal data breach (Recitals 75 and 85) and that, in relation to the rules for notification of a personal data breach, fraud needs to be considered when assessing the implementation of appropriate technical protection measures (Recital 88).
Stakeholder views on the nature and extent of security vulnerabilities:	Interviews have been conducted with two laptop large, global laptop vendors and an industry association representing manufacturers of laptops. In addition to providing factual information that has informed the responses to the other sections of this case study, the interviewees provided their perceptions on a range of key topics, primarily including: the costs that would associated with the adoption of delegated acts on data protection and privacy and protection against fraud; and the challenges facing the RED and the inclusion of cybersecurity requirements. From the interviews, it is clear that **laptop vendors place significant value on the clarity of the legal situation**. Although they noted that the approach under the New Legislative Framework (NLF) can work (for example in relation to the Electromagnetic Compatibility Directive), they stated concerns that the RED is not presently functioning particularly efficiently. More specifically, the vendors perceive that the difficulties in finalising standards developed and proposed by the European Standardisation Organisations (ESO) was undermining the legislative framework. In particular, this resulted in the need to use third party certification and testing bodies Furthermore, the vendors interviewed highlighted market surveillance challenges, including: that Market Surveillance Authorities (MSAs) lack expertise in cybersecurity; that heterogeneous market surveillance practices exist across the Member States; and, as highlighted below, limited information sharing exists between Member State MSAs which results in the duplication of information requests to vendors. It was therefore noted that developing additional requirements could exacerbate existing challenges. Considering the potential delegated acts themselves, the vendors and the industry association noted that the lack of detail on what the delegated acts may contain prevented the provision of any real feedback on the impacts and costs associated to compliance.

[23] CNIL, Active Assurances: Sanction de 180 000 euros pour atteinte à la sécurité des données des clients, 25.07.2019. Last accessed on 21.11.2019 at: https://www.cnil.fr/fr/active-assurances-sanction-de-180-000-euros-pour-atteinte-la-securite-des-donnees-des-clients

[24] European Data Protection Board (EDPB), Polish DPA imposes €645,000 fine for insufficient organisational and technical safeguards, 20.09.2019. Last accessed on 21.11.2019 at: https://edpb.europa.eu/news/national-news/2019/polish-dpa-imposes-eu645000-fine-insufficient-organisational-and-technical_en

Case study title:	Assessment of security vulnerabilities in laptops
	With that said, however, the vendors did outline a range of **anticipated costs**, based on the mechanisms for compliance with other RED and NLF requirements. Primarily, these costs may include: • Hiring additional experts to assess the requirements and lead compliance activities, including compiling documentation (e.g. technical files and Declaration of Conformity), any necessary product redesign and responding to requests from national MSAs; • Additional testing and certification by third parties; and • Engagement with third party suppliers, given the complexity of the laptop production process. It was also noted that, as it will be a new area of certification, testing and certification bodies may also lack expertise in cybersecurity. As such, they will be required to bear additional costs related to obtaining this expertise, which will likely be passed on to the vendors. However, with that said, the vendors both noted that they already approach cybersecurity as a market requirement, investing significantly in cybersecurity measures and ensuring it is a key focus within their production processes. As such, they do not anticipate, based on current assumptions, that the adoption of the delegated acts would require significant alterations to product design. An additional concern, noted by one vendor, was that, depending on the specific requirements, the inclusion of additional cybersecurity measures on low-cost devices may require price increases, which could reduce accessibility to this technology for some consumer groups.

Technical solutions:	*Comment on which technical solutions are available to address identified vulnerabilities. How have these been developed e.g. role of industry grouping working on standards, standards organisations, etc. Add a comment on whether solutions are sufficient to address security concerns.*
	
	A wide range of techniques and technical tools are used to prevent, protect, and detect against exploitation of the vulnerabilities highlighted above. From an information security perspective, these controls include:
	
	• **Network security.** This category deals with controls used to secure the interaction of a laptop with the internet and other RE devices, including firewalls, intrusion detection systems, use of encryption technologies, digital signatures, access control mechanisms between networked devices, authentication exchanges, traffic padding, routing control and notarisation.
	  ▪ There are extensive technical standards produced by ISO/IEC on information and network security controls, including: ISO 7498-2, which defines standard security terminology and standard descriptions for security services and mechanisms.
	  ▪ These standards are often developed in collaboration with prominent industry groups, such as the US-based Trusted Computing Group, which has Microsoft, Cisco, Intel, Dell, HP and many more prominent companies as contributors.
	  ▪ In addition, there are a range of globally accepted security protocols in place to secure connections between connected devices, including: Transport Layer Security (TLS); Secure Sockets Layer (SSL); Hypertext Transfer Protocol Secure (HTTPS); and the 802.11 standard for wireless networking.
	• **Managing identities and rights**, including establishing privileges, logon controls (e.g. password policy) and file access controls (e.g. on the Windows OS through access control lists);

Case study title:	Assessment of security vulnerabilities in laptops
	• **Security auditing** requires the OS to maintain logs of activity, such that the data can be analysed pre-emptively (to detect suspicious behaviour on the computer/network) or following an attack; and • **Physical security** measures, including locks and other physical controls, equipment tamper-proofing. Furthermore, common vulnerabilities are monitored and documented, including through the Common Vulnerabilities and Exposure (CVE) database, which is sponsored by the US Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and maintained by collaboration between technology and cybersecurity organisations (e.g. Lenovo, Cisco, MITRE, Trend Micro, Panasonic etc.), research institutions, government departments, academics and other security experts. In relation to privacy and data protection, specifically, larger firms involved in computing, such as Apple and Microsoft, have been taking steps to provide control to users over their personal data and the data collected and processed about them. The measures reviewed focus on the personal data collected from the wide-variety of applications provided by the firms. For example, Microsoft's privacy dashboard allows users to manage browser data, location data, data collected by Cortana (Microsoft's personal digital assistant) and more.[25] Apple, in a similar fashion, have implemented a range of measures to preserve user privacy across its range of applications, including Intelligent Tracking Prevention in the Safari web browser, not linking location to a user's Apple ID, and their use of end-to-end encryption on iMessage.[26]
Costs and benefits of addressing security vulnerabilities:	There are two aspects that are to be examined in relation to the costs and benefits of addressing security vulnerabilities. Firstly, it is important to understand the costs associated with security vulnerabilities and, in particular, when those vulnerabilities lead to the realisation of data protection / privacy and fraud risks. Secondly, it is important to understand what costs and benefits would arise from the activation of Delegated Acts on: i) data protection / privacy; and ii) protection from fraud. Considering the first point, research has been conducted in relation to the costs of security breaches to businesses. For instance, the UK Cyber Security Breaches Survey identified the average cost of a cyber breach or attack against an organisation was £4,180 in 2019, rising from £2,450 in 2017.[27] However, compared with research in the US, such as the IBM / Pokemon Institute [28]annual updating exercise on the costs of data breaches, this appears to be an under-estimate. In addition, the UK Home Office found that cyber-crime in the UK cost £1.1bn to individuals, although this estimate does not include any costs related to responding to cyber-crime (e.g. police and victim services etc.) and this analysis was not able to estimate the costs of cyber-crime to businesses.[29] As such, it is clear that there are many limitations restricting the accurate and precise measurement of the costs of cyber breaches, including challenges related to capturing indirect, long-term and intangible costs such as reputational damage. It is also worth noting that these data are not specific to this product group.

[25] https://account.microsoft.com/account/privacy?refd=privacy.microsoft.com&destrt=privacy-dashboard
[26] https://www.apple.com/fr/privacy/
[27] UK Government, Department for Digital, Culture, Media & Sport (DCMS), Cyber Security Breaches Survey 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf
[28] https://www.ibm.com/security/data-breach
[29] UK Home Office, The economic and social costs of crime: Second edition, Research Report 99, July 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/732110/the-economic-and-social-costs-of-crime-horr99.pdf

Case study title:	Assessment of security vulnerabilities in laptops
	Considering the second point – i.e. the anticipated costs and benefits related to the activation of the two Delegated Acts under examination – it is hypothesised that, given the GDPR's coverage in relation to the collection and processing of personal data and the onus already placed on security by vendors, limited additional measures would need to be taken by manufacturers (at least for those already correctly implementing the GDPR). The following additional costs will likely be incurred, dependent on the specific requirements adopted: • Hiring additional experts to assess the requirements and lead compliance activities, including compiling documentation (e.g. technical files and Declaration of Conformity), any necessary product redesign and responding to requests from national MSAs; • Additional testing and certification by third parties; Engagement with third party suppliers, given the complexity of the laptop production process and the international nature of the value chain.
Overall findings and lessons learned:	• Significant usage by the EU and global population, as evidenced by the number of devices in the European market and the proportion of EU households that access the internet through their laptop or desktop computer. • Complex global production network with non-EU players holding key positions. • Complex security situation, given the role of laptops as a hub of connectivity to the internet and other devices, as well as the storage of substantial amounts of personal and non-personal data. This is supported by the varied means by which laptops can connect to other RE devices, including WLAN, Bluetooth and LTE. • Emerging trends, such as BYOD, are expanding the cyber-attack surface for businesses. • In terms of data collection, as evidenced by the information on Microsoft's Windows 10 OS, there are various levels of diagnostic data that are shared by the laptop with the manufacturer. In full mode, these data can include data on browsing history. Furthermore, users store significant amounts of data on their laptops. • A wide range of technical, human and operational vulnerabilities exist that can provide a means by which an attack can be successful. These threats can relate to the hardware, software or the data held by the machine, although hardware threats are often the least probable and easiest to safeguard against. • GDPR contains extensive provisions for the protection of personal data by data controllers and data processors. These include: respecting key principles (detailed in Art 5), including ensuring the security of the personal data using appropriate technical or organisational measures; specifying a limited number of legal bases under which personal data can be collected and processed; and stipulating a range of rights for data subjects that must be respected by data controllers. • However, given the recency of its implementation, the effectiveness of the GDPR is not known. With that said, it is clear that enforcement efforts are being made, in particular in relation to data controllers not appropriately securing personal data. • A wide range of technical solutions are available to ensure the protection of the laptop environment and to prevent and detect cyber-attacks. In terms of privacy and data protection, it seems that larger firms have taken steps, since GDPR, to ensure users have control over the use of their personal data, at least on their applications. • Although costs related to product redesign may not be significant for this product group, there will still be a range of additional costs incurred by manufacturers as a result of the adoption of the delegated acts, depending on the specific detail of the requirements.

Case study title:	Assessment of security vulnerabilities in laptops

Literature consulted:

- Apple Privacy Measures, https://www.apple.com/fr/privacy/
- CNIL, Active Assurances: Sanction de 180 000 euros pour atteinte à la sécurité des données des clients, 25.07.2019: https://www.cnil.fr/fr/active-assurances-sanction-de-180-000-euros-pour-atteinte-la-securite-des-donnees-des-clients
- European Data Protection Board (EDPB), Polish DPA imposes €645,000 fine for insufficient organisational and technical safeguards, 20.09.2019: https://edpb.europa.eu/news/national-news/2019/polish-dpa-imposes-eu645000-fine-insufficient-organisational-and-technical_en
- Eurostat, Households – devices to access the internet [isoc_ci_id_h], https://ec.europa.eu/eurostat/web/products-datasets/product?code=isoc_ci_id_h
- Fraud Advisory Panel, Bring your own device (BYOD) policies, Fraud Facts, Information for organisations, Issue 23 June 2014, https://www.fraudadvisorypanel.org/wp-content/uploads/2015/04/Fraud-Facts-23B-Bring-Your-Own-Device-Policies-June14.pdf
- ICO, Intention to fine British Airways £183.39m under GDPR for data breach, 08.07.2019: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/
- Microsoft Privacy Dashboard, https://account.microsoft.com/account/privacy?refd=privacy.microsoft.com&destrt=privacy-dashboard
- Microsoft Windows diagnostics data collection:
  - Enhanced diagnostic data events and fields used by Windows Analytics, 09/11/2018: https://docs.microsoft.com/en-gb/windows/privacy/enhanced-diagnostic-data-windows-analytics-events-and-fields
  - Windows 10, version 1709 and newer diagnostic data for the Full level, 15/04/2019: https://docs.microsoft.com/en-gb/windows/privacy/windows-diagnostic-data#device-connectivity-and-configuration-data
  - Windows 10, version 1903 basic level Windows diagnostic events and fields, 23/04/2019: https://docs.microsoft.com/en-gb/windows/privacy/basic-level-windows-diagnostic-events-and-fields-1903
- Statista data on Laptops & Tablets segment, Europe: https://www.statista.com/outlook/15030100/102/laptops-tablets/europe?currency=eur
- UK Government, Department for Digital, Culture, Media & Sport (DCMS), Cyber Security Breaches Survey 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf
- UK Home Office, The economic and social costs of crime: Second edition, Research Report 99, July 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/732110/the-economic-and-social-costs-of-crime-horr99.pdf
- Yang, D.Y-R. and Chen, Y-C., The ODM Model and Co-Evolution in the Global Notebook PC Industry: Evidence from Taiwan, February 2013. https://pdfs.semanticscholar.org/89e5/73a785c2d917f9c89aa92ff75a6bfc2b9a02.pdf
- Yang, D.Y-R. and Coe, N., The Governance of Global Production Networks and Regional Development: A Case Study of Taiwanese PC Production Networks, February 2009. https://onlinelibrary.wiley.com/doi/full/10.1111/j.1468-2257.2008.00460.x

Interviews (planned):

- Government affairs representative and technical expert, top 5 global laptop manufacturer (**w/c 9th December**)
- Government affairs representative, top 5 global laptop manufacturer (**w/c 9th December**)
- Public policy manager, global tech advisory industry association, focusing specifically on computers (**scheduled 3rd December**)

3. Product case study 2 - Routers

The case study on wireless routers is presented in the table below.

Case study title:	Assessment of security vulnerabilities in wireless routers.
Product group and short definition:	Routers are a piece of network hardware that connects a local network to the internet.
Rationale for selection of product group:	Routers are an interesting product group, as they are both a connected radio equipment (RE) device in their own right, but also serve as the gateway to connecting other RE (especially IoT devices) across networks both in a home and office setting. Moreover, routers are an exceptionally common product in the household. A further justification for looking at routers as a product group is that some previous studies have identified them as being a product where some security vulnerabilities have been identified, of differing levels of severity. This case study also considers the distinction between consumer and enterprise-grade routers, as many of the vulnerabilities identified in academic and grey literature relates to consumer-grade routers.
Case study overview and aims	The aims of this case are to: • Highlight vulnerabilities in routers, and to consider the extent to which technical solutions are available to mitigate these. • Consider the extent to which the vulnerabilities identified are pervasive within the product group, or specific to certain models and manufacturers. • Review available technical solutions on the market to address vulnerabilities, and the nature of these e.g. general security by design and default principles, industry-led standards and technical standards developed by standards bodies etc. • Shed light on the costs and benefits of strengthening product security, specifically from a data protection and privacy / protection from fraud perspective. • Review the extent to which a differentiation can be made between the level of risks associated with consumer and enterprise-grade routers. The case study draws on a combination of secondary research and three interviews with six stakeholders. It should be noted that the research study does not allow scope to test or comment on individual products. Rather, the aim is to identify the main types of vulnerabilities, to categorise the impact of these from a data protection and privacy and protection from fraud perspective.
Number of devices on European market and growth rate:	It is anticipated that there will be positive growth in the router market in future years, as there are a growing number of home networks using Wi-Fi and WLAN technologies that rely on routers embedding these technologies. For instance, a report on The Global Wireless Router Market by BlueWeave Consulting notes that the global market is expected to grow significantly during the period 2019-2025 *"due to factors such as the demand for faster internet, increase in the range of wireless networks, and the number of connected devices"*[30]. However, the launch of 5G networks which will bypass the need for Wi-Fi networks means there is some uncertainty around the number of devices on the market globally. Tech4i2 have also developed market forecasts.

[30] Global Wireless Router Market, By Standard (802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax), By Band (Single Band, Dual Band, and Others), By Application (Residential, Commercial, Industrial), By Region (North America, Europe, Asia Pacific, Latin America, Middle East & Africa), Market Trend Analysis, Competitive Analysis, Size And Forecast, 2015-2025 https://www.wiseguyreports.com/reports/4158687-global-wireless-router-market-by-standard-802-11b

Case study title:	Assessment of security vulnerabilities in wireless routers.
Mapping of key stakeholders in product group:	• Wireless router manufacturers, distributors/traders/wholesalers • Wireless router Subcomponent Manufacturers • Industry Associations representing interests of wireless routers Examples of the major manufacturers in the global wireless router market are AVG, CISCO, D-Link, Linksys, TP-Link Technologies Co, Huawei Technologies Co. Limited, Edimax Technology Co, Tenda, NETGEAR, ASUS, Huawei, Qihoo 360, Gee, Xiaomi Limited, among many others.
Type of data being collected (e.g. personal data and non-personal data) **How transmitted to manufacturer, technology provider or service provider *(e.g. which type of connected network, internet, other secure communications system)***	Regarding the type of data being collected by the router and reported back to the manufacturer, this will include: information regarding the router's running status, the number of devices connected to the router, the types of connections, LAN/WAN status, Wi-Fi bands and channels, IP address, MAC address, serial number, and technical data about the functioning and use of the router and its Wi-Fi network. However, the router may also provide access into a home or office network which could include personal data being transmitted via individual connected RE products are connected to the network via the router. There are therefore implications in terms of data protection and privacy, as well as considerations relating to protection from fraud if the device is not secure. Although routers do not collect personal information in relation to router analytics data, if hacked, they would potentially transmit personal data from other IoT devices, for example, if a home network were to be penetrated by a hacker.
Security vulnerabilities in wireless routers	Among the security vulnerabilities linked to routers are that (a) they are normally left switched on permanently (b) their firmware is not commonly updated that frequently and (c) many consumers leave the devices with the credentials unchanged from the factory setting. Moreover, although they may not collect extensive personal data themselves, rather data relating to the functionality and performance of the router, if an attacker were to obtain administrative access to a home router, then they could potentially gain access to every device connected to it. A number of different security vulnerabilities have been identified in wireless routers through desk research. Examples are: • **Lack of secure credentials.** Many consumers plug in new routers but either don't set up a new password, and continue to use the password on the back of the router making the device susceptible to hacking. Indeed, there have been examples of fraud committed by call centres in India based on retaining the credentials on the back of a router to gain access to the home network. Although default user names and passwords are not used, if the wireless key and other user credentials on the bottom or back of the device are known to third parties, this is a major security vulnerability as home users rarely change their credentials. A further problem is that even when users do change their router's initial log in and password details, they may use a weak password. **Hardware and operating systems** • **Basic design flaws** – having **no Logoff button**, even among major manufacturers. This may make routers more vulnerable to attack, and if penetrated, this could lead to data theft from devices connected to the router. • **Router secure boot flaw – e.g.** a major global router manufacturer identified security weaknesses in network routers, switches and firewalls that could be exploited by hackers to hide spyware inside compromised equipment. • **Flaws in web-based user interfaces of routers** that can be exploited by a logged-in administrator to execute commands as root on the underlying Linux-

Case study title:	Assessment of security vulnerabilities in wireless routers.
	based shell. If an administrator gains root access, they can hide "backdoor" or network surveillance tools in the device's operating system, which could change the bitstream in the firmware to allow malicious code to boot, and block any further attempts to change the bitstream. • **Risk of TCP injection attacks against major operating systems (macOS, Windows, and Linux).** The attack requires a device to be connected to the Internet via a wireless router, and can be reachable from an attack server (e.g. indirectly so by accessing to a malicious website)[31]. TCP injection attacks may stem from router software vulnerabilities. These can however be eliminated via software updates. • **WPS (Wi-Fi Protected Setup) and WPA,** a technology designed to automate the initial setup of Wi-Fi connections was found to have a number of security vulnerabilities[32]. WPS works only for wireless networks that use a password that is encrypted with the WPA Personal or WPA2 Personal security protocols. Such vulnerabilities are not specific to routers, but apply to any device using such Wi-Fi standards to enable Internet connections for devices. • **DNS hijacking campaign** targeting home routers, often older routers, not still in production. Usually a DNS is connected to the ISP. An attacker may hijack a users' settings and redirect them to malicious internet sites. Therefore, DNS hijacking can used for phishing attacks, when the domain name of the targeted site is redirected by the rogue DNS server to a web server controlled by a hacker. **Software and firmware** • **Corruption of application firmware,** such as memory corruption issues, leading to vulnerabilities. **For** example, malformed Wi-Fi packets may be sent to any device WiFi chipset and then when the function launches, this could execute malicious code and take over the device. **Risk of unauthorised third-party obtaining remote root-level access.** In older routers, there is a greater risk of unauthorised access, even without a password, for instance if firmware/ software has not been updated by manufacturers. **Networking and wireless internet protocols** • **Routers with WEP security are seen as being easy to hack.** WEP is a type of encryption tool used to secure wireless connections. However, routers are increasingly secured with WPA-PSK keys. WPA2 and the new WPA3 encryption protocol feature improved security, however vulnerabilities have nevertheless recently been identified. • **Design flaw issues relating to IEEE 802.11 protocols[33].** It may not be possible to eliminate the side channel without substantial changes to the specifications. • **Network intrusion vulnerabilities.** • **An attack via unauthorized internet access to your router** is the least likely to occur. All routers use Network Address Translation (NAT) to filter out unauthorised incoming traffic. The only exception is if the user has purposefully enabled port forwarding or created a demilitarized zone. This would usually only occur to allow access to programmes such as BitTorrent clients or high-bandwidth online video games.

[31] Off-Path TCP Exploit: How Wireless Routers Can Jeopardize Your Secrets, 2018. Authors - Weiteng Chen and Zhiyun Qian, University of California, Riverside www.usenix.org/node/217606
[32] https://routersecurity.org/checklist.php
[33] IEEE 802.11 is part of the IEEE 802 set of LAN protocols, and specifies the set of media access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN);

Case study title:	Assessment of security vulnerabilities in wireless routers.
	Attacks via remote access to routers. A router's administration page may be accessible via the wide area network or the internet. This is instead of accessing the router's configuration page by connecting to it directly via a wired or wireless connection. Consumer-grade routers have been identified as having particular security vulnerabilities, especially routers that have been on the market for some time. This is recognised as a global problem. *"The issue of router vulnerability has become such that the FBI in the US issued a public service announcement when the VPNFilter attack occurred "*[34]. Enterprise-grade routers were found to be less vulnerable generally. Regarding examples of serious scale hacking attempts, in 2018, the **VPNFilter malware** targeted consumer internet routers from a range of vendors[35]. "Stage 1 utilises multiple redundant command and control (C2) mechanisms to discover the IP address of the current stage 2 deployment server, making this malware extremely robust and capable of dealing with unpredictable C2 infrastructure changes," the researchers wrote. The stage 2 malware possesses capabilities such as file collection, command execution, data exfiltration, and device management; however, the researchers said some versions of stage 2 also possess a self-destruct capability that overwrites a critical portion of the device's firmware and reboots the device, rendering it unusable. An assessment was undertaken as to the extent to which there are security vulnerabilities associated with routers. Some interviewees pointed to considerable challenges in ensuring security in consumer routers, at least at the lower price points. A differentiation can also be made in respect of the level of security between the latest generation of wireless router products and older products on the market due to the evolution in the level of security in wireless internet protocols themselves. Although the RED's scope is the period leading up to product placement, it is important to identify vulnerabilities and risks post-product placement. If an older router is taken over with malicious intent, hackers could gain access to a network of IoT devices and use these to gain access to personal data or to commit fraud. Examples of specific weaknesses in security post product placement are: • **Non-updating of software and / or firmware in older routers that have been on the market for some time.** Manufacturers sometimes discontinue the provision of updates. This means that there are risks of the router providing a conduit to IoT devices and other connected RE in the rest of the home or office network. • **Older End of Life (EoL) devices** that may no longer be sold but are still on the market and used by consumers often don't receive investment from manufacturers once placed on the market to fix performance and security-related bugs, even if vulnerabilities have been identified. It should be noted that the examples presented are based on examples from the past 5 years identified through desk research. The intention however is not to adopt a "name and shame" approach highlighting particular brands, but rather to identify examples of common vulnerabilities and late in the case study, potential technical solutions.
Nature and extent of threat, likelihood and impacts of	Research[36] undertaken in 2019 by Independent Security Evaluators (ISE) investigated how far security improvements have been made to identified vulnerabilities in routers. The researchers identified 125 vulnerabilities in 13 IoT devices, which they suggested "reaffirms an industrywide problem of a lack of basic security diligence". It was found

[34] Threat Bulletin - Home Router, January 2019, Allot
[35] https://www.zdnet.com/article/talos-finds-new-vpnfilter-malware-hitting-500k-iot-devices-mostly-in-ukraine/
[36] Source: https://www.helpnetsecurity.com/2019/09/17/vulnerabilities-iot-devices/

Case study title:	Assessment of security vulnerabilities in wireless routers.
security vulnerabilities occurring	that in nearly all the devices (12 of the 13), ISE "achieved its goal of obtaining remote root-level access". The same study identified the main vulnerabilities as being: (1) buffer overflow, (2) cross-site scripting, (3) command injection, (4) SQL injection, (5) authentication bypass, (6) authorisation bypass, (7) cross-site request forgery and file upload path traversal. Of the 13 router products tested, cross-site scripting (11/13 products), command injection (11/13), and file upload path traversal (7/13) had the most frequent problems. However, other products also had vulnerabilities such as authentication bypass (6/13), and authorisation bypass (5/13). In a recent report from the Netherlands[37], routers were one of seven product groups tested to identify whether there were any security vulnerabilities. Where identified, these were then assessed and categorised depending on whether the security vulnerabilities were minor, major or critical. Taking one example of a particular router model tested, this was identified as having a standard set of security measures in place by default, such as the standard Wi-Fi settings including WPA2-PSK. All connections to external cloud resources were found to be initiated using TLS, a further security measure. However, DNS is used to resolve conflicting IP addresses, which suggests that the device may be vulnerable to DNS attacks. Some examples of basic security risks were identified. For example, the initial wireless password configuration of the device accepted a default password, and this is completed automatically by default. This was identified as a medium level of risk, but with a high probability of the risk occurring. However, interviewees from a European router manufacturer stated that the scale of the problem is less severe than it was 5-10 years ago when insecure, cheap routers were more of a problem. Cloud-based systems have improved their security. Most products in Europe go through service provider and not sold in retail product. Given by a network operator to the end user by the network provider providing the service. Price difference between the cheap ones and good routers is not that significant e.g. 60 EUR and 120 EUR for a cybersecure one. Big brands take the market – self-regulating through consumer purchasing behaviours in certain products. Unnamed cheap products are not a problem.
Relevance of existing legislation to product group	Routers collect data and information relating to the product's basic functionality. Therefore, the risks associated with routers are more associated with security vulnerabilities generally that could compromise data protection and privacy in relation to other RE connected devices/ products that connect to the internet via the router. Routers as a product group are not covered by any specific legislation pertaining to their security. Routers do not generally collect personal data, other than when the product is first used if the product is registered via a browser. Wherever routers do collect any personal data / information, data collection and processing, they are subject to the GDPR requirements including data protection by design and default.
Stakeholder views on the nature and extent of security vulnerabilities:	There were differing views even among manufacturers as to the extent to which there are security vulnerabilities in wireless routers, and the impacts of these in respect of the risk of device penetration and data breaches. A major global manufacturer of enterprise grade routers pointed out that there are considerable challenges associated with consumer routers in terms of ongoing security vulnerabilities for cheaper products on the market, whose level of security leaves

[37] Strict Report on IoT Device Security, 2019 (Onderzoek veiligheid apparaten). Report on behalf of the Radiocommunications Agency Netherlands.

Case study title:	Assessment of security vulnerabilities in wireless routers.

deficiencies. However, not all stakeholders agreed with this assessment. A manufacturer of consumer routers interviewed mentioned that the vast majority of routers sold on the European market are provided to the final consumer either by their ISP or network operator rather than sold directly through retail outlets or online. As ISPs and network operators do not want to run the reputational risk of providing their customers with an unsecure product, they provide secure routers to customers and test the products to quite demanding standards, examining both their overall performance and security functionality. Therefore, there are low sales in most European countries of cheaper router products and low instances of device penetration.

Moreover, the manufacturer of consumer routers pointed out that many of the vulnerabilities identified are theoretical only and relate to bugs that can be addressed by improving the software coding or by taking other security measures before these affect consumers directly. Evidence was also provided that despite the risks, the actual incidence of router-related security incidents leading to device penetration and / or data theft is actually quite low. From 2015 to 2019, for example, according to statistics from the German Federal Office for Information Security, there were very few incidents involving routers. The disaggregated statistics by product[38] show that PCs / laptops accounted for 46% of incidents, Smart Phones: 36%, Miscellaneous: 20% and Routers: 1.3% of incidents in 2015-19.

Nonetheless, the large global manufacturer of enterprise routers acknowledged that whilst routers themselves do not collect much personal data, there is a risk that once a router has been compromised or penetrated, it could serve as an access point into a home network, and a means of accessing personal data via any unsecured connected consumer IoT devices.

The researchers into security vulnerabilities in routers found that many vulnerabilities linked to routers stemmed from weaknesses in Wi-Fi standards themselves, although the degree of cybersecurity to protect personal data and to prevent data breaches has been improved over successive generations of development of Wi-Fi standards. An overview of their evolution over time is provided in the following Figure:

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
Year Released	1999	1999	2003	2009	2014	2019
Frequency	5Ghz	2.4GHz	2.4GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz
Maximum Data Rate	54Mbps	11Mbps	54Mbps	600Mbps	1.3Gbps	10-12Gbps

Common vulnerabilities include bypassing and modifying the configuration. However, the nature of risks for routers relating to wireless standards are similar to those identified for all RE connected wireless products.

The WPA2 security protocol had to be replaced following the discovery of a security flaw in this common protocol which was used in securing most modern wireless networks[39]. A weakness was identified in the protocol's four-way handshake, which securely allows new devices with a pre-shared password to join the network. That

[38] Source: https://www.bsi-fuer-buerger.de/BSIFB/DE/Home/home_node.html
[39] https://www.zdnet.com/article/wpa2-security-flaw-lets-hackers-attack-almost-any-wifi-device/

Case study title:	Assessment of security vulnerabilities in wireless routers.
	weakness could potentially allow an attacker to decrypt network traffic from a WPA2-enabled device, to hijack connections, and to inject content into the traffic stream. Vulnerabilities have subsequently also been identified in respect of WPA3[40]. The vulnerabilities could allow attackers to leak information from WPA3 cryptographic operations and to brute-force a Wi-Fi network's password. There are also new and emerging vulnerabilities identified such as TCP injection attacks. A feature in all generations of wireless routers is that there should be a mechanism to allow interference to be detected to allow back–off and to measure delay in packets. There is a risk that certain packets could be injected into a side channel in a TCP injection attack. If the machine is connected through a Wi-Fi network e.g. through a smart phone. If there is a TCP connection between the router and an IoT device, the malevolent attacker can pretend to be the server. They are not attacking the router itself, but rather the client server behind the router. Regarding the extent of engagement by industry addressing security vulnerabilities, both manufacturers interviewed stated that they invest significantly in security, they have not. Many router manufacturers already take security very seriously, even in the absence of dedicated legislation within the RED. This is partly as data protection by design and default principles are already embedded into the product design, engineering and software testing phases. The GDPR was moreover seen as having led to the consideration of data protection and privacy issues being incorporated into business processes as part of documenting data protection by design and default obligations.
Technical solutions:	**Technical solutions suggested by industry:** Overall, industry manufacturers stated that there are already a range of technical solutions to address security vulnerabilities. However, these can never provide total protection, as new vulnerabilities may arise and unforeseen security flaws may be detected. Regarding what types of technical solutions routers manufacturers rely upon, a number of solutions have been developed. Both manufacturers interviewed have their own internal divisions working on security-related testing, legal compliance with exiting legislation, such as embedding data protection by design and default into product design. Sometimes, international standards are utilised, especially those relating to wireless internet protocols and the use of encryption technologies. Regarding the development of new security features, router manufacturers often test their products according to their own internal standards. Some external testing is undertaken to improve security systems, but this is not according to particular technical standards. The manufacturer pointed out that they are not looking for companies that follow A or B, but rather external testing partners that have new ideas and an understanding of emerging threats that nobody else has thought of yet. It was pointed out that to be effective, product security has to take as a starting point the mindset of hackers to anticipate potential vulnerabilities. A router manufacturer also noted that in common with many other connected RE product groups, there is already a network of technical standards in place covering testing for router functionality, performance, speed and security. Therefore, technical solutions are already being applied, including in respect of security through a combination of technical standards and industry-own standards. Examples of technical solutions to ensure minimum security functionality in routers are now provided. It should be stressed that the first four (WPA2/ WPA3, TLS, SSL, and the

[40] https://www.zdnet.com/article/new-dragonblood-vulnerabilities-found-in-wifi-wpa3-standard/

Case study title:	Assessment of security vulnerabilities in wireless routers.
	wireless 802.11 protocol) relate to addressing security vulnerabilities in wireless technologies providing connectivity themselves rather than to router-specific security standards. The latter tend to rely on internal security testing protocols developed by router manufacturers themselves to test their own products (see point above and further example provided under "costs and benefits". • **WPA2-PSK and WPA3 encryption by default** (Wi-Fi Protected Access Version 2). ▪ Built-in Firewall. ▪ Password authentication for changes to device configuration. ▪ Guest Network Access. ▪ VPN capabilities on the router to protect privacy. • **Transport Layer Security (TLS)**[41] a security protocol that provides privacy and data integrity over Internet communications. TLS was proposed by the Internet Engineering Task Force (IETF), an international standards organisation in 1999. TLS is a widely adopted security protocol **to facilitate privacy and data security for communications over the Internet.** A use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website. TLS can also be used to encrypt communications such as email, messaging, and voice over IP (VOIP). • **Secure Sockets Layer (SSL)** is an encryption-based Internet security protocol for the purpose of ensuring privacy, authentication, and data integrity in internet-based communications. SSL was developed in 1995 and is the predecessor to TLS encryption more commonly used today. • **The 802.11 Wireless Standard is** the most widely used and accepted standard in the wireless router market. Wireless internet standards are used for sending and receiving data over the Wi-Fi network. The standard was developed by industry. There are different variants of the standard, depending on the speed of data transmission. For example, 802.11n has a maximum speed of 600 Mb per second for data transfer, whereas 802.11a a maximum speed of 11Mbps[42]. • Wireless routers should incorporate a **mechanism to allow interference to be detected to allow back–off and to measure delays in packets**. • Technical standards provide solutions, such as those developed by the Internet Engineering Task Force (IETF). It is important to differentiate between implementation-related bugs linked to Wi-Fi technologies which can be rectified relatively easily using standards and network-level bugs. The latter can be addressed by standards, but there has been a lack of standardisation in this area to date. In the IoT field, standards are useful, but are not the panacea that people think. It is difficult to anticipate all problems ahead of time and new vulnerabilities emerge. Therefore, standards should be regularly amended and updated. • Sometimes standards take considerable time to develop. For example, regarding the TCP injection attack, there is no fix in the near term. An IEEE standards protocol could be developed to define a standard, but this might take 5 years. • It may be necessary to change the fundamental design of routers to address the threat of TCP attacks as this would allow both parties to transmit packets at the same time. Presently, only one party can transmit at any given time. However, it remains unclear whether this will be adopted to address this particular vulnerability. **Technical solutions proposed by regulatory bodies at national level:** In 2018, the German Federal Office for Information Security (BSI) published an initial draft set of rules (BSI TR-03148: Secure Broadband Router, Requirements for a secure

[41] Source: https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/

[42] https://www.marketwatch.com/press-release/wireless-router-market-2019-global-trends-market-share-industry-size-growth-opportunities-and-market-forecast-to-2025-2019-08-09

Case study title:	Assessment of security vulnerabilities in wireless routers.
	Broadband Router, Date: 11/02/2018) to secure Small Office and Home Office (SOHO) routers. The rules were put together with input from router vendors, German telecoms, and the German hardware community. The reason why Germany is taking steps to standardize router security was linked to a security incident at the end of 2016 when a hacker attempted to hijack Deutsche Telekom routers, but messed up a firmware update and crashed nearly a million routers across Germany. [43] The guidance suggests that the following minimum security measures should be adopted: • Only DNS, HTTP, HTTPS, DHCP, DHCPv6, and ICMPv6 services should be available on the LAN and WiFi interface. • If the router has a guest Wi-Fi mode, this mode must not allow access to the router's configuration panel. • The Extended Service Set Identifier (ESSID) should not contain information that is derived from the router itself (such as the vendor name or router model). • The router must support the WPA2 protocol, and use it by default. • WiFi passwords should have a length of 20 digits or more. • WiFi passwords must not contain information derived from the router itself (vendor, model, MAC, etc.). • The router must allow any authenticated user to change this password. • The procedure of changing the Wi-Fi password should not show a password strength meter or force users to use special characters. • After setup, the router must restrict access to the WAN interface, with the exception of a few services, such as (CWMP) TR-069, SIP, SIPS, and ICMPv6. • Routers must make CWMP available only if the ISP controls the router's configuration from a remote, central location. • Password for the router's configuration/admin panel must have at least 8 characters and must have a complex setup involving two of the following: uppercase letters, lowercase letters, special characters, numbers. • Just like Wi-Fi passwords, admin panel passwords must not contain router-related information (vendor, model, MAC, etc.). • The router must allow the user to change this default admin panel password. • Password-based authentication MUST be protected against brute force attacks. • Routers must not ship with undocumented (backdoor) accounts. • In its default state, access to the admin panel must only be allowed via the LAN or Wi-Fi interfaces. • If the router vendor wants to expose the admin panel via WAN, it must use TLS. • The end-user should be able to configure the port to be used for access to the configuration via the WAN interface. • The router admin panel must show the firmware version. • The router must users about an out-of-date or end-of-life firmware. • The router must keep and display a last login log. • The router must show the status and rules of any local firewall service. • The router must list all active services per each interface (LAN/WAN/Wi-Fi). • Routers must include a way to perform factory resets. The routers must support DHCP over LAN and WiFi. This is an interesting example as it shows that minimum security guidelines can be put in place when industry and other stakeholders come together and work with regulators on the development of more secure standards.

[43] https://www.zdnet.com/article/germany-proposes-router-security-guidelines/

Case study title:	Assessment of security vulnerabilities in wireless routers.
Costs and benefits of addressing security vulnerabilities:	No data was available on the costs that would be incurred if routers were subject to essential requirements pertaining to data protection and privacy / protection from fraud under the RED if the DAs were to go ahead. One of the manufacturers interviewed stated that as minimum security baseline requirements have not yet been defined for routers, it is difficult to know what these would mean and the associated compliance costs. For instance, it is not presently known whether certification is needed, if an external testing body would be needed, etc. A contrast was drawn with the software study as it might be possible to provide costs data if software updates were required for 5 years post placement on the market. Some data on the cost of ensuring security in routers was obtained under the current baseline scenario (in which there is legislation on data protection and privacy by design and default). It was pointed out that responsible router manufacturers do take security issues (including the prevention of device breaches leading to data loss or fraud) very seriously already. Therefore, ensuring that their products are secure already costs router manufacturers a considerable amount. This may suggest that the costs of activating the DAs – a regulatory approach – would be discounted as high Business as Usual costs would be applicable. This would however depend on various factors such as whether existing technical standards could be utilised, as if requirements were introduced where no standards presently exist, then this would be costly as it would require a third party. As for current testing costs prior to putting a new router product on the European market are concerned, one manufacturer stressed that security is not a one-off. Products are tested all year around through internal testing, complemented by external testing prior to every new product release. Internal and external testing to review code embedded in software is carried out, and dedicated tests of the hardware. As router products are increasingly dependent on software, a lot of time is invested in checking the quality of software coding to ensure optimal performance and security. It was stated that it is difficult to separate costs for the two as fixing bugs to ensure performance and security functionality are difficult to separate, as part of the same overall process of checking product quality prior to launch. An example of external testing costs was provided: • Prior to the launch of a new router, the firm engages 5 -6 software coders to check the coding for about 1 month of input each. • A person day costs 1500 EUR for a coder with knowledge of QA in coding. • Therefore, over one month, the cost would be 1500 EUR X 21 days av. working days/ month X 5.5 coders = €173,250. However, evidently, only some of these costs relate to security, whereas the rest relate to checking performance. Working assumption – 30% of costs relate to security, 70% to performance, hence €51,975 for security. • In addition, there would be internal testing costs. Router developers within the consumer router manufacturer have developed secure development guidelines by themselves and have developed their own approach to testing security. There is also the implementation of the four-eyes principle on critical parts of the software i.e. software developers have to develop and test code together through a peer programming approach. No single individual can develop a crucial part of the software alone. One means of reducing testing costs (for performance, security) is to use high-tech machinery capable of performing dynamic and static code analysis. Many hardware vendors always include software to support improvements in the quality of code once the product has been launched. Many bugs – including theoretical security flaws – are

Case study title:	Assessment of security vulnerabilities in wireless routers.
	identified and fixed through software patches once the products are already on the market.
Overall findings and lessons learned:	• Enterprise grade routers were found to pose a lower risk than consumer grade routers. However, even some enterprise grade routers are not immune from security vulnerabilities, for instance, those relating to flaws identified in wireless protocols such as WPA2, WPA3, etc. However, these aren't router-specific, but common across all connected RE products i.e. relating to wireless connectivity technologies themselves. • Consumer grade routers have basic security functionality, but there are concerns as to whether this is sufficient to protect products from vulnerabilities. • Some security vulnerabilities could be addressed using common sense security by design and default principles, which could be integrated into good practice guidance. For example: ▪ When initially configured, does the router force the user to provide new, non-default passwords for the router itself and for the Wi-Fi network? ▪ Has the router's web interface been protected from malicious web pages that exploit CSRF bugs? ▪ Can administrator access be limited exclusively to a secure protocol e.g. HTTPS? ▪ Routers should not allow multiple computers to log on at the same time using the same user ID. ▪ Has the hardware been appropriately designed? For example, is there an on/off button for the router and for the WiFi connection? ▪ Users of Guest Wi-Fi network should not be allowed to access the router's admin interface. • However, other vulnerabilities might risk compromising the data protection and privacy of users. Some of these are of a complex, technical nature. These can be best addressed through industry-led standards and secure protocol development / or harmonised technical standards. • Although software is being covered in a parallel study, it is important to note that software should be secure not only when the product is placed on the market to ensure users' data protection and privacy, but also that software and firmware are regularly updated by manufacturers as and when new vulnerabilities are identified post-market placement. Otherwise, there is a risk of network penetration and gaining access to data across connected IoT devices.
Data / research on market size and structure@	• Wireless Router Market 2019 Global Trends, Market Share, Industry Size, Growth, Opportunities, and Market Forecast to 2025 • Tech4i2 – updated forecasts for device-demand produced for this study.
Relevant literature providing examples of router security vulnerabilities and flaws:	• Report on IoT Device Security, Strict Consultants, on behalf of Agentschap Telecom, 'Onderzoek veiligheid apparaten', kenmerk 201901072, 15-02-2019 • Federal Office for Information Security, Germany, BSI TR-03148: Secure Broadband Router, Requirements for a secure Broadband Router, Date: 11/02/2018. • Weiteng Chen and Zhiyun Qian, Off-Path TCP Exploit: How Wireless Routers Can Jeopardize Your Secrets, 2018. University of California, Riverside https://www.usenix.org/conference/usenixsecurity18/presentation/chen-weiteng • Lili Qiu, G. Varghese and S. Suri, "Fast firewall implementations for software and hardware-based routers," *Proceedings Ninth International Conference on Network Protocols. ICNP 2001*, Riverside, CA, USA, 2001, pp. 241-250. - https://ieeexplore.ieee.org/document/992904

Case study title:	Assessment of security vulnerabilities in wireless routers.

- Independent Security Evaluators (ISE), Cybersecurity study of network attached storage (NAS) systems and routers, 2019. https://www.helpnetsecurity.com/2019/09/17/vulnerabilities-iot-devices/
- Security flaws in 802.11 data link protocols, Communications of the ACM - Wireless networking security CACM Homepage archive, Volume 46 Issue 5, May 2003, Pages 35-39
- Understanding the difficulties in security protocol design and attempting to relocate the struggle between hacker and defender to a different protocol layer.

Articles and blogs regarding security vulnerabilities and flaws:

- Comprehensive list of router bugs and vulnerabilities in routers and assessment of their potential exploitation, such as the risk of unauthorized access and bugs in software integrated into routers. https://routersecurity.org/bugs.php
- Article by Catalin Cimpanu for Zero Day | January 18, 2019 - https://www.zdnet.com/article/wifi-firmware-bug-affects-laptops-smartphones-routers-gaming-devices/
- WiFi firmware bug affects laptops, smartphones, routers, gaming devices
- List of impacted devices includes PS4, Xbox One, Samsung Chromebooks, and Microsoft Surface devices.
- Threat Bulletin - Home Router, January 2019, Allot - https://www.allot.com/resources/TB_Threat_Bulletin_Home_Router.pdf
- Article on how consumers might best protect themselves when using routers, Andy O'Donnell, October 2019 https://www.lifewire.com/wireless-router-security-features-you-should-turn-on-right-now-2487665
- https://www.zdnet.com/article/hacking-attacks-on-your-router-why-the-worst-is-yet-to-come/

- **Interviews:** three interviews were carried out with six individuals, four from router manufacturers (two from a large global player, and one from a company with a strong national position in the market and a further two with stakeholders researching security vulnerabilities in routers in academia.

4. Product case study 3 – Security Cameras and Baby Monitors

Case study title:	Assessment of security vulnerabilities in domestic close circuit TV that could compromise data protection and privacy.
Product group and short definition:	This case study focuses on *domestic closed circuit television.* These can be defined as products and systems set up to automatically take pictures inside or from a house and then transmit these over the internet. For simplicity, the term CCTV has been used. Commercial CCTVs (i.e. devices to secure commercial, public buildings or open spaces) have been excluded.
Rationale for selection of product group:	There are three main reasons for the selection of these types of products. Firstly, there is the link between images and personal data: information via CCTV is personal information. The Court of Justice of the European Union (CJEU) noted "*What seemed central was the existence of surveillance via the CCTV system*" (Woods, L. 2014). The judgment of the Court (2019) included "*It must be borne in mind that surveillance in the form of a video recording of persons, which is stored on a continuous recording device … constitutes… the automatic processing of personal data*". Secondly, there is a large and increasing range of devices which use images from within or from the house. "*Technology companies are selling a lot of new gadgets to increase home security … Many are part of the trend towards "smart homes" with internet-connected doorbells, lighting, voice assistants and so on. Most of this stuff comes under the general tech-industry label of the internet of things (IoT)".*[44] Devices which use images include those used to monitor pets in the house (Phelen, D. 2019). Images can also be used in devices to monitor babies: "*you can watch your baby or hear whenever she wakes up or cries, wherever you are in the house and with some newer apps, even if you're miles away!"*[45]. The case study also provides scope to explore what difference can be made by the way in which the RE device is connected to the internet. For non-Wi-Fi baby monitors, for example, the average range for a Bluetooth range is 215 meters, but the range can extend to more than 300 meters. When using a Wi-Fi connection, baby monitors can be accessed from anywhere via a mobile phone app. Thirdly, this product group was selected due to cases of security breaches: "*the discovery of a botnet running on Internet of Things (IoT) devices. Dubbed Mirai [it] exploited a vulnerability in digital video recorders (DVRs) used with CCTV systems".*[46] The extent of vulnerability and the information at risk can be wide, wireless security cameras have been tested and *"found critical issues with all of them. Risks range from private data being exposed, to a hacker being able to gain complete control of the camera and potentially seeing into people's home.*[47] Additionally, there have been examples of security breaches in respect of Wi-Fi connected baby monitors[48].
Case study overview and aims	As with other case studies, the aims are to: • Highlight vulnerabilities in CCTV, and to consider the extent to which technical solutions are available to mitigate these. • Consider the extent to which the vulnerabilities identified are pervasive within the product group, or specific to certain models and manufacturers.

[44] Schofield, J. (2019)
[45] O'Donnell, C. (no date)
[46] Mansfield-Devine, S. (2017)
[47] Laughlin, A. (2019)
[48] Joseph, R. (2018), Associated Press (2015)

Case study title:	Assessment of security vulnerabilities in domestic close circuit TV that could compromise data protection and privacy.
	• Review available technical solutions on the market to address vulnerabilities, and the nature of these e.g. general security by design and default principles, industry-led standards and technical standards developed by standards bodies etc. • Shed light on the costs and benefits of strengthening product security, specifically from a data protection and privacy / protection from fraud perspective.
Number of devices on European market and growth rate:	The estimates and forecasts shown here are for the large CCTV market and includes CCTV that operates on commercial buildings or public open spaces. A report by Transparency Market Research revealed that the global market for CCTV camera is expected to reach a value of US$23.32bn by 2025[49]. This can be adjusted to estimates of the EU market as between €2.8 billion – €4.6 billion in 2025. In terms of possible future growth, one forecast is that "*The global closed-circuit television camera market size will grow by USD 8.65 billion during 2019-2023*[50]." From this estimate, it is expected that the closed-circuit television camera market for the European Union from 2019 to 2023 will grow by €1 billion – €1.6 billion.
Mapping of key stakeholders in product group:	CCTV is manufactured **globally** for sale within the EU. The UK International Fire and Security Exhibition and Conference gives information on 130 companies listed as CCTV[51]. This includes those who deliver external or commercial CCTV as well as those who provide internal or domestic CCTV. More information is provided for 50 of these companies: 36% are from China, 32% from the UK, 16% from the remainder of the EU and 10% from Korea. There are a wide range of devices on the European market. For internal CCTV products, one store provides information on 41 devices with cameras - under the heading "CCTV, Wi-Fi Cameras & Kits"[52]. The price range is €35 to €695. Examples of brands that manufacture CCTV cameras are: Foscam, Linksys and Panasonic. There also smaller niche market players active in the market. For baby monitors, both Wi-Fi and non-Wifi, the price range is €35 to €400. Smart baby monitors, which go beyond video and audio feeds and offer a range of automatic monitoring features, are the priciest product group. Examples of top selling brands and manufacturers are Vtech and Nest. For wholesale customers there are several suppliers of the cameras used in baby monitors most of which offer "OEM/ODM" services. These include custom branding. This makes it more difficult to identify who is involved in the supply chain.
Type of data being collected (e.g. personal data and non-personal data)	Security cameras, such as CCTV capture images and sometimes also audio. As such the data being collected is highly personal. There are also issues relating to the use of personal data with the growing development and deployment of "facial recognition" technologies – the linking of video images to individuals as represented by their names[53]. A facial recognition system is used to identify an individual by matching the face in the image captured live through a camera with images of faces stored in a database, through similarity in facial features. There are

[49] Transparency Market Research, (2018)
[50] Technavio, (2019)
[51] Informa Markets, (2019)
[52] B&Q (2019)
[53] E.g. Although focusing on images and mobile phones, ARTICLE 29 DATA PROTECTION WORKING PARTY, 00727/12/EN WP 192 examines the legal context. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf

<table>
<tr><th>Case study title:</th><th>Assessment of security vulnerabilities in domestic close circuit TV that could compromise data protection and privacy.</th></tr>
<tr><td>How transmitted to manufacturer, technology provider or service provider</td><td>
concerns that the collection of such data may contravene the GDPR, as recently commented upon in February 2020 by the Commissioner at DG CNCT. [54]

In terms of the transmission of information, an indication of the radio configuration is given from the following 812F Wireless Camera. This is advertised as a “Wireless camera kit with colour day and IR night vision, audio, weatherproof, range up to 100 meters, watch the wildlife in your garden or field, in a bird box, tree, from your home tv.[55]”

<table>
<tr><th></th><th>Item</th><th>Value</th></tr>
<tr><td>GENERAL</td><td>Transmission Frequency</td><td>ISM 2,400~2,483 MHz</td></tr>
<tr><td></td><td>Transmission Power</td><td>10mW/CE</td></tr>
<tr><td></td><td>Operating Frequency</td><td>2414MHz;2432MHz;2450MHz;2468MHz</td></tr>
<tr><td></td><td>Unobstructed Effective Range</td><td>100m(Min.)</td></tr>
<tr><td></td><td>Modulation Mode</td><td>FM</td></tr>
<tr><td></td><td>Operating Temperature</td><td>-10 ~ +50(Degree C) / +14~ +122(Degree F)</td></tr>
<tr><td></td><td>Storage Temperature</td><td>-20 ~ +60(Degree C) / -4 ~ +140(Degree F)</td></tr>
<tr><td></td><td>Operating Humidity</td><td>≤85%RH</td></tr>
<tr><td>CAMERA</td><td>Imaging Sensor Type</td><td>CMOS</td></tr>
<tr><td></td><td>Picture Total Pixels</td><td>PAL:628×582 Pixels</td></tr>
<tr><td></td><td>Horizontal Resolution</td><td>380 TV Lines</td></tr>
<tr><td></td><td>View Angle</td><td>PAL:60°; NTSC:40°</td></tr>
<tr><td></td><td>Minimum Illumination</td><td>0Lux</td></tr>
<tr><td></td><td>Night Vision Range</td><td>7m</td></tr>
<tr><td></td><td>BandWidth</td><td>18M</td></tr>
<tr><td></td><td>Consumption Current</td><td>85mA(IR OFF) & 160mA(IR ON)(Max.)</td></tr>
<tr><td></td><td>Power Supply</td><td>DC +8V</td></tr>
<tr><td></td><td>Dimensions(W×D×H)</td><td>45*78*83 mm</td></tr>
<tr><td></td><td>Weight</td><td>217g</td></tr>
<tr><td>RECEIVER</td><td>Antenna</td><td>50 ohm SMA</td></tr>
<tr><td></td><td>Receiving Sensitivity</td><td>≤-85dBm</td></tr>
<tr><td></td><td>Intermediate Frequency</td><td>480MHz</td></tr>
<tr><td></td><td>Video Output Signal Level</td><td>1.1Vpp±0.2Vpp@75 ohm, S/N >38dM</td></tr>
<tr><td></td><td>Audio Output Signal Level</td><td>3.0Vpp±1Vpp@600 ohm</td></tr>
<tr><td></td><td>Consumption Current</td><td>190mA(Max.)</td></tr>
<tr><td></td><td>Power Supply</td><td>DC +5V</td></tr>
<tr><td></td><td>Dimensions(W×D×H)</td><td>68*78*16 mm</td></tr>
<tr><td></td><td>Weight</td><td>119 g</td></tr>
</table>

Information collected by CCTV may move through wireless transmission e.g. “Your CCTV or fire and intruder alarm system will be connected to a remote monitoring station via the Internet”[56].

To give one example of the connectedness of CCTV at home: “The owner, who was not at home at the time, was alerted to the fire by an app on their mobile phone.

The fire service said the owner's device allowed them to view live feeds from a camera that was set up in their house”[57].
</td></tr>
<tr><td>Security vulnerabilities in CCTV</td><td>
As a general description of the types of vulnerabilities that have emerged, there are issues relating to the highly personalised nature of images and audio in the case of home security systems, if these are connected directly to the internet.

Examples of security vulnerabilities identified in security cameras are:

• Over-usage of default passwords and easily guessable passwords (see examples below):
• The lack of end-to-end encryption in cameras – network-based IP or internet security cameras send unencrypted data over the internet and could allow hackers to access video footage without their owners’ knowledge.
• Security cameras using peer-to-peer (P2P) technologies have some vulnerabilities because they allow users to connect to the camera once they come online.
</td></tr>
</table>

[54] Valero, J. (2020)
[55] GLI Cameras, (2019).
[56] Farsight Security Services, (2019).
[57] BBC, (2019).

Case study title:	Assessment of security vulnerabilities in domestic close circuit TV that could compromise data protection and privacy.
	Mozilla[58] illustrate the interconnectedness of devices allowing a weakness in one to enable breaches in other devices. A problem is the common use of default passwords. *Some cameras may use default passwords – which you should always change – or they will be easy to hack*." (Jack Schofield, 2019)[59] A fictional scenario relating to the use of default passwords is now presented: *January 2012: You, a diehard fan of hand-egg action, decide to host a Super Bowl party and invite a bunch of friends. You set up an Evite account for the first time and select "football" as your password. … You forget all about setting up an Evite account and go on with your life.* *August 2013: Unbeknownst to you, Evite was breached. The dates of birth, email addresses, genders, names, passwords, phone numbers and physical addresses of over 100 million accounts were exposed...* *July 2018: You get a new Ring camera for your house so you can make sure your pricey home entertainment system is protected when you're out of town. When it's time to set up the password, you happen to pick "football". And you use the same email address, because, well, it's your email address. You don't bother turning on Ring's two-factor authentication because that sounds tricky.* *July 2019: The Evite data breach is discovered and made public. You get a message from Evite telling you to change your password, which you had forgotten all about. You end up deleting your account, but that compromised data set, containing your email address and "football" password have possibly been circulating for six years.* *December 2019: Some hackers decide to run the breached Evite data set against Ring accounts to see if they get any matches, which they do. Among the many matches, they get a hit on yours. Now they can access your Ring cameras and peer into your family room while you watch the game, and they can shout ugly things at your family through the device."* Increased security is recommended by the: • use different passwords for every account • creation of strong passwords • use of a password manager • addition of two factor authentication
Nature and extent of threat, likelihood and impacts of security vulnerabilities occurring	Key elements of the nature and threat from internet-connected CCTV (including baby monitors) can be described as the: • collection of photographs from within or outside the house • transmission of voice linked to CCTV devices • intrusion into the home and other areas where babies and children are present and there is a risk unencrypted access to livestreaming images and audio. In 2014, thousands of personal webcams, CCTV cameras and baby monitors using weak or default passwords were hacked and the footage broadcast on a Russian website[60]. IoT devices could be remotely accessed online and this footage was broadcast publicly and allowed users to see inside people's homes and even into babies' bedrooms. Of the live feeds found on the website, 4,000 are from the U.S.,

[58] Mozilla (2019).
[59] Schofield, J. (2019).
[60] Kelion, L. (2014) and Smith, A. (2014)

Case study title:	Assessment of security vulnerabilities in domestic close circuit TV that could compromise data protection and privacy.
	2,000 are from France and 500 are from the UK. Each link to footage includes the GPS coordinates of the camera where the feed is coming from, the post code and time zone of the location, and a map that shows the precise spot where the device is located. An example is that "a *Nest camera owner discovered last month his smart baby monitor had been taken over by a hacker who was talking to his baby* [61]. A further example reported was the hacking of a Babyphone in Miami[62]. There have been further incidents reported in the U.S[63]. Many video baby monitors have UPnP and port forwarding settings that can be enabled to make the camera less secure. As another example of potential security risk, Samuel Gibbs (2019) reviews Amazon's new Ring Alarm. This has a strong relationship with home CCTV and can easily be linked with cameras. It uses the ZV Wave wireless protocol wifi to connect to the various different components. The connection with concerns over privacy can come through "*Ring is under scrutiny for the way it links with police in the US, and the use of its neighbours app, and the use by users of footage captured by its cameras.*" Security (privacy) protection can be inherent but requiring users to take action. Following concerns about the Ring Alarm the company issued the statement "*Consumers should always practice good password hygiene and we encourage Ring customers to change their passwords and enable two-factor authentication*"[64] As an example of where security can be enhanced, Amazon has now revised the steps to the way users log in to their accounts for the system[65]. The impact of threats through CCTV is hard to measure. The potential is reported "*Off-the-shelf devices that include baby monitors, home security cameras, doorbells, and thermostats were easily co-opted by cyber researchers at Ben-Gurion University of the Negev (BGU). As part of their ongoing research into detecting vulnerabilities of devices and networks expanding in the smart home and Internet of Things (IoT)… "It is truly frightening how easily a criminal, voyeur or paedophile can take over these devices," says Dr. Yossi Oren*"[66]. One aspect of the risk is the (potential) invasion without specific action taken with the personal information: "*A Scottish couple have been awarded damages of more than £17,000 in total for the "extreme stress*" they suffered as a result of the "highly intrusive" use of CCTV systems by the owner of a neighbouring property. [67]
Extent to which covered by existing legislation	The key elements of how existing legislation relates to CCTV are "*If you install CCTV, it should only capture images within your own property: your home and your garden. If it captures images of your neighbours' homes, shared spaces and the public street, … then the General Data Protection Regulation (GDPR)"* applies[68]. The European Data Protection Supervisor has issued guidance on video-surveillance[69]. This is mainly focused on public buildings but as the images can be used to identify individuals there will be factors which can be applied to the

[61] Palmer, A. (2019).
[62] Reported in Metro Belgique, 16th December, 2019
[63] Vaas, L. (2019).
[64] Quoted in Noor, P (2019).
[65] BBC (2020)
[66] Quoted in American Association for the Advancement of Science (2018).
[67] OUT-LAW.COM, (2017).
[68] Schofield, J. (2019).
[69] European Data Protection Supervisor, (2019a).

Case study title:	Assessment of security vulnerabilities in domestic close circuit TV that could compromise data protection and privacy.
	transmission of images via radio equipment *"According to Article 3 (1) of Regulation (EU) 2018/1725: "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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;"*[70]. • The considerations depend on the **location of the person** whose image is captured. Data protection rights do not apply to images captured within the boundaries of a property. If the cameras capture images outside the boundary of the user's property (e.g. a neighbour's garden or a public street) then, for example, neighbours or passers-by caught on camera have rights under the data protection laws[71]. The capturing of images is not in itself a breach of the data protection laws but CCTV users must ensure they comply with these laws and respect the data protection rights of people whose images they capture. • The application relates to any video surveillance equipment mounted or fixed on a home, and can include cameras fitted into doorbells. The rights of the people whose image is captured (in the circumstances described) are: • The CCTV user must let people know they have CCTV. Signs are the most common way of doing this. They must be clearly visible and legible. • To ask for a copy of the information that is held about you. • To ask the CCTV user to erase any personal data they hold about you. • To ask that the CCTV user does not capture any footage of you in future. Though the nature of CCTV systems may make this very difficult and it might not be possible for the user to do this. An additional aspect of the use of domestic CCTV is external use which intrudes on other people. Similar concerns have been raised with IoT devices such as video-enabled smart doorbells.[72] An aspect for consideration is the nature of privacy which can be monitored through images. *"A tech firm says it has developed software that enables CCTV cameras using artificial intelligence to "read" the emotions of people in crowds*[73]*"*. The invention has a European patent. The firm, Sensing Feeling, is stated as being aware of privacy and ethics and that safeguards are in place to ensure it compliance with data laws. However (in Blunden, M. (2019) Silkie Carlo, director of Big Brother Watch, said: "*This kind of surveillance aims not to monitor your physical movements but your mental state which is a profoundly dangerous concept.*"
Stakeholder views on the nature and extent of security vulnerabilities:	Stakeholder views, reported and referenced, have been given by a range of stakeholders including members of the public and experts. In addition to these an interview was held with a consultant specialising in disseminating general information concerning Closed-circuit television. Their view was that home CCTV operate via radio and have no built-in cyber security. Security

[70] European Data Protection Supervisor, (2019b).
[71] Information Commissioner's Office (no date).
[72] Maras, M.-H. and Wandt, A. (2019). Enabling Mass Surveillance: Data Aggregation in the Age of Big Data and the Internet of Things. *Journal of Cyber Policy,* DOI: 10.1080/23738871.2019.1590437.
[73] Blunden, M. (2019).

Case study title:	Assessment of security vulnerabilities in domestic close circuit TV that could compromise data protection and privacy.
	would be an obligation from manufacturers and measures would need to be those which could not be simply be disabled. Some regulation was needed and any legislation would need to be policed and enforced.
Technical solutions:	The following ways are suggested in the Mozilla review[74] as minimum security standards; "*basic steps every company should take to protect consumer privacy*". Similar solutions are relevant to the smart watch case study reviewed later in this report. **Encryption** Data sent between a device and an app can be protected with strong encryption. For security the product must use encryption for all of its network communications functions and capabilities. This ensures that all communications are not eavesdropped or modified in transit. The product must also use encryption at rest to ensure that customer data is protected in storage. **Security updates** Updates can be pushed automatically when a device is paired with the companion app. The product must support automatic updates for a reasonable period after sale, and be enabled by default. This ensures that when a vulnerability is known, the vendor can make security updates available for consumers, which are verified and then installed seamlessly. Updates must not make the product unavailable for an extended period. **Strong password** If the product uses passwords for remote authentication, it must require that strong passwords are used, including having password strength requirements. Any non-unique default passwords must also be reset as part of the device's initial setup. This helps protect the device from vulnerability to guessable password attacks, which could result in a compromised device. For baby monitors specifically, the use of default passwords has been a particular problem resulting in a number of scandals. A software alteration can be made as part of regular software updates to force users to update their passwords. **Managing vulnerabilities** The vendor must have a system in place to manage vulnerabilities in the product. This must also include a point of contact for reporting vulnerabilities or an equivalent bug bounty program.[75] This ensures that vendors are actively managing vulnerabilities throughout the product's lifecycle. A number of the companies run "bug bounty" program - anyone who finds a security issue and discloses it responsibly may get paid. **Privacy policy** The product must have privacy information that applies specifically to the device, not a generic privacy policy that is written to cover just the company web properties. Additional privacy considerations include how data is shared with third parties, whether data can be deleted, and the readability of the privacy information.

[74] Mozilla (no date).
[75] A number of the companies run "bug bounty" programs - anyone who finds a security issue and discloses it responsibly may get paid.

Case study title:	Assessment of security vulnerabilities in domestic close circuit TV that could compromise data protection and privacy.

In the UK, the Surveillance Camera Commissioners (SCC) have issued guidance for organisations which manufacture Video Surveillance Systems[76]. This is designed to highlight the areas of vulnerability and recommend ways in which they can be tackled. The key elements are shown below[77].

The Guidance has more detail than shown here e.g. for Encryption the advice offered is that "*In order to mitigate security vulnerabilities associated with unencrypted communications and data storage, a compliant product must use HTTPS (HyperText Transfer Protocol Secure) for all communications with a web based interface, TLS (Transport Layer Security) for all communication across untrusted networks and an appropriate level of baseline encryption for all data being stored at rest*".

Element	Notes
Default Passwords	• Force the installer to change the password on boot up • Include a strength indicator or 'weak password not accepted' facility
Hardcoded Engineer Reset Passwords	• The device must not have hidden user accounts • The device must not have hardcoded account passwords • Vendors must not be able to assist users recovering lost/forgotten device passwords
Protocols and Ports	• All ports and communication protocols must be disabled by default unless vital to the functioning of the component • Commonly accepted vulnerable or obsolete communication protocols must not be present on the device • Where a newer version of a communication protocol has been developed and released, this must be incorporated into the development lifecycle and rolled out within a reasonable timeframe
Encryption	• HTTPS must be used for communication with any web interfaces. It must not be possible to connect to an out-of-the-box device without HTTPS (using self-signed certificates) • Where encryption is used for protecting network communications across untrusted networks, facilitating remote access etc. then up to date Transport Layer Security must be used • Where encryption is to be used for securing data at rest then it must utilise the current industry accepted standards
Open Network Video Interface	• ONVIF protocol must be disabled at boot up, although products can still be discovered by VMS/NVRs

[76] Surveillance Camera Commissioner, (no date).

[77] The Surveillance Camera Commissioner, (no date). Secure by Design, Secure by Default, provides clearer definition of the protocols e.g. ONVIF Protocol - Open Network Video Interface Forum Protocol

Case study title:	Assessment of security vulnerabilities in domestic close circuit TV that could compromise data protection and privacy.	
	Forum Protocol (ONVIF Protocol)	• Video stream(s) must be disabled until a new user/password is set up
	Remote Access	• Remote access must be fully disabled as default, and must be explicitly enabled before use, or permissions granted for device to 'call home'. The device may need to use DHCP, DNS etc. in line with best practice cyber security principles to achieve this • The device must never attempt to access external vendor-controlled network services without system owner consent • Remote access into a VSS must not, by default, enable access onto other connected network services • Where servers and workstations are to be provided as part of the VSS, these must be configured to be locked down in line with industry best practice, this should include no remote access in the baseline configuration
	Software Patching and Firmware Upgrades	• Manufacturers must have a portal policy/resource centre for handling upgrades/patches with transparency/community sign up programmes • For critical updates whereby a product is vulnerable, an appropriate notification is essential at base level and must be issued to those who have signed up to the portal resource centre • A non-critical and functional advisory service must also be made available to subscribers
	Penetration/Fuzz Testing (Vulnerability Scanning)	• The device must have a documented procedure and be self-tested at manufacturing source to comply with SCC/BS conformity
	Use of IEEE 802.1x	• Devices must be IEEE 802.1x capable
	• Consumers could also take responsibility and ensure that security considerations are considered when making purchasing decisions. In addition to video baby monitors using Wi-Fi and Bluetooth connections, there are also non-internet connected, radio-based baby monitors on the market, which are more secure. These work using locally-available radio frequency (short to medium range on a specific frequency) or via a digital video signal, which provides a secure connection, as there is no internet or Bluetooth connection involved. • There are a number of questions that consumers should pose before purchasing a baby monitor, and these common sense security (and data protection and privacy) by default and design practices could be integrated by manufacturers into product design: ▪ Register product with manufacturer to receive software updates and fix potential security risks	

Case study title:	Assessment of security vulnerabilities in domestic close circuit TV that could compromise data protection and privacy.
	▪ Remove default login details and set up a new password. Check if the product forces customers to change the default password before using the baby monitor. ▪ Disable DDNS (Dynamic Domain Name System) if an option ▪ Disable port forwarding or UPnP if an option ▪ Disable remote access ▪ Check that product offers at least SSL/TLS encryption for video transmission over the internet? ▪ Check that product offers AES for encrypting any data that's stored on a device or in the cloud? ▪ Check what is the company's privacy policy that produces the camera and / or audio recording facility on the baby monitor? Is the policy made publicly available in accordance with GDPR?
Costs and benefits of addressing security vulnerabilities:	No feedback on costs was received from interviewees in terms of quantification. However, there is some information available on the costs of different types of CCTVs and baby monitor products. There does not appear to be a big cost differential in the prices of Wi-Fi and non-Wi-Fi products. In terms of what activating the delegated acts might cost, many of the baseline security requirements (such as requiring a compulsory password change before the product can be activated) can be simple in nature. These would have minimal costs as they could be designed in from the outset.
Overall findings and lessons learned:	• The use of devices to take images, or livestream video and/ or audio in the home through CCTV and baby monitors is a growing and changing market. • There are a wide range of manufacturers of these devices and accompanying software and firmware updates across the world, including many OEM product suppliers and ODM manufacturers from China, who provide wholesale to different brands. • As the economic operators operating upstream in the supply chain are difficult to identify, it is also more difficult to check whether they comply with existing EU legislation, such as data protection requirements in the GDPR and privacy requirements in the e-Privacy Directive. • There are identified examples of security vulnerabilities which could lead to personal data being compromised, including the theft of sensitive images and video, with adverse child safeguarding implications. • Many of the vulnerabilities (e.g. lack of adequate password protection, unencrypted data) will be the same as for other IoT devices and not specific to CCTV and baby monitors, although there are particular issues around the sensitivity and personal nature of the data e.g. images, video and audio. • There are a number of areas where greater security protection could be designed-in through the integration of security by design. This could avoid many of the vulnerabilities associated with these product groups. • There is no clear additional cost to strengthen security that would be different to that for other devices. Many of the baseline security requirements would involve simple steps to secure devices. • There are a number of identified vulnerabilities for baby monitors which could be addressed through a combination of technical solutions. These include forcing password changes when products are activated through to the use of encryption for streaming of Wi-Fi connected baby monitors. Some stakeholders argue that IP-connected security cameras and baby

Case study title:	Assessment of security vulnerabilities in domestic close circuit TV that could compromise data protection and privacy.
	monitors pose much more of a risk than devices indirectly connected to the internet via Bluetooth as you need to be physically close to the baby monitor (within range) for it to work. This raises the issue of whether a risk-based approach may be needed in activating the Delegated Acts. Arguably, baby monitor products directly connected to the internet pose a much higher risk than those indirectly connected.

Literature consulted:

- American Association for the Advancement of Science (2018). Off-the-shelf smart devices found easy to hack. American Association for the Advancement of Science. Viewed 17th December 2019]. Available from: https://www.eurekalert.org/pub_releases/2018-03/aabu-osd031218.php
- Associated Press (2015). Several baby monitors vulnerable to hacking, cybersecurity firm warns. CBC [Viewed 19th February 2020]. Available from: https://www.cbc.ca/news/business/several-baby-monitors-vulnerable-to-hacking-cybersecurity-firm-warns-1.3213046
- B&Q (2019). CCTV, Wi-Fi Cameras & Kits, B&Q. [Viewed 9th December 2019]. Available from: https://www.diy.com/departments/electrical-security/security-alarms-cctv/cctv-wi-fi-cameras-kits/DIY580617.cat#Icamp=Nav_Safety_security_DIY580617
- BBC, (2019). Dog starts house fire in Essex by turning on microwave. BBC. [Viewed 9th December 2019]. Available from: https://www.bbc.co.uk/news/uk-england-essex-50641442
- BBC (2020). Ring doorbell makes two-factor verification mandatory. BBC. [Viewed 19th February 2020]. Available from: https://www.bbc.co.uk/news/technology-51555450
- Blunden, M. (2019). A London start-up is developing CCTV cameras that can 'read' emotions of people in crowds. Evening Standard. [Viewed 17th December 2019]. Available from: https://www.standard.co.uk/tech/cctv-cameras-that-can-read-emotions-of-people-in-crowds-a4314311.html
- Caught on Camera, (no date). What Are the Different Types of CCTV Camera? Caught on Camera. [Viewed 9th December 2019]. Available from: https://www.caughtoncamera.net/news/different-types-of-cctv/
- Data Protection Working Party (2012). Opinion 02/2012 on facial recognition in online and mobile services, 00727/12/EN WP 192. European Commission. [Viewed 9th December 2019]. Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf
- European Data Protection Supervisor, (2019a). Video-surveillance. European Data Protection Supervisor. [Viewed 9th December 2019]. Available from: https://edps.europa.eu/data-protection/data-protection/reference-library/video-surveillance_en c
- European Data Protection Supervisor, (2019b). Personal data. European Data Protection Supervisor. [Viewed 9th December 2019]. Available from: https://edps.europa.eu/node/3110#personal_data
- Farsight Security Services, (2019). How remote CCTV monitoring works. Farsight. [Viewed 9th December 2019]. Available from: https://www.farsight.co.uk/installers/resources/how-remote-cctv-monitoring-works/
- Gibbs, S., (2019). Ring Alarm review: Amazon's smart security upgrade. Guardian Newspaper. [Viewed 12th December 2019]. Available from: https://www.theguardian.com/technology/2019/dec/12/ring-alarm-review-amazon-diy-wireless-home-security-system
- GLI Cameras, (2019). Outdoor Wireless Camera. GLI Cameras. [Viewed 9th December 2019]. Available from: http://www.trail-camera.co.uk/812F.htm
- Info Curia Case Law (2019). JUDGMENT OF THE COURT (Third Chamber). [Viewed 13th December 2019]. Available from: http://curia.europa.eu/juris/document/document.jsf?text=&docid=221465&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=7576859
- Informa Markets, (2019). Global Directory. Informa. [Viewed 9th December 2019]. Available from:https://directory.ifsecglobal.com/cctv-monitoring-code004999.html

Case study title:	Assessment of security vulnerabilities in domestic close circuit TV that could compromise data protection and privacy.

- Information Commissioner's Office (no date). Domestic CCTV systems - guidance for people using CCTV. Information Commissioner's Office. [Viewed 10th December 2019]. Available from: https://ico.org.uk/your-data-matters/domestic-cctv-systems-guidance-for-people-using-cctv/
- Joseph, R. (2018). Wi-Fi baby monitor hacked: Parents wake up to voice threatening to kidnap their child. Global news. [Viewed 19th February 2020]. Available from: https://globalnews.ca/news/4785542/wifi-baby-monitor-hacked-kidnap/
- Kelion, L. (2014). Breached webcam and baby monitor site flagged by watchdogs. BBC. [Viewed 19th February 2020]. Available from: https://www.bbc.co.uk/news/technology-30121159
- Laughlin, A. (2019). The cheap security cameras inviting hackers into your home. Which. [Viewed 9th December 2019]. Available from: https://www.which.co.uk/news/2019/10/the-cheap-security-cameras-inviting-hackers-into-your-home
- Mansfield-Devine, S, (2017). Weaponising the Internet of Things, Volume 2017, Issue 10, pages 13-19.
- Mozilla (2019). Tips to improve your Ring camera security. Mozilla. [Viewed 30th December 2019]. Available from: https://blog.mozilla.org/firefox/ring-camera-security/?utm_source=desktop-snippet&utm_medium=snippet&utm_campaign=p100-security-tips-blogs-2019&utm_term=22184&utm_content=REL
- Mozilla (no date). Minimum Security Guidelines Explained. Mozilla. [Viewed 9th December 2019]. Available from: https://foundation.mozilla.org/en/privacynotincluded/about/
- Noor, P (2019). Ring hackers are reportedly watching and talking to strangers via in-home cameras. The Guardian. [Viewed 17th December 2019]. Available from: https://www.theguardian.com/technology/2019/dec/13/ring-hackers-reportedly-watching-talking-strangers-in-home-cameras?
- OUT-LAW.COM, (2017). Scottish court issues damages to couple over distress caused by neighbour's use of CCTV. The ARegister. [Viewed 9th December 2019]. Available from: https://www.theregister.co.uk/2017/02/10/scottish_court_issues_damages_to_couple_over_distress_caused_by_neighbours_use_of_cctv/
- Palmer, A. (2019). Google DENIES it's to blame for recent Nest camera hacks but warns owners to reset passwords after numerous devices were taken over remotely. The Daily Mail. [Viewed 30th December 2019]. Available from: https://www.dailymail.co.uk/sciencetech/article-6679383/Google-warns-Nest-camera-owners-reset-passwords-hackers-devices.html
- Phelan, D. (2019) 8 best pet cameras. The Independent. [Viewed 17th December 2019]. Available from: https://www.independent.co.uk/extras/indybest/house-garden/pets/best-pet-cameras-a8184141.html
- Schofield, J. (2019). Home alarm systems: how can I improve my security? Guardian Newspaper. [Viewed 9th December 2019]. Available from: https://www.theguardian.com/technology/askjack/2019/nov/21/home-alarm-systems-security
- Smith, A. (2014) Russian Website Streams Footage From Thousands of Hacked Webcams. Newsweek. [Viewed 19th February 2020]. Available from: https://www.newsweek.com/russian-website-streams-footage-thousands-hacked-webcams-285721
- Surveillance Camera Commissioner, (no date). Surveillance Camera Commissioner-Secure by Design, Secure by Default. Surveillance Camera Commissioner. [Viewed 9th December 2019]. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/810183/Secure_by_Default_Requirements_and_Guidance_FINAL.pdf
- Technavio, (2019). Closed-circuit Television (CCTV) Camera Market by Product and Geography - Global Forecast and Analysis 2019-2023. Technavio. [Viewed 9th December 2019]. Available from: https://www.technavio.com/report/closed-circuit-television-cctv-camera-market-industry-analysis
- Transparency Market Research, (2018). Global CCTV Camera Market to Reach US$23.32 bn by 2025 with Rising Focus on Technological Developments. Transparency Market Research. [Viewed 9th December 2019]. Available from: https://www.transparencymarketresearch.com/pressrelease/cctv-camera-market.htm
- Valero, J. (2020). Vestager: Facial recognition tech breaches EU data protection rules. . EURACTIV.com [Viewed 19th February 2020]. Available from:

Case study title:	Assessment of security vulnerabilities in domestic close circuit TV that could compromise data protection and privacy.

https://www.euractiv.com/section/digital/news/vestager-facial-recognition-tech-breaches-eu-data-protection-rules/

- Vaas, L. (2019). Parents say creep hacked their baby monitor to tell toddler they 'love' her. [Viewed 19th February 2020]. Available from: https://nakedsecurity.sophos.com/2019/11/26/parents-say-creep-hacked-their-baby-monitor-to-tell-toddler-they-love-her/
- Woods, L. (2014). Big Brother's Little Brother? The scope of the 'household exception' to EU data protection law. EU Law Analysis. [Viewed 13th December 2019]. Available from: http://eulawanalysis.blogspot.com/2014/07/big-brothers-little-brother-scope-of.html

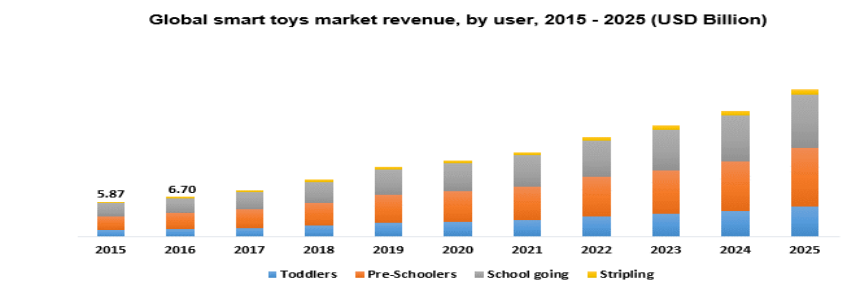
Baby monitors

- Hacking incidents and other security vulnerabilities in baby monitors
- https://www.huffingtonpost.co.uk/entry/your-baby-monitor-could-be-hacked-security-tips_uk_5bd6d75be4b0d38b58854c9d?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAJEl1pqrgXo61pJ88kL_cLjo_zSH2ec9VfWGj5X7IfVJ4RsTnEMQEw7u_EY5BFowSPIjEqm16ATnQfpHc8Ecf0jly-dQ_LmlBkTbQXXHqAm00ceA0vp8DuHuL1ZlUBurYWPPbZ9rADlhUAFgLz1csWMPeVRxLdkqZ_k5azbWanHd
- The National Cyber Security Centre (NCSC) found vulnerabilities in existing baby monitors that would allow would-be attackers to obtain audio from the device, or to change information about the position and temperature of a child in their bedroom.
- https://globalnews.ca/news/4785542/wifi-baby-monitor-hacked-kidnap/ , https://www.cbc.ca/news/business/several-baby-monitors-vulnerable-to-hacking-cybersecurity-firm-warns-1.3213046
- https://babygearessentials.com/hacked-baby-monitor/
- https://www.npr.org/sections/thetwo-way/2018/06/05/617196788/s-c-mom-says-baby-monitor-was-hacked-experts-say-many-devices-are-vulnerable?t=1578046656034
- https://www.groovypost.com/howto/secure-your-video-baby-monitor/
- Costs of baby monitors and products available (Wi-Fi, non-Wi_FI)
- O'Donnell, C. (no date). Buyer's guide to baby monitors. Made for Mums. [Viewed 17th December 2019]. Available from: https://www.madeformums.com/reviews/buyers-guide-to-baby-monitors/
- How to Choose the Best Baby Monitor - Babylist, https://www.youtube.com/watch?v=71dw5nkGF7k

Interviews:

For this case study views have been sought from manufacturers, market research organisations and those carrying out academic research which relates to this. In addition to the references given above there has also been a direct interview with a consultant on CCTV security.

5. Product case study 4 – Smart Toys

Case study title:	Assessment of security vulnerabilities in smart toys.
Product type and short description:	**Connected smart toys** Smart toys have emerged in recent years in the European and global market as conventional toys have been equipped with electronic components, sensors and a micro-processors to enable wireless network communication with mobile devices that provide services via apps to enhance functionalities in toys. Depending on which technology underpins a particular smart toy, the market is classified into toys that use Wi-Fi, Bluetooth, RFID or NFC. Voice recording and speech recognition capabilities may be included in smart toys as technologies to develop innovative and interactive toys have evolved. They may also embed artificial intelligence.
Market size and structure.	According to Hexa Research[78], "the global smart toys market was valued at USD 7.78 billion in 2017 and is expected to grow at a CAGR of 15.5% from 2017 to 2025". Although sales of connected smart toys have grown in the past five years, they still only represent a small percentage of the overall global toy market. An overview of the anticipated evolution in the market between 2015 and 2025 is provided below.  *Source: Hexa Research[79]* It was suggested however by interviewees from a leading global manufacturer that the market share of smart toys as a proportion of the total is only about 5% in the US and much smaller in Europe, perhaps 1-2%. European consumers appear more reluctant to purchase smart toys (whether the market share differs from the US due to cultural differences or due to privacy considerations is unclear). In the next decade, geographically, the Americas and Asia Pacific region are expected to be key growth markets. Various market research reports[80] have pointed to one of the drivers of sales growth being interest in smart toys that focus on subject matter, such as toys that engage young people in science, technology, engineering and mathematics (STEM) learning.
Key manufacturers	Examples of the larger market participants are Dream International (Hong Kong), Hasbro Inc. (U.S.), Jakks Pacific (U.S.), Kids II Inc.(U.S.), KNEX Industries Inc. (U.S.), Konami Corporation (Japan), Leapfrog Entertainment (U.S.), Playmobil (U.S.), The Lego Group (Denmark), and Mattel Inc.(U.S.). Collectively, these firms have a very significant share of the global market of toys generally and of smart toys. There are also some SMEs active in the market.

[78] Smart Toys Market Size and Forecast, By User, Distribution Channel and Trend Analysis, 2019 - 2025 February, 2019 https://www.hexaresearch.com/research-report/smart-toys-market

[79] Smart Toys Market Size and Forecast, By User (Toddlers, Pre-schoolers, School-going, Stripling), By Distribution Channel (Convenience Stores, Specialty Stores, Online Channel) and Trend Analysis, 2019 - 2025

[80] See for example a report by Technavio on the Global Smart Toys Market, November 2018 https://www.technavio.com/report/global-smart-toys-market-industry-analysis

Case study title:	Assessment of security vulnerabilities in smart toys.
Type of personal data being collected.	The type of personal data collected by smart toys may include commonly collected account data such as on the name, gender, age, address etc. of the user (or their parent). In addition, some toys may have recording capabilities to record, capture and retain voice messages. Localisation data i.e. data on the geolocation of the child using the smart toy may also be kept if the device contains GPS. As of May 2018, the GDPR has provided protection for all users - including children - as to what type of data can be collected. In some jurisdictions, such as the US, there are strict laws about what type of data can be collected about children. In the UK, the Information Commissioner's Office has published good practice guidance on what type of data can be collected about children online.
Security vulnerabilities relating to data protection and privacy:	The Norwegian Consumer Council carried out tests on internet-connected toys and identified a number of security vulnerabilities in smart products such as dolls. The Council looked into the technical features of selected connected toys, and the terms of use. The findings showed a lack of understanding of children's rights to privacy and security. Among the findings in terms of the vulnerabilities identified were that: • The connected toy could engage in 'conversations' with children by using built-in microphones and speech recognition technologies. Spoken data, collected during the use of the toys, could potentially be shared with third-parties, especially via third-party mobile applications. • Risks from a child safeguarding perspective, as it was possible to use a mobile phone to speak to children through toys using Bluetooth connections up to 20 metres away. The Bluetooth connection had not been secured, so testing bodies were able to gain access without a password or other form of authentication. • Bluetooth has a range limit, usually 10-20 metres, so the immediate concern would be someone with malicious intentions close-by. However, there are methods for extending Bluetooth's range[81]. Ranges can be stretched by using signal repeaters and moreover, newer versions of Bluetooth have longer ranges from around 75m - 250m. Unsecured Bluetooth connections have been identified in several other Smart Toy products[82]. • There were security vulnerabilities in software in the Cayla doll that allowed unauthorised users to hack the toy. • A further problem identified was that examples of hidden marketing were identified, raising privacy concerns and ethical considerations for children playing with the doll. Localisation data (i.e. the geolocation of the child using the device) was a further risk identified in both smart toys and in smart watches targeted at children. This is less a security vulnerability *per se* as the product may be expressly designed to include GPS capabilities. However, it raises issues as to the trade-off between parents who want to know the whereabouts of their children and issues around child safeguarding. It would be difficult to solve such issues through the RED. There have also been further examples of security problems associated with particular types of smart toys, such as a 2017 hack of smart teddy bears[83], where the company responsible leaked 800,000 user account credentials and hackers then locked these

[81] https://www.scienceabc.com/innovation/what-is-the-range-of-bluetooth-and-how-can-it-be-extended.html
[82] https://www.which.co.uk/news/2017/11/safety-alert-see-how-easy-it-is-for-almost-anyone-to-hack-your-childs-connected-toys/ - Which?
[83] https://www.vice.com/en_us/article/pgwean/internet-of-things-teddy-bear-leaked-2-million-parent-and-kids-message-recordings

Case study title:	Assessment of security vulnerabilities in smart toys.
	accounts and held them for ransom. Two million message recordings were also left exposed online for anyone to see and listen. A security researcher also revealed that the toys could easily be hacked and turned into spying devices. Other smart toys have also been found to raise security concerns, for instance, a report by "Which?"[84] in the UK found that when Bluetooth connections had not been secured, meaning that unauthorised persons would not need a password, Pin code or any other authentication to gain access, although they would need to be in physical close proximity, given the distance limitations of Bluetooth. There have also been examples of problems in the US. For example, data breaches relating to customer accounts of smart toy owners occurred. Data was being collected by an app that was bundled in with many electronic toys. However, the data was not properly secured online and was hackable. Moreover, a hacker was also able to access an internal database at the company that held copies of encryption keys that, if used, would have let an attacker view photos and audio files uploaded by children and parents. The means of collecting data was found to have broken US laws governing the way data about children is gathered and consequently, the regulator, the FCC, issued a fine to the company concerned[85]. Given the above examples of security vulnerabilities in smart toys, a key issue is whether consumer safety requirements for toys should be updated in light of the specific challenges relating to ensuring security, given their increased digitisation. However, it should be recognised that smart toys still only account for a small percentage of the total European toys market (see section on market size/ structure). A recent study in 2020 found that there are considerable implications from a consumer safety and security perspective. In total, there were found to be 28 new consumer requirements due to the digitization of toys. *"Most of the consumer requirements relate to data protection and data security of "smart" toys. In addition, two types of consumer requirements can be distinguished: 21 consumer requirements, which generally apply to networked devices of the "Internet of Things", and seven consumer requirements, which are specific to "smart" toys".* [86] Interviewees from industry however pointed out that many of the vulnerabilities relate more to vulnerabilities that have not been exploited by hackers, but have rather been identified by security researchers. As such, they remain of concern but somewhat theoretical risks as they have not materialised as a threat in practice. An example was given that unsecured Bluetooth connections are only an issue if an unknown or unauthorised adult is within 10-20m of the child, and poses a much lower risk than an unsecured direct internet connection via wireless or mobile.
Technical solutions to address identified vulnerabilities	**Many of the security vulnerabilities identified relate to the smart toy's internet connectivity not being secured.** Unsecured Bluetooth connections could for instance be made password-protected by default as an example of a simple means of strengthening their protection. Several examples of existing technical standards were identified, such as DIN EN 71-1 (safety of toys) or DIN EN 62115 (safety of electric toys). These provide manufacturers with clear guidelines for the construction of toys and how certain requirements can be

[84] https://www.which.co.uk/news/2017/11/safety-alert-see-how-easy-it-is-for-almost-anyone-to-hack-your-childs-connected-toys/

[85] https://www.bbc.com/news/technology-42620717

[86] Institute for Consumer Policy (ConPolicy) has on behalf of the DIN consumer council carried out a study on "Digitization aspects and consumer requirements with regard to smart toys – Implementation in standardization".

Case study title:	Assessment of security vulnerabilities in smart toys.

met. [87]

In addition, further more generic standards were also found to be potentially relevant to strengthening the security of smart toys from a data protection and privacy perspective, namely:

- ETSI TS 103 645 (Cyber Security for Consumer Internet of Things)
- DIN SPEC 27072 (IoT devices – Minimum requirements for information security)
- ISO 31700 (Consumer Protection – Privacy by Design for Consumer Goods and Services), which is currently in draft.

Combating fraud is not presently explicitly addressed in such standards.

The documenting of business processes has become more ubiquitous in the design of smart toys. For example, Security Requirements Engineering (SRE) (the process of identifying, analysing and documenting requirements) has become better known and used. Examples are: Lightweight Application Security Process (CLASP), Security Quality Requirements Engineering (SQUARE), and the Security Development Lifecycle (SDL) from Microsoft.

Some technical solutions to address security vulnerabilities could be low cost, such as designing in greater security by design and default at the product design stage.

Many potential security vulnerabilities in smart toys could be addressed through data encryption and requiring authentication.

There has been an effort by some stakeholders interested in strengthening the security of connected toys to define good practices that could be integrated into the development of baseline security requirements in future using a software development approach that embeds security principles. Some of these principles are based on a common sense approach to ensuring security by design and default. Moreover, data protection and privacy by design and default is already not just a principle, but legally enshrined in the GDPR.

The following table presents is a longlist intended to stimulate debate on possible good practices in the design of smart toys and outlines potential technical solutions. Were the delegated acts to go ahead, however, baseline security requirements would need to be developed to translate these principles into technical standards.

1. The smart toy app must provide the user with a notice about what information it collects, the further use of such data (including by third parties) and disclosure practices.
2. The smart toy app must provide a specific interface in order to identify user age and obtain user consent before the personal information collection and manipulation; in the case of child user, obtain verifiable parental consent and parental consent review.
3. The smart toy app must not ask for more personal information in order to continue its operation.
4. The smart toy app must authenticate users.
5. Communication between physical toy and mobile device must use a protocol that allow authentication and authorization mechanisms.
6. Mobile services providers must own digital certificates allowing identity verification.
7. Configuration file integrity must be maintained and verified in every mobile app play session.
8. Every communication in toy computing environment must use cryptographic mechanisms.
9. The Database Management Systems (DBMS) must provide user authentication.
10. The DBMS must provide security mechanisms against to external modification of stored

[87] See "Digitization aspects and consumer requirements with regard to smart toys – Implementation in standardization", Institute for Consumer Policy (ConPolicy) on behalf of the DIN consumer council.

Case study title:	Assessment of security vulnerabilities in smart toys.
	data. 11. The smart toy app must request authentication renew before every financial transaction. 12. The DBMS must provide data encryption feature or allow data encryption by third-party tools. 13. The smart toy app must encrypt personal information accessed from others apps inside the same mobile device. 14. The mobile app must not access unnecessary files from others mobile apps inside the same mobile device. 15. The physical toy must nor accept commands from mobile devices outside the current play session. 16. Every communication must use secure protocol with cryptographic mechanisms. 17. The smart toy must delete unnecessary personal information collected. 18. The smart toy must maintain personal information accurate, complete and up-to-date as is necessary. Feedback on technical solutions was sought from industry. A distinction was identified between technical standards developed by international standards bodies and those developed in-house by industry. • Regarding the use of technical standards, a large toy manufacturer interviewed mentioned that they work with different national security frameworks and with some international standards. The NIST framework in the US provides the basis for monitoring their compliance with standards, but there is often a need to carry out a lot of testing and to make adaptations to products that go to a further level of customisation beyond the standard alone. • The firm also carries out a lot of radio frequency testing (e.g. checking performance functionality and the security of Bluetooth and WiFi embedded within smart toys using industry standards, and checking product for child safety and radio equipment transmissions). • There is also an effort to use the latest leading industry protocols, such as the most recent Bluetooth version to ensure security. • There may be benefits of using more secure chips in smart toys, but there is an issue as to which secure chips should be used, as processing power needs may differ. There are also difficulties in combining high-end chips that allow for strong data encryption with lower-capacity chips used in other parts of the hardware. This depends how much data processing speed and memory is needed.
Regulatory gaps:	Children may be exposed to potential data leakages if there is an inadequately secure internet connection (e.g. indirect via an unsecured Bluetooth) and/ or if the data is stored in an insecure way (leading to a risk of a hack). However, children's data and privacy should already be protected in theory via the data processing requirements in the GDPR and the rules on ensuring privacy in the transmission of data under the e-Privacy Directive (e-PD). The Cayla doll example provides an illustration that there are some EU level regulatory gaps. Several security flaws were identified with the product. This exposed vulnerable users i.e. children to potential breaches of their data protection rights and did not adequately ensure their privacy. Despite this, market surveillance authorities (MSAs) were unable to remove the products under either the RED since the Directive's essential requirements focus on: ensuring the physical safety of users using the product and on preventing harmful interference. It was also not possible to use any other relevant EU legislation, such as the GDPR or e-PD, as although there is scope to impose large fines under the GDPR, which could have been issued against processors

Case study title:	Assessment of security vulnerabilities in smart toys.
	using data subjects' data without user consent, such sanctions are under the responsibility of national data protection authorities, rather than MSAs responsible for industrial products. There was accordingly no legal scope to remove the Cayla doll (or other products raising security or privacy concerns) from the market. Some MSAs were instead able to remove products from the national market by using an array of national legislation. For example, in Germany, a law preventing spying was used to ban such devices from recording children which was used to remove them from the market. Recourse to diverse pieces of national legislation to remove products from national markets arguably risks undermining the Single Market, especially as some Member State authorities (supported by MSAs) have held back on the introduction of national legislation in the expectation that the Commission was considering activating the two delegated acts in the RED. For example, in 2017, Germany's Federal Network Agency (Bundesnetzagentur) prohibited the sale of children's smartwatches[88] with eavesdropping capabilities under an old piece of national legislation preventing equipment from having spying capabilities. The agency even urged parents to destroy such watches on the basis that they may pose a threat to children's privacy and the privacy of others.
Impact of inadequate security and identified vulnerabilities in connected smart toys:	Regarding the impacts, such products are often distributed widely and globally. For instance, Cayla and i-Que are distributed in the US, Norway, Sweden, Denmark, Australia, Netherlands, and the Middle East. They therefore pose an ongoing risk to children not only in Europe, but in other countries, and fail to protect children adequately. Overall, the Council found that the internet-connected toys My Friend Cayla and i-Que fail to safeguard basic consumer rights, security, and privacy. This was posited as being illegal since the report points out that "the right to privacy is enshrined in the European Convention of Human Rights, and further reflected in the European Data Protection Directive".
Industry views on key issues raised (security vulnerabilities):	Recognising the complexity of the issues raised, it is important to provide an industry perspective and reaction to the issues raised both in relation to earlier security vulnerabilities in smart toys. The extent to which – and how – these are being addressed by industry but also to consider how large manufacturers of smart toys are embracing good practices to address the risk of vulnerabilities by designing these out from the outset of the design and engineering process. Whilst recognising some flaws and vulnerabilities, toy manufacturers and their representatives noted that the industry is moving up the maturity curve and has made improvements over the development of successive generations of smart toys. They also contested some of the findings from the research by consumer organisations. For example, the references to commercial brands among the phrases that the doll spoke were due to the manufacturer intending to use phrases and words the child may already be familiar with to make the toy appealing. There was no intention of using hidden marketing insofar as there were not commercial deals with place with the brands that were mentioned. The risks associated with Bluetooth connections were also seen as having been taken out of proportion in that the range of many Bluetooth devices is quite limited. A further point raised was that whereas there has been a lot of media attention to concerns regarding data getting into the wrong hands, the fears may be overblown. Non-sensitive personal data tends to be gathered by many smart toy products partly due to the strict regulatory regime under which global manufacturers have to operate (e.g. GDPR in Europe, COPPA in the US) regarding data collection and processing. This

[88] https://www.theverge.com/circuitbreaker/2017/11/19/16671428/germany-bans-smartwatches-kids-parents-destruction

Case study title:	Assessment of security vulnerabilities in smart toys.
	means that the impact of a hacking attack could be localised to the relatively limited data collected on the device itself. The large toy manufacturer interviewed explained that they already treat children's data protection and privacy seriously and have integrated security by design and default principles into their business processes. This has complemented more specific procedures relating to data protection and privacy by design and default required under EU legislation (e.g. the GDPR and e-PD) in the design of smart toys. Large manufacturers are concerned about such issues both due to non-regulatory and regulatory drivers. From a non-regulatory perspective, leading toy manufacturers recognise that their main customer base is children and young people and are therefore concerned about the potential reputational issues if they did not take such issues very seriously and integrate them into business processes. Moreover, it was pointed out that smart toys are an increasingly regulated market, and therefore have to be designed accordingly, with a consequent reluctance among some leading manufacturers to collect any more than the absolute minimum personal data and information when the product is registered. In Europe, the GDPR has made a significant difference in that business processes have to be more carefully documented to demonstrate that data protection and privacy by design and default (and appropriate technical and organisational measures) have been implemented during the design and engineering phases, supported by extensive testing. In the US, there is already longstanding legislation through the Children's Online Privacy Protection Act (COPPA), a U.S. federal law took effect in April 2000 designed to limit the collection and use of personal information about children by the operators of Internet services and Web sites. A further risk for manufacturers is that other actors in the value chain may take decisions outside their control regarding selling particular smart toys if they perceive that the toy concerned does not meet particular requirements. "*Stores may make decisions based on their interpretation of the law".* Therefore, big manufacturers increasingly tend to play it very safe by avoiding taking risks with product security, reducing the amount of personal data that they collect and transmit via internet and containing much of the data on the localised device.
Costs, benefits and impacts were delegated acts to be activated	It was highlighted that integrating data protection and privacy by design and default implies significant resource, with a number of different functional business units involved in the process, including teams specialising in legal compliance for new products, data protection and privacy teams, product engineers and senior managers. Moreover, data protection and privacy issues are thought about carefully not only at design stage but during rigorous testing. From a cost perspective, the research found that at least among leading global manufacturers, there is already considerable resource devoted to managing compliance with existing data protection and privacy legislation globally and in seeking to minimise reputational risk. Activating the two delegated acts may therefore involve high 'business as usual' costs in that firms are already taking steps to ensure that potential vulnerabilities are designed out, and reflecting in new product development processes in line with a security baseline requirements approach. However, the actual costs would depend on how security baseline requirements are defined, and on whether existing testing carried out in-house and documented by product engineers would be accepted or if additional testing would be needed to check compliance against technical standards. The level of cost would also depend on whether there are specific levels of encryption specified in chips or in hardware. Regarding hardware, it was noted that different industries use different protocols and the toy industry uses specific chipsets that follow specific protocols. Therefore, any future possible harmonised technical

Case study title:	Assessment of security vulnerabilities in smart toys.
	standards (under a DA) would need to be very careful about requiring specific hardware, otherwise it would impose additional costs on the toys industry. A number of factors determine the cost of a smart toy. The chips used are one of the most expensive elements. Regarding the types of chipsets used in smart toys, chips that allow for encryption are typically used by major toy manufacturers. However, secure chips can be costly and the economic viability of a product may depend on the encryption level, as if chips are too costly on a low retail value product, it may not get produced at all.
Conclusions and lessons learned	• Due to the fact that children are vulnerable consumers from a product security perspective, smart toys raise particular considerations around the need to ensure that users are safeguarded. • The research identified many security vulnerabilities, some linked to the risk of device level penetration, and risks associated with unauthorised access via unsecured Bluetooth connections. • There were also specific privacy concerns raised around what type of information and data can legitimately be collected by manufacturers and service providers, such as whether voice recordings are intrusive and if retained, raise particular concerns regarding their accessibility online (see Teddy Bear hack). • Whilst recognising that the vulnerabilities identified in this case raise concerns, the toy industry noted that smart toys account for a small share of the total market, and alluded to progress having been made in addressing vulnerabilities over successive generations of development of smart toys. Other literature confirms that the situation has improved over time, albeit slowly. *"For a long time, systems were developed almost exclusively to meet functional requirements and limited attention was given to security requirements"*[89]. • The toy industry moreover is already aware of the need to protect children and of the reputational risks and potential damage that could be done if these risks are not adequately mitigated through the implementation of security by design and default principles at the design phase. • The industry could cope with the formalisation of these requirements through the activation of delegated acts in the RED, as leading global smart toy manufacturers (who account for a high market share), are already carrying out similar testing. • However, their preference is for industry self-regulation as they are already subject to the GDPR in Europe and to COPPA in the US, and therefore take data protection and privacy concerns seriously as part of existing regulatory compliance efforts.
Bibliography	**Smart toys generally** • "Digitization aspects and consumer requirements with regard to smart toys – Implementation in standardization", Institute for Consumer Policy (ConPolicy) on behalf of the DIN consumer council. • Information about four internet-enabled toys, I-Que Intelligent Robot, Toy-fi Teddy, the Furby Connect and CloudPets cuddly toy. • https://www.which.co.uk/news/2017/11/safety-alert-see-how-easy-it-is-for-almost-anyone-to-hack-your-childs-connected-toys/ **Research published by EU and national consumer associations, as well as by security researchers.** • The Norwegian Consumer Council (NCC) - #Toyfail, an analysis of consumer and privacy issues in three internet-connected toys, December, 2016, https://fil.forbrukerradet.no/wp-content/uploads/2016/12/toyfail-report-

[89] Security Requirements for Smart Toys, Brazil, 2016. https://www.scitepress.org/Papers/2017/63370/63370.pdf

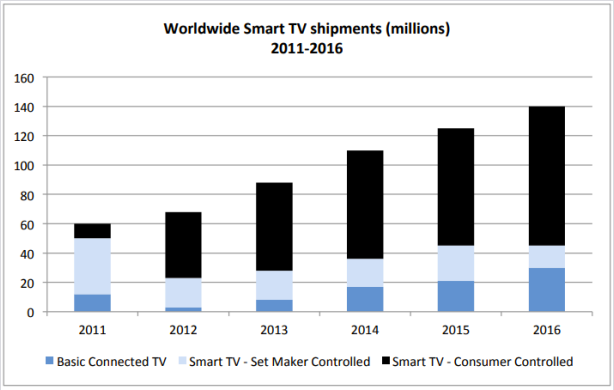
Case study title:	Assessment of security vulnerabilities in smart toys.
	desember2016.pdf • Holloway, Donell & Green, Lelia. (2016). The Internet of toys. Communication Research and Practice. Holloway, Donell & Green, Lelia. http://www.tandfonline.com/doi/abs/10.1080/22041451.2016.1266124 • Mascheroni, G., & Holloway, D. (Eds.) (2017). The Internet of Toys: A report on media and social discourses around young children and IoToys. DigiLitEY. Frames privacy as a Children's Right and considers hidden marketing practices. http://digilitey.eu/wp-content/uploads/2017/01/IoToys-June-2017-reduced.pdf • Lindqvist, Jenna - 'The Internet of Toys is no child's play: Children's data protection on internet of things and in digital media: new challenges'. Data Protection, Privacy and European Regulation in the Internet Age (Forum Iuris, Helsinki 2016) 84-109. • Luciano Gonçalves de Carvalho and Marcelo Medeiros Eler, School of Arts, Sciences and Humanities, University of São Paulo, Brazil, FATEC Mogi das Cruzes, São Paulo State Technological College, Brazil, Security Requirements for Smart Toys, Brazil, 2016. http://www.scitepress.org/Papers/2017/63370/63370.pdf Extensive grey literature was reviewed and in addition, research published by EU and national consumer associations, as well as by security researchers. **Smart dolls** • https://www.theguardian.com/world/2017/feb/17/german-parents-told-to-destroy-my-friend-cayla-doll-spy-on-children • https://www.fastcompany.com/90270035/reminder-dont-buy-smart-toys-for-kids-this-year • https://www.npr.org/sections/thetwo-way/2017/02/17/515775874/banned-in-germany-kids-doll-is-labeled-an-espionage-device?t=1577970505323 **Smart watches for children** • https://www.fastcompany.com/40496691/maybe-santa-shouldnt-bring-the-kids-any-internet-enabled-toys-this-year • Germany has taken regulatory action to ban smartwatches and internet-connected dolls for children due to privacy concerns. ▪ https://www.datenschutz-notizen.de/bundesnetzagentur-verbietet-smartwatches-mit-abhoerfunktion-2819532/ ▪ https://www.fastcompany.com/90151786/when-is-the-u-s-going-to-ban-the-internet-of-things-for-children ▪ https://www.theverge.com/circuitbreaker/2017/11/19/16671428/germany-bans-smartwatches-kids-parents-destruction **Teddy bears** - user account credentials and voice messages left unprotected online • https://www.vice.com/en_us/article/pgwean/internet-of-things-teddy-bear-leaked-2-million-parent-and-kids-message-recordings • https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/
Interviews	Interviews were undertaken with eleven different people in total in five separate interviews (some of which were group discussions): • EU and national consumer councils (3) • Toy industry association at EU level (1) • Six staff from global manufacturer of toys representing different business units (e.g. product engineers, compliance managers, senior management)

6. Product case study 5 – Smart TVs

The case study on Smart TVs is presented in the table below:

Case study title:	Assessment of security vulnerabilities in Smart TVs.
Product group and short definition:	Smart TVs, also known as connected TVs, have integrated Internet and Interactive "Web 2.0" features, which allows consumers to browse the Internet, stream music/videos, and more.
Rationale for selection of product group:	***Specify why has this product group been chosen for the IA study?*** Smart TVs are an interesting product group, as they are a connected radio equipment (RE) device in their own right. Since 2015, the trend is for replacing old TV sets with smart TVs, as they have become a device standard on the market: "smart TVs will be considered a household necessity in most markets" in the future.[90] The cost of buying smart TVs has been steadily decreasing in parallel[91] such that the sale of smart TVs and percentage of households in Europe with a Smart TV is steadily increasing.[92] A further justification for looking at Smart TVs as a product group is that studies have identified security vulnerabilities for this product, with differing levels of severity.
Case study overview and aims	***Comment on case study aims*** The aims of this case are to: • Highlight vulnerabilities in Smart TVs, and to consider the extent to which technical solutions are available to mitigate these. • Consider the extent to which the vulnerabilities identified are pervasive within the product group, or specific to certain models and manufacturers. • Review available technical solutions on the market to address vulnerabilities, and the nature of these e.g. general security by design and default principles, industry-led standards and technical standards developed by standards bodies etc. • Shed light on the costs and benefits of strengthening product security, specifically from a data protection and privacy / protection from fraud perspective. The case draws on secondary research and interviews. It should be noted that the research does not allow scope to test or comment on individual products. Rather, the aim is to identify the main types of vulnerabilities, and to categorise the impact of these from both a data protection and privacy perspective and a protection from fraud perspective.
Number of devices on European market and growth rate:	***Estimate number of devices on European market and % growth rate. Comment on baseline situation and projected demand.*** Overall, data on Smart TV uptake at EU-level is not up-to-date (most reliable source is a Eurostat study that dates back to 2016). Other research only considers certain regions in Europe or does not provide the full picture. Alternatively, a few Member States have conducted their own research on smart TV (at national-level). According to figures from Eurostat in 2016, Smart TVs are most prevalent in households in the Netherlands and the UK. At EU-level, 11% of Europeans watched

[90] Advanced Television, 2019, Forecast: Smart TVs 81% of total TV sales in 2024
[91] Frost & Sullivan as seen in: Council of Europe, 2016, Smart TV and data protection
[92] IHS Markit, 2018, TV market update, HbbTV Symposium, Berlin

Case study title:	Assessment of security vulnerabilities in Smart TVs.
	Internet-streamed TV or other video; only 4% browsed on the Internet; 3% accessed other apps (e.g. games, shopping) on a smart TV.[93] Another study by IHS Markit estimated that 50% of households had a smart TV in 2019 in Western Europe. [94] This is expected to increase to 63% by 2020. Ovum reports 269 million TV unit sales for 2024, of which 81% will be smart TVs.[95] **Figure 1: Smart TV shipments (2011-2016)**  *Source: NPD DisplaySearch* As shown in Figure 1, there is a clear tendency towards Smart TVs with user-controlled browsers, which allows consumers to browse the web or connect their TVs to the Internet.
Mapping of key stakeholders in product group:	***Brief bullets on stakeholders by type. Selected examples of individual firms that are leading manufacturers.*** • Smart TV distributors, traders, wholesalers • Smart TV subcomponent manufacturers (e.g. equipment manufacturer, audio-visual media service provider, online content and service providers) • Software manufacturers (e.g. operating systems) • Industry associations representing interests of Smart TVs The manufacturing process for smart TVs varies by brand, however all big brands design the product themselves and contract providers to assemble/deliver different components of the TV. Retailers then receive the device and sell it on. An important piece of the puzzle is the software: it varies by brand (popular software providers include: Roku, Android, etc.). Globally, Android is the most common operating system (OS). This is because smart TVs in China use Android or adapt it to create their own version of Android; in Europe, the most common OS is Tizen, which is used by Samsung, the market leader in Europe. Examples of the major manufacturers in the smart TV market: Samsung Electronics, LG electronics, Sony, Hisense, TCL, Skyworth, Panasonic, Vizio, among many others. In addition to basic software (i.e. OS), manufacturers can also integrate additional features/ connectivity platforms. Some examples include: • **Sony:** the company has a range of smart TVs that use Android's operative system. Special features include 4K HDR, which enhances gaming experience. Some models also build-in Google Assistant.

[93] Eurostat, 2016, How popular are smart TVs?
[94] IHS Markit, 2018, TV market update, HbbTV Symposium, Berlin
[95] Advanced Television, 2019, Forecast: Smart TVs 81% of total TV sales in 2024

Case study title:	Assessment of security vulnerabilities in Smart TVs.
	• **Samsung:** Some models come with Bixby Voice, a virtual assistant that helps find streaming & live TV shows through voice command. • **LG:** some of its latest models has Google Assistant built-in, allowing greater convenience for consumers that want to control smart home devices (e.g. smart lights, smart meters, etc.) Operating systems have the capacity to support TV steaming services, which are becoming increasingly popular amongst consumers (e.g. Netflix, Amazon Prime, etc.). There is evidence that smart TVs are also enhancing the TV's interactivity with these services. For example, the subscription-based streaming service Netflix, requires TV manufacturers to meet certain criteria to be considered 'Netflix recommended TVs'. To carry this logo, a Smart TV needs to fulfil 5 out of the 7 criteria set by Netflix (e.g. when the TV starts up, apps need to be ready to use straight away; a Netflix button on the remote control that turns on the TV and gets you straight to Netflix; or the Netflix app is easy to access from the icon on the TV menu).[96]
Type of data being collected (e.g. personal data and non-personal data) **How transmitted to manufacturer, technology provider or service provider *(e.g. which type of connected network, internet, other secure communications system)***	A global smart TV manufacturer confirmed that the only data they collect includes: the TVs IP address; the device ID and data on software updates (which provides information on whether the consumer has updated their device or not). Their security system covers three layers: applications, data and data transmission. Consumers can voluntarily register their device online, after which the manufacturer stores some data on the consumer. The manufacturer noted that overall, they try to collect as little data as possible from consumers, however, third-parties (e.g. software, applications, smart devices connected to the TV) all collect large amounts of data. If the manufacturer is playing a role in the collection and processing of personal data (i.e. integration of product software allowing data collection and sharing for commercial benefits), it is considered to be a data controller, which is covered by the GDPR. To understand the type of data that is being transmitted on a Smart TV, a study was conduct on a specific brand of Smart TV by the Council of Europe The Smart TV is generally equipped with a SMART hub, which is the heart of the device, allowing consumers to access apps and other smart functions. The Smart hub includes the following features:[97] **1) Voice recognition** To receive voice commands, the Smart TV has to be equipped with a microphone that will record sound from the surroundings of the device. Since the TV is recognising voices, it means that the TV is able to filter this data and translate it into a command. As such, the Smart TV is collecting and storing all words that are spoken near it. **2) Motion control and facial recognition** Smart TVs can also respond to gestures by way of facial recognition. Many TVs come with built-in cameras, which means images are recorded, allowing software to recognise and distinguish consumers' faces. **3) Account creation** Specific apps or streaming channels will require users to create a profile and to consent to their data being used. Although this is beyond the scope of the RED, this data is later used to make content suggestions or recommendations based on

[96] Norton (Symantec), 2019, What is a smart TV and the privacy risks of a smart TV
[97] Council of Europe, 2016, Smart TV and data protection

Case study title:	Assessment of security vulnerabilities in Smart TVs.
	viewing behaviour or response to previous advertising. Although users might expect services such as Netflix or Amazon Prime to use their data to improve their experience, they generally unaware that the Smart TV also collect data on viewing patterns. Since Smart TVs also ask users to create an account (i.e. an account with the manufacturer), different manufacturers in the supply chain are also collecting data on viewing habits. The Smart TV is equipped with a number of sensors that allow it to observe its surroundings, making it capable of collecting vast amount of data and potentially transmitting it via the Internet (including data on vulnerable populations, such as children). Other categories of data collected includes data about location, the device, content, data collected by applications, browsing data, viewing history, and voice service interactions. Some of this data is considered to be 'personal data' as defined by the GDPR. [98] In the context of Smart TVs, there are potentially several third-party controllers processing consumers' personal data, including: the equipment manufacturer, the digital and app platform provider, audio-visual media service provider, online content and service providers. When users accept to share their data with the manufacturer, it is not clear what type of data is being monitored or collected, or how it is being used. There is evidence (from the interview feedback) that built- in software also collects data on consumer viewing habits, in line with GDPR. Indeed, all manufacturers have to ask users to consent to their data being processed, however, consumers tend to be misinformed about how their data is being used (e.g. manufacturers could set users' profile settings to the most privacy-friendly option by default to protect consumers). In most cases, the declared purpose of data collection includes: [99] • Service provision (e.g. personalised content, advertising, etc.) • Product and service development • Marketing (e.g. profiling) • Security assurance (e.g. product maintenance) • Fraud prevention and investigation When users accept to share their data with the manufacturer, it is not clear what type of data is being monitored or collected, or how it is being used. There is evidence (from the interview feedback) that in-built software also collects data on consumer viewing habits. It is not clear whether this data is anonymised or not.
Security vulnerabilities in smart TVs ***(differentiate between latest generation products and older products on market)***	***To what extent are there risks associated with the product group? Ensure differentiation between general security vulnerabilities and vulnerabilities that could compromise data protection and privacy or lead to fraud (focus on two latter). When assessing security vulnerabilities, comment not only on device overall but on the specific elements of the product hardware (and any components), software, operating system.*** A research analyst with over 30 years in the industry, noted the following main vulnerabilities with Smart TVs: • <u>Software:</u> the analyst commented that "manufacturers are naïve about software and the Internet in general". The reduced frequency of security updates and the impossibility for users to find out if their smart TV has

[98] Article 29 Working Party, Working document on biometrics adopted on 1 August 2003; Opinion 3/2012 on developments in biometric technologies, adopted on 27 April 2012

[99] The International Institute for Academic Development, 2018, Joint conference on social sciences

Case study title:	Assessment of security vulnerabilities in Smart TVs.
	been compromised means TVs are vulnerable. A three to four year old device might no longer be able to get software/ firmware updates if these are discontinued by the manufacturer for older models. Moreover, sometimes, a product may be launched on the European market but then continue to be sold for a couple of years post-launch, even though newer models will have superseded the old model (with discounting to attract consumers). This means that some consumers may find that their "new" TV is only maintained through software and firmware updates for a couple of years after they bought it. Although this is dealt with under Art. 3(3)(i) rather than within the scope of this study, it has implications for Art. 3(3)(e) and 3(3)(f) as without updates a smart product risks becoming the weakest link in the chain. • Consumers may not realise the security implications. Even if consumers are able to access software/ firmware updates, they may not be aware that they need to keep their RE-connected devices up-to-date. • Hacking smart TVS: Researchers have proved that Smart TVs can easily be hacked, since the SSL is not encrypted. At the RSA Conference Europe 2013, researchers showed the lack of security in TV app stores, particularly since TVs ask for weak passwords (i.e. 4 digits, no capital letters). [100] A well-known manufacturer of a particular TV was found to be the only smart entertainment device that has a two-factor authentication system and that asks for a strong password. Since that time, more TVs have adopted this security approach but it is still not widespread. • Access to home network: Gaining access to the household's home network through the smart TV is possible. There are also risks of cybercriminals spying on individuals via cameras and microphones to gather sensitive data or private information on the consumer. A study revealed that smart TV users generally accept default security and privacy settings and authentication methods, making smart TVs vulnerable by default.[101] However, "the home network is only as secure as the weakest device connected to it" and smart TVs are unlikely to be the weakest point of entry as there are many other RE devices that are easier to break into, due to the fact that they use the same operating system or have no security measures installed. • Privacy & data protection: Smart TVs are able to track and profile individuals' viewing habits. There have been numerous scandals about tracking viewership and how this data is being processed by third-parties. Consumers are generally unaware about the data being collected and the risks associated with this process. • Connectivity to other devices: there have been questions about what data is being exchanged on the Smart TV when the manufacturer build-in other connectivity features (e.g. Alexa or Google Assist). Equally, there are issues about data usage when consumers voluntarily connect their TVs to other smart devices or external features in their homes. It is important to note that smart TVs cannot be heavily interacted with. This means that financial and cyber security risks (i.e. fraud) are low because it is difficult to load software or malware onto a Smart TV (although it is possible). For instance,

[100] Gai, A., et. al, 2018, Categorisation of security threats for smart home appliances
[101] Bitdefender, 2018, Studiu Bitdefender: Una din patru locuințe din mediul urban este smart. Televizoarele inteligente, cele mai folosite

Case study title:	Assessment of security vulnerabilities in Smart TVs.
	consumers are unlikely to browse the web or buy items through their Smart TVs – they will most likely use their laptop or smartphone.
Nature and extent of threat, likelihood and impacts of security vulnerabilities occurring	***Comment on the cybersecurity threat from a data protection and privacy / protection from fraud perspective. Also, the level of severity of the risk, probability of it occurring and the impacts if it did occur. E.g. concept of low-probability, high-impact, or conversely high-probability, low-impact etc.*** As mentioned in the previous question, the probability of fraud or cyber security breaches is not high for Smart TVs. Although vulnerabilities exist, there are weaker RE-connected devices in people's households (i.e. Bluetooth connected kettles or fridges) that are easier targets. Compared to other cheap and poor-quality RE devices, Smart TVs are harder to break into. Indeed, hackers or fraudsters need to choose the brand of the Smart TV they wish to break into (i.e. Smart TVs use different software). This makes Smart TVs relatively safer but not immune to cyberattacks. Also, it is important to note that there are not many Smart TVs (yet) on the European market, especially compared to the USA or Asia. There is generally only one Smart TV per household, and consumers frequently do not connect their TVs to their home network. Academic literature explores numerous real and proof-of-concept attacks, including the vulnerability of software-based attacks; the possibility for neighbours and broadcasting stations to track users; fake analytics (i.e. falsifying numbers of viewers for a show to influence its continuation); or arbitrary video display hijacking the users' screen.[102] The biggest concern with Smart TVs is the business model of the industry as a whole: companies are focused on finding new revenue streams, instead of protecting users' data and privacy. There is evidence that consumers can be monitored through their Smart TVs (i.e. through microphones, cameras, etc.) and that data is being actively processed. Interview feedback noted that some stakeholders in the manufacturing supply-chain (i.e. software, OS, etc.) sell data and share percentages of revenue with the Smart TV brand. The interviewee did note that smart TV manufacturers are probably not deliberately harvesting personal data. However, Smart TVs are designed to permit data oversharing by default.[103] Manufacturers may also integrate software that track viewing habits (e.g. by asking consumers if they consent to their data being used to improve services) or monitoring habits through integrated microphones. An academic and expert on cyber security explained that despite the advantages of a smart TV (i.e. interactivity, recommendations based on views, etc.), many back-door channels are opened due to the TV being connected to the Internet. Smart TVs are continuously transmitting data, whether this is personal data, credentials, viewer history or other, it is possible to track and identify users.
Extent to which security vulnerabilities and data protection and privacy issues covered by existing legislation	***Extent to which security vulnerabilities are covered in existing legislation.*** ***Data protection and privacy / protection from fraud. Measures to overcome any compromise of personal data.*** One interviewee noted that the TV industry is largely reactive, rather than proactive. Since it is a highly competitive business, the industry is actively pursuing new revenue streams (i.e. selling data to third parties or advertisers). Android (as an operating system) has not taken measures to overcome data protection issues.

[102] The International Institute for Academic Development, 2018, Joint conference on social sciences
[103] The International Institute for Academic Development, 2018, Joint conference on social sciences

Case study title:	Assessment of security vulnerabilities in Smart TVs.
	The issue is that consumers expect the TV brand to protect data/privacy, but the industry expects software companies to take responsibility for GDPR compliance. Since Smart TV and online media enables precise monitoring of online media consumption (i.e. viewing habits), this raises new practical challenges for EU regulation. Indeed, data protection laws addresses the legality of monitoring individual media consumption and the use of personal data (e.g. to make personalised recommendations). However, tracking viewer behaviours and the personalisation of content affects individuals' freedom to receive information and pluralism – this has so far not been reflected in current legislation.[104] The extent to which data protection extends to viewer habits and interactions with smart TVs is unclear. There is evidence that smart TVs are profiling users through the collection of large amounts of data; the processing of such data is covered by GDPR. Although consumers are asked to consent to such the processing of their data, the extent to which they are subject to tracking and targeting is also not transparent. While third-parties need to ensure that the data they seek to commercialise is collected and processed in accordance with the GDPR requirements, there are ethical questions as to the processes by which data is sold on by economic operators to other actors in the value chain. One issue for example is whether it is sufficiently clear to the end consumer that their data is being collected and then exploited for commercial purposes leveraging the power of big data. Here, the issue of consent as to how the data subject's data will be used is key. Consumers are protected by the GDPR but it is unclear without evidence through evaluations of the GDPR's implementation at this stage how far third parties collecting and processing such data are fully GDPR-compliant.
Stakeholder views on the nature and extent of security vulnerabilities:	In terms of the nature and extent of security vulnerabilities, stakeholders shared the following information: • Consumers tend to keep their TVs for a long time, so if manufacturers no longer updating the software, there are moderate to high security risks. • Interviewees highlighted the apathy of consumers when faced with cybersecurity and privacy. Consumers often do not take the necessary steps to protect their devices, which increases the risk of security incidents. For example, consumers tend to accept default password and authentication measures, which makes smart TVs vulnerable by default. However, it is important to note that smart TVs are unlikely to be the weakest point of entry, as there are many other weak links (i.e. low-cost IoT devices). The risks of hacking smart TVs is therefore moderate to low: although research suggests that they can easily be hacked, smart TVS cannot be heavily interacted with: it is difficult to load software or malware onto these smart devices.
Technical solutions:	Based on interview feedback, there are limited technical solutions available or being developed to address vulnerabilities. There are however some exceptions among top manufacturers. One large manufacturer for example has started introducing virus and malware tracking on their Smart TVs. They also published communications reminding consumers to check their TVs security and update the software. Other manufacturers are using multi-factor identification or adding biometrics – however, the latter raises other security concerns.

[104] Irion, K., e.t. al, 2017, Smart TV and the online media sector: User privacy in view of changing market realities, Telecommunications Policy, Volume 41, Issue 3, April 2017, Pages 170-184

Case study title:	Assessment of security vulnerabilities in Smart TVs.
	Further to this, some software companies are taking a proactive approach and take data protection/ privacy more seriously. For example, they are more transparent about how they use consumer data.
Costs and benefits of addressing security vulnerabilities:	In terms of costs, a large manufacturer noted that the more operations are run locally, the higher the costs (e.g. the storage of data). The cost of setting up organisational structures for security by design is very high. Since the HQ of the large manufacturer (that was interviewed) is in Asia, compliance and security is coordinated at a global scale (costs are shared). Experts on EU regulation provide feedback to the global compliance teams (i.e. on digital single market, or new regulation), so these departments are active all the time. If the EU were to activate a delegated act, this leads to a deviation of international standards. This is particularly challenging, as devices are built at global level, and then configured to each region, but if the EU deviates too much, it is more costly. Security standards that are not aligned is a major challenge for manufacturers.
Overall findings and lessons learned:	• Based on interview feedback, the industry doesn't have the right approach to data protection and privacy: manufacturers started producing Smart TVs in about 2012-2013 without thinking about the impacts and implications of data collection. • The number of Smart TVs sold in Europe is still relatively small and fragmented (unlike smartphones), but it is likely that in 1-3 years, the majority of Europeans will have a smart TV. • Although our research found that Smart TVs are at present not a major target for cybercriminals, the fact that they do not have basic security measures means they will become more and more interesting to target in the future. • The potential risks resulting from the over-collection of data on Smart TVs includes the mass aggregation of personally-identifiable information; invasive targeted advertising; and loss of autonomy, among others. • A possible explanation is that legislation on data protection (mainly the GDPR) does not satisfy the business models of Smart TV companies. In the context of the complex Smart TV supply-chain, it is unclear who is responsible or held accountable for aspects relating to compliance. The extent to which GDPR and the future e-Privacy Regulation covers the interactivity of smart devices across the value-chain is also unclear. • Traditional media regulation, such as the Audiovisual Media Services Directive did not include points about interactivity and privacy, suggesting that GDPR is crucial for the protection of individuals' digital rights on smart TVs. • There is evidence that a large amount of data is being collected by Smart TVs and transmitted to manufacturers and other third parties, without consumers understanding how their data is being used. • Indeed, companies are not transparent about their data collection practices. Smart TV users are left in the dark about how their device gathers data and what companies on the supply chain are doing with it. • New developments in the Smart TV market are potentially dangerous for the future in terms of data protection and privacy. Hybrid Broadcast Broadband TV (HBB TV) will soon become the norm in Europe, whereby advertisements shown on TV will be personalised and adapted to data received from consumer interaction with smart TVs (profiling based on demographics, neighbourhood, viewing habits, etc.)

Case study title:	Assessment of security vulnerabilities in Smart TVs.

Literature consulted: *Mention any studies that have tested product group in question. Wider research, blogs and articles, reports by national authorities / MSAs*

Data / research on market size and structure

- Advanced Television, 2019, Forecast: Smart TVs 81% of total TV sales in 2024
- Eurostat, 2016, How popular are smart TVs?
- Frost & Sullivan as seen in: Council of Europe, 2016, Smart TV and data protection
- IHS Markit, 2018, TV market update, HbbTV Symposium, Berlin
- Norton (Symantec), 2019, What is a smart TV and the privacy risks of a smart TV

Relevant literature providing examples of Smart TV security vulnerabilities and flaws:

- Article 29 Working Party, Working document on biometrics adopted on 1 August 2003; Opinion 3/2012 on developments in biometric technologies, adopted on 27 April 2012
- Council of Europe, 2016, Smart TV and data protection
- Irion, K., e.t. al, 2017, Smart TV and the online media sector: User privacy in view of changing market realities, Telecommunications Policy, Volume 41, Issue 3, April 2017, Pages 170-184
- Norton (Symantec), 2019, What is a smart TV and the privacy risks of a smart TV
- Bitdefender, 2018, Studiu Bitdefender: Una din patru locuințe din mediul urban este smart. Televizoarele inteligente, cele mai folosite
- Gai, A., e.t. al, 2018, Categorisation of security threats for smart home appliances
- Business Insider, 2019, There's a simple reason your new smart TV was so affordable: It's collecting and selling your data, and serving you ads

Interviews:

- Research analyst **(interviewed)**
- University of Computer Science and Engineering in the US **(interviewed)**
- TV manufacturer's Association **(interviewed)**
- Top 10 global manufacturer **(interviewed)**

7. Product case study 6 – Smart Watches

Case study title:	Assessment of security vulnerabilities in smart watches and wearable devices that could compromise data protection and privacy.
Product group and short definition:	Smart watches are a popular and growing wearable device. They are a significant component in the increasing range of wearable computing devices which have embedded processing units. The technology is based on permanent communication between user and device; "*as a rule, they track individual data throughout the day or even for 24 hours*": a "*wearable computer is more personal device than laptop or smartphone as it is worn on the body, customized for a range of uses by humans and they gather individual, often confidential information*.[105]"
Rationale for selection of product group:	Smart watches have been chosen as one of the case studies as: 1) Wireless communication is necessary for wearable devices to transmit data to proximate devices. This brings up many problems of transmission and software control.[106] 2) Smartwatches have a wide range and a growing set of functions. They are designed, either on their own or when paired with a smartphone, to provide features such as connecting to the internet, running mobile apps, making calls, messaging via text or video, checking caller ID, accessing stock and weather updates, providing fitness monitoring capabilities, offering GPS coordinates and location directions, and more.[107] 3) The use of smart watches and wearables has grown and is likely to increase in the future. "*smartwatches represent the most popular type of wearable devices… Empirical results reveal perceived usefulness and visibility as important factors that drive intention, suggestion that smartwatches represent a type of 'fashnology' (i.e., fashion and technology)*"[108].
Case study overview and aims	The aims of this case study are to: • Examine the range of data which is transmitted by smart watches • Highlight vulnerabilities • Consider the extent to which the vulnerabilities identified are pervasive within the product group • Review available technical solutions on the market to address vulnerabilities and the nature of these • Report any identified costs and benefits of strengthening product security, specifically from a data protection and privacy / protection from fraud perspective The case study draws on secondary research, marketing and opinions from experts. The aim is to identify the main types of vulnerabilities and to categorise the impact of these from a data protection and privacy and protection from fraud perspective.

[105] Both quotes are from Mikhalchuk, D., (2018).
[106] Shivram, S., (2017).
[107] Stroud, F., (no date).
[108] Chuah, S., et al. (2016).

Case study title:	Assessment of security vulnerabilities in smart watches and wearable devices that could compromise data protection and privacy.

Number of devices on European market and growth rate:

In 2016, Bluetooth headsets were the largest segment of the wearables industry, followed by fitness bands and **smartwatches**[109].

Looking at the sales of wearable devices, Statista report and forecast the following number of wearable devices:[110][111]

Year	Western Europe	Central and Eastern Europe	Total
2015	16.75 million	5 million	21.75 million
2017	88 m	28m	116m
2022	192m	68m	260m

Source: Statista

An alternative perspective for relating the use of smart watches to the population is the Statista estimates and forecasts of wearable devices in the US: in 2018 20.3% of adults have a wearable device and by 2022 this would grow to 25.3%[112]. The application of these to information from Eurostat gives the potential for the 430.9m people in the EU27 Member States aged 15+ to have 89 million wearable devices[113].

Gartner[114] have provided forecasts of the use of wearable devices worldwide (shown in table below). These forecasts a 121% increase in the spending on smartwatches between 2018 and 2021 and an increase of 35% over the same period for sports watches.

Worldwide Wearable Devices End-User Spending by Type, 2018-2021 (Millions of Dollars)

Device Type	2018	2019	2020	2021
Smartwatch	12,412	17,047	22,803	27,388
Head-mounted display	5,354	7,183	10,609	15,501
Ear-worn	6,780	7,885	8,716	9,927
Sports watch	3,647	4,121	4,555	4,912
Wristband	3,405	3,194	3,115	3,055
Smart-clothing	848	1,151	1,746	2,202
Total	**32,446**	**40,581**	**51,545**	**62,985**

Source: Gartner 2019.

Mapping of key stakeholders in product group:

The top ten Wearable Technology Companies in 2018 have been listed by global market research firm Technavio[115]. They are given ranked by size.

Company	Headquarters	Key wearable products
Apple	U.S.	Apple Watch Series and AirPods
Samsung	South Korea	Gear S3 Frontier, Gear Sport, Gear Fit2 Pro, Gear IconX, and Samsung Gear VR
FitBit	USA	FitBit Versa, FitBit Ionic, FitBit Charge 3, FitBit Flex 2, and FitBit Ace

[109] Liu, S. (2019a).
[110] Liu, S. (2019b).
[111] Clarity has been sought from Statista on the geographical definition. It is unlikely that Western Europe and Central and Eastern Europe together amount to the whole of the EU as it is possible that northern Europe has been omitted.
[112]Liu, S. (2019c).
[113] Eurostat (2017).
[114] Gartner 2019.
[115] Technavio (2018).

Case study title:	Assessment of security vulnerabilities in smart watches and wearable devices that could compromise data protection and privacy.

Xiaomi	China	Mi Band 3, Mi Band – HRX Edition, and Mi VR Play 2
Osterhout Design Group (ODG)	USA	R-7, R-8, and R-9 smartglasses
Garmin	USA	Fenix 5 Plus Series, vivomove HR, vivosport, Approach S60, and quatix 5 Series
HUAWEI	China	HUAWEI TalkBand B5, HUAWEI FIT, HUAWEI WATCH 2, and HUAWEI Band 2
Polar Electro	Finland	Polar Vantage V, V800, M600, Polar A370, and H10 Heart Rate Sensor
Vuzix	USA	Smart Glasses, Video Headphones
Kopin	USA	Voice Extraction Technology

With specific reference to smartwatches, work was commissioned by the Norwegian Consumer Council (NCC) on smartwatches for children[116]. The devices tested were bought in Norway and were named as: Gator 2, Tinitell, Viksfjord, and Xplora.

Type of data being collected

Data stored on phones includes personal health data on users and geo-locational data.

Chordas, L. (2019)[117] writes about consumer and medical wearable devices "*opening up a new data portal for health insurers, but many are still grappling with how to use that information*". It is noted that smartwatches and wrist-worn fitness trackers, smartphone health apps and consumer and medical wearable devices, can now measure just about every health metric, including heart rate, blood pressure, respiratory rate and blood glucose level. They can also detect and monitor diseases such as chronic obstructive pulmonary disease, cystic fibrosis and diabetes. *"Most carriers are still grappling with regulatory constraints, data privacy concerns and questions about the accuracy of information generated by wearable devices*". [118]

How transmitted to manufacturer, technology provider or service

Further types of personal data collected includes geo-locational data, which may, if unauthorised access is gained, pose a risk to the user, especially children.

An issue around the type of data stored by smartwatches is that whilst they are typically devices that are used in connection with smartphones and app's on the phone, they store data in their own right.

In *Communications for Wearable Devices* Shivram Tabibu (2017) reviews basic wearable deployments and their open wireless communications[119]. The report notes that there are many devices operating in the localized region or within human body contact, such as the smart phone watch, wearable computing devices, Radio-frequency identification (RFID) and health care monitoring devices. The RF band is shared with mobile / cellphones, Wireless Local Area Networks, Personal Area Networks, satellite communications and many other applications.

As a generalisation of the smartwatch connection: "*most Smartwatches operate via Bluetooth 4.0, also known as Bluetooth Low Energy. The connection to another device (such as a laptop, tablet or phone) needs to be in network proximity, this enables complete companion functionality with the device*".

One of the further problems is that data transmitted via smartwatches is often sent unencrypted. A further problem – examined in the next sub-section - is that data is

[116] Sand, H. et al. (2017)
[117] Chordas, L. (2019).
[118] Chordas, L. (2019).
[119] Tabibu, S. (2017).

Case study title:	Assessment of security vulnerabilities in smart watches and wearable devices that could compromise data protection and privacy.
	often stored locally on the device itself, but if it is stolen, it cannot be erased thereby exposing users to the risks of personal data breach.
Security vulnerabilities in smart watches	A concern over the data collected through smart watches is from its use for other purposes. *"Politicians and privacy campaigners have called for Google's $2.1bn deal for Fitbit to be blocked, over fears the search giant will feed its growing healthcare business with the data of the 27 million people who use Fitbit fitness trackers… the takeover, if it is passed by regulators, also gives Google access to a huge trove of heart rate, activity and sleep data which it could use to create a new range of personalised health services."* (Kuchler, H, 2019)[120]. The Mozilla Foundation is a non-profit organization which has the aim to protect the internet as a global public resource. In November 2019 it released a guide to shopping for safe, secure connected products ("*Privacy Not Included Buyer's Guide."[121]. The guide reviews the privacy and security of 76 popular connected products. For this case study the assessment of 10 wearable devices from five companies is included.

Device	Encryption	Security updates	Strong password	Manages vulnerabilities	Privacy policy
Apple Watch 5	Yes	Yes	Yes	Yes	Yes
Fitbit Ace 2	Yes	Yes	N/A	Yes	Yes
Fitbit Charge 3 Tracker	Yes	Yes	N/A	Yes	Yes
Fitbit Versa 2	Yes	Yes	N/A	Yes	Yes
Fitbit Inspire HR	Yes	Yes	N/A	Yes	Yes
Garmin Vivoactive Series	Yes	Yes	N/A	Yes	Yes
Garmin Vivosmart 4	Yes	Yes	Yes	Yes	Yes
Huawei Band 3 Pro	Yes	Yes	N/A	Yes	Yes
Motiv Ring	Yes	Yes	Yes	Yes	Yes
Samsung Galaxy Fit	Yes	Yes	Yes	Yes	Yes

In 2015, Trend Micro issued a report which highlighted a major issue with the security of smartwatches: physical protection of sensitive data. Physical protection mechanisms need to complement the prevention of online device penetration. Otherwise, the devices remain insecure. Trend Micro found that *"smartwatches save data locally when out of range from their associated smartphone. This effectively means that, if a watch were to be stolen, the thief would have instant access to all the data saved onto that device, including messages, contact details, photos, etc.".* [122]

A further study also confirmed that vulnerabilities linked to smartwatches are not confined to risks linked to them being connected to the internet, but also to the lack of physical device security. For example, *"physical device protection across all*

[120] Kuchler, H. (2019).
[121] Mozialla (no date A).
[122] See Micro Trend report on SmartWatch security - https://blog.trendmicro.co.uk/security-flaws-common-on-most-popular-smartwatches/#more-363 and also article about this report https://www.scmagazineuk.com/smartwatches-arent-so-clever-when-comes-security/article/1479523

Case study title:	Assessment of security vulnerabilities in smart watches and wearable devices that could compromise data protection and privacy.
	smartwatches was found to be poor, with no authentication via passwords or other means being enabled by default. This would enable free access if the wearable was stolen. All devices apart from the Apple Watch failed to contain a timeout function, meaning that passwords had to be activated by manually clicking a button". Ensuring improved device security was found to be a **trade-off between ensuring usability and strong UX** (user experience) on the one hand, and **high levels of security** on the other. For example, the report by Micro Trend on smartwatch security vulnerabilities noted that "the lack of authentication features can make devices appear easier to operate, but the risk of having personal and corporate data compromised is much too big of an issue to forget about". [123] Despite having better security features than some of the Android models tested in a 2015 study by Trend Micro, the Apple Watch was found to contained the largest volume of sensitive data. [124] Concerns have been expressed about the use of smartwatch devices designed for children: "*Nobody needs a smartwatch. But for parents, they can be tempting. Loaded with GPS and a cellular data chip, they can both track a child and offer them a way to communicate in emergencies*.[125]" Parents can track the movements of their children in real time through a companion mobile app. However, a report by the Norwegian Consumer Council (NCC) on smartphones for children in 2017 identified a number of **security vulnerabilities**. [126] The NCC's report points to tests done by Mnemonic that have uncovered critical security flaws in three smartwatch apps and devices. *"Two of the devices have flaws which could allow a potential attacker to take control of the apps, thus gaining access to children's real-time and historical location and personal details, as well as even enabling them to contact the children directly, all without the parents' knowledge. "* [127] A further problem related to in **adequate levels of data privacy.** *"Inadequate and unclear user terms deny consumers their basic consumer and privacy rights when engaging with these products. Only one of the services actually asks for consent to data collection, none of them promise to notify users of any changes to their terms, and there is no way to delete user accounts from any of the services."*
Nature and extent of threat, likelihood and impacts of security vulnerabilities occurring	A number of studies have been carried out to examine the extent to which personal data can be accessed or transferred from smart watches or wearable devices. These studies illustrate some of the weaknesses in the protection of personal data. Lee, Yang, and Kwon (2018)[128] examine data security problems that can occur in smartwatch device pairing, coining a new term "data transfusion". Their research includes a study of data extraction from devices such as in Android Wear, watchOS, and Tizen platforms. The study reveals that large amounts of sensitive data are being transfused without sufficient user notification. They were able to extract some of following data from the devices they studied: • Contact and SMS/MMS messages: the user's own contact information and SMS/MMS messages as the data was unencrypted. • Contact information: it was stored unencrypted in SQLite database file

[123] https://blog.trendmicro.co.uk/security-flaws-common-on-most-popular-smartwatches/#more-363
[124] https://blog.trendmicro.co.uk/security-flaws-common-on-most-popular-smartwatches/#more-363
[125] Wilson, M. (2017)
[126] Research by the Norwegian Consumer Council (NCC) in study #WatchOut, Analysis of smartwatches for children, October, 2017, https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-october-2017.pdf
[127] Idem. Pg 3.
[128] Lee, Y., Yang, W., and Kwon T., (2018).

Case study title:	Assessment of security vulnerabilities in smart watches and wearable devices that could compromise data protection and privacy.
	• Hashed lock pattern: the hashed lock pattern was extracted and decrypted • Wi-fi ssid/password: the extracted Wi-Fi connection information was accessed using a paired smartphone. The revealed access point was connected with the acquired Wi-Fi password to different devices, and the connection was successfully established. • Fitness data: was extracted with a linked additionally installed app. The data contains GPS location, speed, direction, and time-stamp values. Lee, Yang., and Kwon. (2018) also provide links to related publications which examined data extraction risks. Kim, J and Youn, J.M. (2017) examined threats of password pattern leakage using smartwatch motion recognition sensors and showed the threat of sufficient leakage of users' password patterns through the motion recognition sensors embedded in smartwatches: "*Most smartwatches are provided with motion recognition sensors to expand the functionality and to overcome the limitations of hardware in smartwatches. However, users' passwords can be sufficiently leaked through these motion recognition sensors.*" [129]
Extent to which covered by existing legislation	The Bundesnetzagentur[130] prohibits the sale of children's watches that have an "eavesdropping" function. The regulation is focussed on children aged between 5 and 12. The concern is that "*the watches have a SIM card and limited telephony function that are set up and controlled using an app. …The user can then eavesdrop on the wearer's conversations and surroundings*"[131]. Relevant legislation outside the European Union was identified in some articles. For example, Bodin, Jaramillo, Marimekala. and Ganis. (2015)[132] refer to the US HIPAA privacy rules "*Acceptance of Smartwatch in areas such as health care industries, where regulations such the HIPA act makes it much more difficult for easy acceptance of network devices due to security and data privacy concerns.*[133]" However there are also concerns that the level of protection in the US is not sufficient: "*what is the United States doing about it?* [Privacy and the Internet of Things] *Nothing. We know that U.S. regulatory authorities like the FCC*[134] *are quite lax when it comes to privacy, in the USA is not sufficient*" (Diaz, J. 2017). Wilson, M. (2017) gives the gave the view on the investigation by Sand, H. et al. (2017) for the Norwegian Consumer Council (NCC): "*Crucially, none of the investigated watches allowed you to delete your child's data or ensured that marketers couldn't use that data to sell something to your child. Nor did they make it clear where all of this data was being stored. These practices aren't just crude or careless; depending on a country's privacy laws, they can actually be illegal*".

[129] Kim, J. and Youn, J.M., (2017).
[130] The Bundesnetzagentur is responsible for the application of EU Directives 2014/53/ EU (RED) and 2014/35/EU (EMC Directive) in Germany, transposed into national law by the EMVG (Elektromagnetische-Verträglichkeit-Gesetz) and the FuAG (Funkanlagengesetz). The European regulatory framework for product marketing requires EU Member States to carry out efficient market surveillance to protect consumers against unsafe products and products – also from third countries – not meeting the essential requirements. Source: https://www.bundesnetzagentur.de/EN/Areas/Telecommunications/Companies/Technology/Technology_node.html
[131] Homann, J., (2017)
[132] Bodin, W. K., Jaramillo, D., Marimekala, S.K. and Ganis, M. (2015).
[133] HIPAA is Health Insurance Portability and Accountability Act of 1996. See "Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule")" https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
[134] FCC: Federal Communications Commission. https://www.fcc.gov/

Case study title:	Assessment of security vulnerabilities in smart watches and wearable devices that could compromise data protection and privacy.
Stakeholder views on the nature and extent of security vulnerabilities:	In 2015 Computer Business Review gives reaction from 5 cybersecurity experts on Smartwatch security failings[135]. • **Symantec, Sian John, Chief Security Strategist EMEA[136]** "*There are a few basic security precautions to help guard against the risk of exposing personal and self-tracking information when using these devices including the use of stronger passwords, not reusing the same user name and password between different sites and by using a device-based security solution on your mobile device if available*." • **Bitdefender, Alexandru Catalin Cosoi, Chief Security Strategist** "*All smartwatches, regardless of their brand, are exposed to security vulnerabilities. To enhance security, manufacturers need to consider encrypting communications in transit, securing mobile interfaces from account enumeration and providing regular firmware updates*. "*Users should do their part by enabling two-factor authentication and locking their smart devices with complex passcodes to prevent unauthorised access*." • **Good Technology, Phil Barnett, GM of EMEA** "*Many users will be blindly adding their new watches to mobile devices that hold a wealth of corporate information, creating a potential security vulnerability for their employers. With native Mail and Calendar applications sending alerts and notifications to the watch by default, even more devices will have access to corporate information, potentially putting more important data at risk*. "*One way to ensure enterprise data is secure on smartphones, tables and wearable devices is keeping it in separate, encrypted containers.*" • **KPMG, Matt White, SM for cyber security** "*Many of the watches (and other wearable technologies) use 'device pairing' along with pin/password to provide authentication, but this alone provides limited protection form a serious assailant. As with many security conversations, the level of security is a recipe of convenience, user experience and security*." • **Accellion, Paula Skokowski, CMO[137]** "*From a technical perspective, IT and security teams need to ensure that employees have approved apps for securely accessing and sharing content on all the types of devices they use to do their work including laptops, smartphones, tablets, desktops and wearables.* "*Access to enterprise content should only be allowed via approved apps that include the following security features.*" As the Gartner 2019 report on possible future spending indicates, smartwatches can be identified as separate from other wearable IoT devices. However, many of the security issues apply across many different devices. The following examples on the nature and extent of security vulnerabilities can apply to smart watches. In 2019 a review article, Mobile Devices and Health, by Ida Sim, in the new England Journal of Medicine[138] concluded that "*With respect to privacy and autonomy, the potential threats are particularly worrisome. Mobile health technologies will increasingly connect to the Internet of Things, in which, like a "one-way mirror," our*

[135] Vinod, (2015).
[136] Europe, the Middle East and Africa
[137] Chief Marketing Officer (CMO) - Mobile Information Security SaaS
[138] Sim,I., (2019) page 964

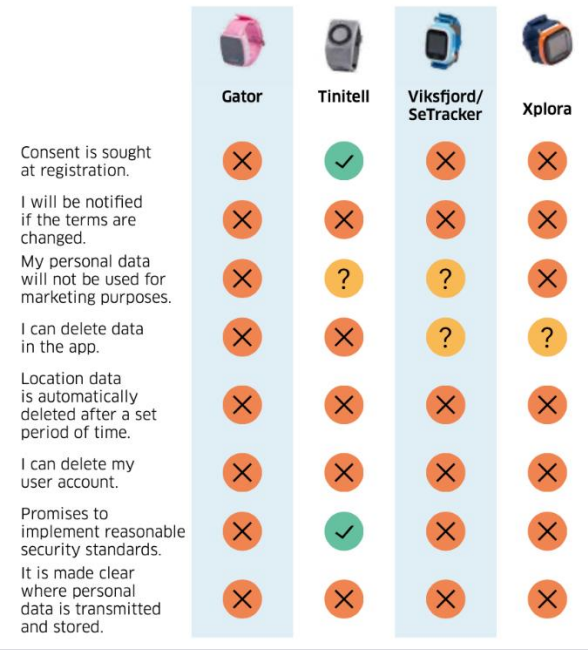
Case study title:	Assessment of security vulnerabilities in smart watches and wearable devices that could compromise data protection and privacy.

virtual bodies and behaviour will be visible on a grand scale for purposes to which we have not directly consented. When personal health and non-health data co-mingle in the cloud, companies and governments may access physiological biomarkers to monitor employee stress in the workplace, or marketers may offer us only certain products at differential prices based on our health history. Coupled with algorithms that are not in the public domain, these approaches could deliberately or inadvertently reinforce and entrench existing biases against disadvantaged groups, and incautious deployment of mobile health technology could potentially result in loss of privacy and autonomy amounting to net harm to patients".

Rouven-B. Wiegard & Michael H. Breitner carried out research to investigate the readiness of customers to adopt Pay-As-You-Live (PAYL) services using wearable technology by comparing perceived privacy risks and perceived benefits[139]. In a (PAYL) service, insured track activities, transfer current data on the lifestyles of users, who receive rewards from their insurance companies. The research found that information sensitivity has the greatest impact on perceived privacy risk for customers. Many of the respondents to their survey did not feel comfortable with the type of information wearables collect from them. Furthermore, they felt that the gathered data are very sensitive and that it is too risky to disclose their personal health information to insurance companies.

Additionally, regulatory expectations have been verified to positively influence perceived privacy risk. Respondents believe that the law should protect them from the misuse of personal health data and regulate the way in which insurance companies collect, use, and protect private information. Since data transmission is defined by the wearable manufacturer or app service provider, customers tend to feel insecure using wearable devices. It is possible that the success of services such as PAYL can be ensured if laws regulate the boundaries of data deployment and data transmission.

The report to the Norwegian Consumer Council (Sand, H. et al. (2017)) shows the main terms and conditions for users for the smartwatches for children they tested.



Source: Sand, H. et al. (2017), Norwegian Consumer Council

[139] Wiegard, RB. & Breitner, M.H., (2019).

Case study title:	Assessment of security vulnerabilities in smart watches and wearable devices that could compromise data protection and privacy.
Technical solutions:	The following ways are suggested in the Mozilla review as minimum security standards; "basic steps every company should take to protect consumer privacy"[140]. **Encryption** Data sent between a device and an app can be protected with strong encryption. For security the product must use encryption for all of its network communications functions and capabilities. This ensures that all communications are not eavesdropped or modified in transit. The product must also use encryption at rest to ensure that customer data is protected in storage. **Security updates** Updates can be pushed automatically when a device is paired with the companion app. The product must support automatic updates for a reasonable period after sale, and be enabled by default. This ensures that when a vulnerability is known, the vendor can make security updates available for consumers, which are verified and then installed seamlessly. Updates must not make the product unavailable for an extended period. **Strong password** If the product uses passwords for remote authentication, it must require that strong passwords are used, including having password strength requirements. Any non-unique default passwords must also be reset as part of the device's initial setup. This helps protect the device from vulnerability to guessable password attacks, which could result in a compromised device. **Proactive management of security vulnerabilities** The vendor must have a system in place to manage vulnerabilities in the product. This must also include a point of contact for reporting vulnerabilities or an equivalent bug bounty program. This ensures that vendors are actively managing vulnerabilities throughout the product's lifecycle. A good practice is that some companies run a so-called "bug bounty" program, especially in the US, – whereby those that identify security issue and disclose it responsibly may be paid at a company's discretion. This applies across a number of internet-connected products, such as routers, and isn't specific to smart watches. **Privacy policy** The product must have privacy information that applies specifically to the device, not a generic privacy policy that is written to cover just the company web properties. Additional privacy considerations include how data is shared with third parties, whether data can be deleted, and the readability of the privacy information. In their paper "Data Transfusion: Pairing Wearable Devices and Its Implication on Security for Internet of Things" Lee, Y., Yang, W., and Kwon T. (2018) identify a number of measures which could be undertaken to make smartwatches more secure. These include • Volatile transfusion: if a smartwatch is isolated, transfused data should be removed from the smartwatch after a certain amount of time according to the descending order of the priority. When the original user returns and wears the smartwatch again, the data removed is re-transfused. This can be called volatile transfusion, which enables safe data deletion when the device is separated from its user or the host device.

[140] Mozilla, (no date).

Case study title:	Assessment of security vulnerabilities in smart watches and wearable devices that could compromise data protection and privacy.
	• Notification inducing active response: the lack of notifications is serious from security and privacy perspectives, a solution would be an explicit notification message to the user regarding data transfusion of high-priority data.
Costs and benefits of addressing security vulnerabilities:	No feedback on costs has been received.
Overall findings and lessons learned:	This case study illustrates: • The wide and growing range of personal data used by smart watches and wearable devices • A number of areas of weakness which allow access to this data • Public views of needed protection of personal data • Possibilities of assessing some aspects of weakness and initiating a classification or ranking system

Literature consulted:

In order to help follow links between material used and where it came from the references have been put as footnotes where they are used. The literature which is used comes from a wide range of sources including peer reviewed journals, journals of specific interest to those who work in an area, information released by marketing companies who publish sector wide information and comment.

- Bodin, W. K., Jaramillo, D., Marimekala, S.K. and Ganis, M. (2015). Security Challenges and Data Implications by using Smartwatch devices in the Enterprise. IEEE. [Viewed 10th December 2019]. Available from: https://ieeexplore.ieee.org/document/7338164?section=abstract
- Chordas, L. (2019). Weighing in on Wearables. Ambest. [Viewed 10th December 2019]. Available from: http://news.ambest.com/ArticleContent.aspx?pc=1009&altsrc=158&refnum=284675
- Chuah, S. et al. (2016). Wearable technologies: The role of usefulness and visibility in smartwatch adoption. Computers in Human Behavior. 65. 276-284
- Diaz, J. (2017). When Is The U.S. Going To Ban The Internet Of Things For Children? Fast Company & Inc. [Viewed 2nd January, 2020]. Available from: https://www.fastcompany.com/90147796/dont-buy-your-kid-a-smart-watch
- Eurostat (2017). People in the EU - statistics on demographic changes. Eurostat. [Viewed 10th December 2019]. Available from: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=People_in_the_EU_-_statistics_on_demographic_changes#EU_population_structure_and_historical_developments
- Goasduff, L. (2019). Gartner says Global End-user Spending on Wearable devices to Total $52 billion in 2020. Gartner. [Viewed 2nd January, 2020]. Available from: https://www.gartner.com/en/newsroom/press-releases/2019-10-30-gartner-says-global-end-user-spending-on-wearable-dev
- Homann, J., (2017) Bundesnetzagentur takes action against children's watches with "eavesdropping" function. . Bundesnetzagentur. [Viewed 2nd January, 2020]. Available from: https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2017/17112017_Verbraucherschutz.html
- Kim, J. and Youn, J.M., (2017). Threats of Password Pattern Leakage Using Smartwatch Motion Recognition Sensors. Symmetry 2017, 9, 101
- Kuchler, H. (2019). Calls for Google's $2.1bn Fitbit deal to be blocked over data fears. Irish Times. [Viewed 10th December 2019]. Available from: https://www.irishtimes.com/business/technology/calls-for-google-s-2-1bn-fitbit-deal-to-be-blocked-over-data-fears-1.4091788
- Lee, Y., Yang, W., and Kwon T., (2018). Data Transfusion: Pairing Wearable Devices and Its Implication on Security for Internet of Things, IEEE. [Viewed 9th December 2019]. Available from: https://ieeexplore.ieee.org/document/8418356

Case study title:	Assessment of security vulnerabilities in smart watches and wearable devices that could compromise data protection and privacy.

- Liu, S. (2019a). Smartwatches - Statistics & Facts. Statista. [Viewed 10th December 2019]. Available from: https://www.statista.com/topics/4762/smartwatches/
- Liu, S. (2019b). Number of connected wearable devices worldwide by region from 2015 to 2022 (in millions). Statista. [Viewed 10th December 2019]. Available from: https://www.statista.com/statistics/490231/wearable-devices-worldwide-by-region/
- Liu, S. (2019c). Adult wearable users penetration rate in the United States from 2016 to 2022. Statista. [Viewed 10th December 2019]. Available from: https://www.statista.com/statistics/793800/us-adult-wearable-penetration/
- Mikhalchuk, D., (2018). What is wearable computer: simple guide to the technology. Teslasuit. [Viewed 10th December 2019]. Available from https://teslasuit.io/blog/what-is-wearable-computer-simple-guide/
- Mozilla (no date A) Be Smart. Shop Safe. Mozilla [Viewed 19th February 2020]. Available from: https://foundation.mozilla.org/en/privacynotincluded/
- Mozilla (no date B). Minimum Security Standards Explained. Mozilla [Viewed 9th December 2019]. Available from: https://foundation.mozilla.org/en/privacynotincluded/about/meets-minimum-security-standards
- Sand, H. et al. (2017) Security Assessment Report, GPS Watches for Children, The Norwegian Consumer Council. Mnemonic. [Viewed 2nd January 2020]. Available from: https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-october-2017.pdf
- Shivram, S. (2017). Communications for Wearable Devices. arXivt. [Viewed 10th December 2019]. Available from https://arxiv.org/ftp/arxiv/papers/1705/1705.03060.pdf
- Sim,I., (2019). Mobile Devices and Health, N Engl J Med 2019;381:956-68
- Tabibu, S. (2017). Communications for Wearable Devices. ArXiv. [Viewed 10th December 2019]. Available from: https://arxiv.org/abs/1705.03060
- Technavio, (2018). Top 10 Wearable Technology Companies in the World 2018. Technavio. [Viewed 10th December 2019]. Available from: https://blog.technavio.com/blog/top-10-wearable-technology-companies-worldwide
- Vinod, (2015). Smartwatch security failings: Reaction from 5 cybersecurity experts. Computer Business Review. [Viewed 10th December 2019]. Available from: https://www.cbronline.com/news/internet-of-things/wearables/smartwatch-security-failings-reaction-from-5-cybersecurity-experts-4630114
- Wiegard, RB. & Breitner, M.H., (2019). Smart services in healthcare: A risk-benefit-analysis of pay-as-you-live services from customer perspective in Germany. Electronic Markets, 29: 107.
- Wilson, M. (2017). Don't Buy Your Kid A Smartwatch. Fastcompany. [Viewed 2nd January 2020]. Available from: https://www.fastcompany.com/90147796/dont-buy-your-kid-a-smart-watch

Interviews: Views have been sought from manufacturers, market research organisations and those carrying out academic research which relates to this. An informal interview has been carried out with an Apple employee and SMART watch trainer.