This report is part of the RAND Corporation research report series. RAND reports present research findings and objective analysis that address the challenges facing the public and private sectors. All RAND reports undergo rigorous peer review to ensure high standards for research quality and objectivity.

EUROPE

Living Room Connected Devices

Opportunities, security challenges and privacy implications for users and industry

Neil Robinson, Jon Freeman, Jan Gaspers, Veronika Horvath,
Tess Hellgren, Alex Hull

RAND EUROPE

Living Room Connected Devices

Opportunities, security challenges and privacy implications for users and industry

Neil Robinson, Jon Freeman, Jan Gaspers, Veronika Horvath,
Tess Hellgren, Alex Hull

Prepared for Ofcom

For more information on this publication, visit www.rand.org/t/rr604

Published by the RAND Corporation, Santa Monica, Calif., and Cambridge, UK

RAND Europe is an independent, not-for-profit policy research organisation that aims to improve policy and decisionmaking in the public interest through research and analysis. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Preface

RAND Europe was commissioned by Ofcom, the UK communications regulator, to investigate and prepare an independent expert report on the growth of the connected living room and the implications of this growth for UK citizens and consumers. As the living room becomes an Internet connected space, this shift offers opportunities to consumers and industry while also raising potential privacy and security concerns. Although currently a nascent market, the uptake of living room connected devices is expected to grow significantly in the coming years. However, it appears that there is a low awareness of how the capabilities of living room connected devices might be used, either legitimately by industry or illegitimately by criminal actors. This report addresses the security and privacy implications of the Internet connected living room for both industry and consumers, discussing potential benefits and emerging threats associated with living room connected devices and their technical capabilities.

Ofcom has a principal duty to further the interests of citizens and consumers in relation to communication matters. It is also guided by a regulatory principle to research markets constantly. Ofcom aims to remain at the forefront of technological developments and it is on this basis that this report was commissioned.

RAND Europe is an independent not-for-profit policy research organisation that aims to improve policymaking and decisionmaking in the public interest through research and analysis. RAND Europe's clients include European governments, institutions, NGOs and firms with a need for rigorous, independent, multidisciplinary analysis.

For more information about RAND Europe or this document, please contact:

Neil Robinson
Research Leader
RAND Europe
Westbrook Centre
Milton Road
Cambridge CB4 1YG
United Kingdom
+44 (1223) 353 329
neilr@rand.org
More information about RAND Europe is available at:
http://www.rand.org/randeurope.html

Table of Contents

Figures

Tables

Executive summary

Ofcom, the UK's independent communications regulator, has a principal duty to further the interests of citizens and consumers in relation to communications matters. In doing so, Ofcom is guided by a regulatory principle to research markets constantly and to remain at the forefront of technological developments, which will increasingly be central to the communications sector, and could bring significant new benefits and risks to citizens and consumers.

In order to further this objective, Ofcom has commissioned RAND Europe to conduct an independent research study on the growth of the connected living room, challenges for industry and emerging benefits for citizens and consumers, such as greater entertainment and communication opportunities. The report also discusses potential threats to consumers arising from the connected nature of such devices.

Summary

The living room is increasingly an Internet connected space, and living room devices, such as smart TVs, set-top boxes and games consoles, offer sophisticated PC-like capabilities. These devices provide access to greater entertainment, personalised services and communications opportunities than their non-connected predecessors.

When used as second screens, smart phones and tablets enhance the experience of watching TV, enabling users to interact with programmes and to share comments and opinion with others. Ofcom's own research has shown just how these devices are being used to enable families to share the living room while accessing and viewing different content simultaneously. Over half (53 per cent) of UK adults are now media multitasking while watching TV on a weekly basis.

The popularity of living room connected devices (LRCDs) in the UK is expected to continue to grow rapidly.

Several companies which previously had a presence in a related sector, such as Sony and Microsoft, have entered the marketplace for connected devices, but the potential revenues from both the devices and the applications running over those devices has also proved tempting to new entrants, such as Amazon. The growth potential has also attracted new content platforms and content creators, such as Netflix, increasing choice and availability for consumers.

However, the connectivity offered by such devices creates potential risks for the user in so far as they may be susceptible to the same sort of vulnerabilities as more traditional connected devices (PCs and laptops).

The study identified a number of potential risks associated with connected devices; however, they remain theoretical. It seems reasonable to assume that more vulnerabilities will be uncovered as the use of these

devices becomes more widespread. Manufacturers and software companies will clearly have a strong incentive to invest in security measures in order to protect their brand reputations.

One area of potential concern identified in the study is the process for issuing software upgrades and patches. Where devices are not regularly patched, they may be vulnerable to attack using malicious software. In the event of an infection, the evidence suggests that the only option for consumers may be to purchase a new device. It would appear that, in practice, it is difficult even for informed consumers to take protective measures. Some devices have no suitable interface through which a consumer could install and manage protective software settings, while for some smart TVs the interface may be too complex for many consumers to use. In some cases, installing third-party software, such as antivirus solutions, may be restricted by the manufacturer for technical reasons, such that so doing invalidates the warranty.

Low levels of consumer awareness of how connected devices could be misused means, we believe, that some consumers may not be able to protect themselves sufficiently. Users rarely read privacy policies and/or terms of service when signing up to services and are likely to be unaware of the way in which service providers can use their personal data. Moreover, the initial set-up process for connected devices is typically where universally applicable permissions are sought for data capture and use, rather than at the time when the data is actually being gathered, and where more context could be provided. Also, the ability for consumers to use the full functionality of the device may be conditional upon granting the manufacturer permission to gather, and use, a broad range of data.

The report also considers whether the social nature of the living room environment raises new risks. Sensors on LRCDs could gather physical or location information about users and their gestures, and also record audio, pictures and video from their surroundings. This constitutes a broader challenge about privacy relating to the integrity of the personal space around an individual.

Conclusion

In conclusion, the market for LRCDs is nascent, although evolving rapidly, and therefore many of the concerns identified are somewhat hypothetical in character. These theoretical possibilities should be acknowledged in order to open a constructive debate about the potential impact of these issues and the effectiveness of measures. Such a debate is an important step to help realise the opportunities in this emergent technological domain.

Abbreviations

BBFC	British Board of Film Classification
DoS	Denial of service
DDos	Distributed denial of service
DRM	Digital rights management
ESRB	Entertainment Software Rating Board
HD	High definition
ICLR	Internet connected living room
IPR	Intellectual property rights
ISP	Internet service provider
LRCD	Living room connected device
OFT	Office of Fair Trading
NTB	Net-top box
PEGI	Pan-European Game Information
RAT	Remote Access Trojan
STB	Set-top box
VoD	Video on demand

1. Understanding the growth of the Internet connected living room

1.1. Introduction

This chapter introduces the Internet connected living room (ICLR) and the benefits and capabilities of living room connected devices (LRCDs). LRCDs provide users with new opportunities to interact with living room entertainment technologies, enabling a higher level of personalisation and convenience.

The consumer benefits of LRCDs are driving market growth, which is forecasted to be significant in coming years. While estimates vary as to current and future use of LRCDs among UK households, existing evidence suggests that the ICLR has established itself as a growing trend.

Engaged in this growing area is a complex value chain of industry actors, ranging from device manufacturers to broadband service providers. Industry actors support existing LRCD trends and seek to use new levels of connectivity to expand their customised services for users. However, user demand for new services is uncertain. According to one market research firm, a significant proportion of LRCDs appear to remain disconnected despite their Internet capability (Analysys Mason 2013).

1.2. The living room is transforming through growing use of living room connected devices

The living room, often the main shared social space in a home, is becoming more Internet connected as its common devices are increasingly enabled with online connectivity. The ICLR is a phenomenon that is emerging due to the growth of LRCDs.

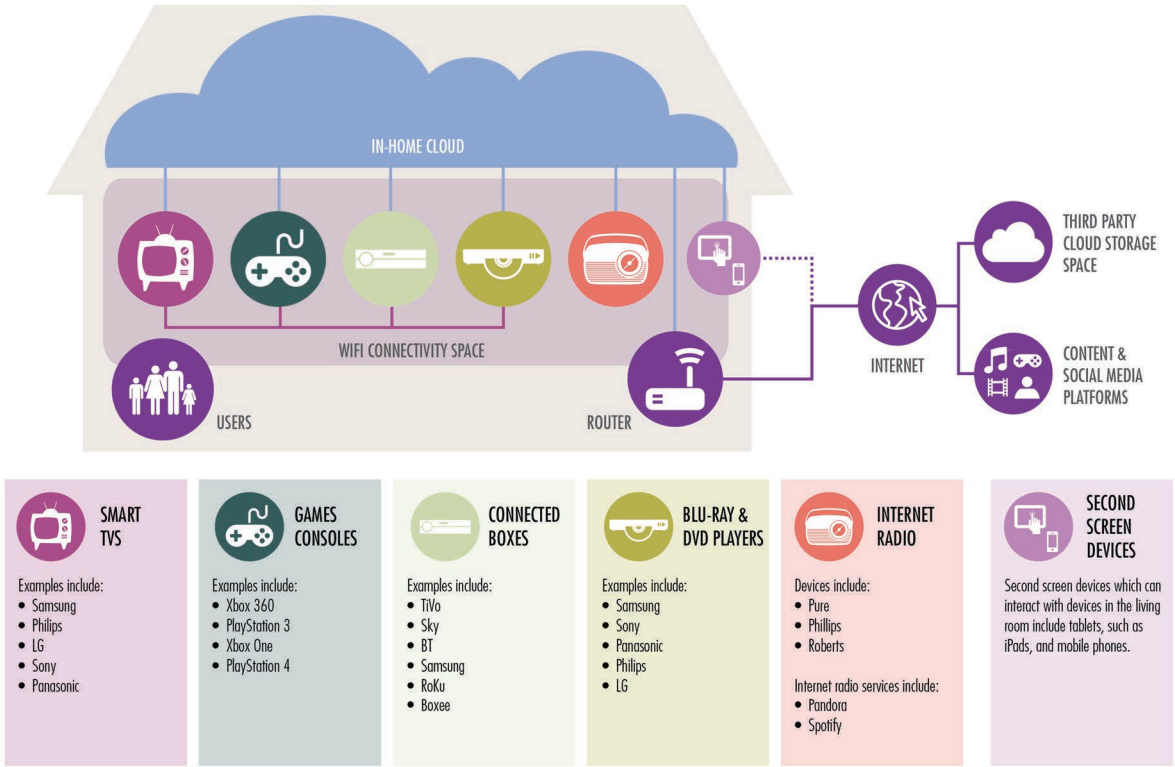
1.2.1. LRCDs are primarily used for entertainment and draw upon enabling technologies

LRCDs are any items of consumer electronics normally found in the living room – such as televisions, games consoles or radios – which are connected to the Internet, either directly or through a wireless router. While LRCDs may not appear to be much different from their earlier, unconnected versions, their heightened computing power increasingly gives them 'PC-like' capabilities similar to that of a home computer. The most common LRCDs seem to be smart TVs, set- or net-top boxes (STBs or NTBs), connected Blu-ray disc players and games consoles, all of which are primarily used for entertainment, such

as watching TV or playing games (some people also listen to radio through their TV). Smart meters are not a living room device and so are excluded from the scope of this study.

LRCDs are also enabled and supported by a range of technological tools. The primary enabling technology for the ICLR is a broadband Internet connection, which is often supported through a wireless (Wi-Fi) router. LRCDs are also supported by 'second screen' devices, which are smart phones or tablet computers used to interact with LRCDs (particularly smart TVs and games consoles). The network of LRCD technologies is illustrated in Figure 1.1.

Figure 1.1. The LRCD technology network



Source: RAND Europe analysis.

1.2.2. LRCD services vary depending on device manufacturers

LRCDs from different manufacturers often operate on different software without a single unifying standard.[1] There are different platforms, different software programming languages and different modes for connecting one device to another. For example, it is possible to connect a smart TV to a PC through a standard Wi-Fi network protocol (e.g. 802.11g), Bluetooth or wireless High Definition Multimedia Interface (HDMI). Smart TV apps, for example, are software tools that enable users to enjoy a range of services, such as the Netflix app for streaming movies or the DailyBurn app for gym workout routines. Smart TV apps may work on other devices, but this will depend on compatibility between the operating systems. Smart TV apps are developed in a software development language (such as HTML5, CSS or

[1] For example, they may use different operating systems or frameworks providing the environment for apps to run.

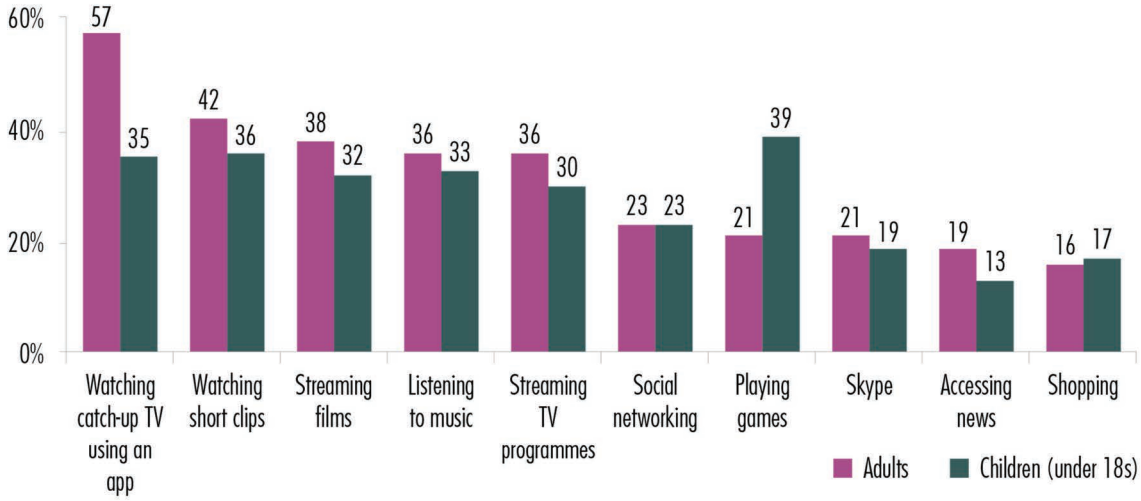
Google's Android) to work on different smart TV platforms (such as Google TV or Yahoo! Connected TV). Market forecasters have predicted that more smart TV manufacturers will move towards HTML5 as the preferred development language for apps because it will allow them to integrate different types of content and advertisements in a more effective manner, regardless of the particular operating system used on the device (NextMarket Insights 2013).

The challenges of variability across ICLR devices and services will be explored further in Chapters 2 and 3, when considering the origin of potential security or privacy threats and the measures that could be taken to address these.

1.2.3. LRCDs are engaged with by the traditional range of living room users

The users of smart TVs appear to not differ widely from traditional living room users. Both adults and children are using smart TVs to access online content, with the only major differences being that children tend to play more games than adults and watch less catch-up TV (see Figure 1.2). Evidence from an interview with a representative of Decipher Media Research (2013), a market research firm in the field, also suggests that different age groups have different viewing behaviours, for example, teenagers may be more likely to seek out quicker and cheaper access to entertainment.

Figure 1.2. Activities undertaken on smart TVs by adults and children



Source: Ofcom (2013).
(1) Q.B8. Which of the following, if any, do you use the internet functionality of your smart TV for? (2) Q.B15. What types of activity are they doing?
Base: (1) All respondents who have used the internet functionality of their smart TV (541) (2) Smart TV owners with children under the age of 18 years who use the Internet functionality on the smart TV set at least sometimes (253).

1.3. LRCDs are blurring the line between passive and active entertainment

The devices in an ICLR are primarily used for consuming entertainment such as music, games or video (including catch-up TV or films). Some types of LRCDs like the Sony Bravia or Samsung HDTV Plasma models of smart TVs even make it possible to enjoy the full range of Internet services, including social media platforms like Facebook, without requiring a separate computer. However, questions arise about how users will behave when accessing these online capabilities in the context of their living room rather than on personal computers.

The ways in which users interact with living room devices has been characterised by researchers Vinayagamoorthy et al. as 'lean-back,' which describes a user experience of relatively passive, relaxing consumption, often involving a large screen across the room (Vinayagamoorthy et al. 2012). Many living room entertainment devices, such as televisions, enable both passive and social viewing. Passive viewing occurs, for example, when the TV is on in the background while users undertake other activities such as preparing or eating a meal. Televisions also enable social viewing, such as when family and friends gather around the TV for a shared viewing experience of a programme such as a live talent show or sporting event (Vinayagamoorthy et al. 2012). Another researcher (Hommerberg 2012) suggests that the big consumption advantage of a TV is its large screen, allowing more people to watch it simultaneously; this makes it a device of choice for social consumption (which would include game-playing).

In contrast to this passive type of interaction, personal computers encourage more active participation by users. This type of 'lean-forward' activity is often performed at a desk by an individual in an active engagement or working role, physically involving a smaller screen positioned much closer to the user (Vinayagamoorthy et al. 2012). This 'lean-forward' use of devices has traditionally been the mode in which new Internet content is discovered.

1.4. The market for LRCDs is forecast to grow significantly in coming years

The ICLR is blurring the distinctions between 'lean-back' and 'lean-forward' devices by introducing opportunities for active user interaction into devices which have been traditionally used for passive engagement; for example, a smart TV can be used like a computer to search the Internet. However, fully active engagement with the Internet through a television medium is generally difficult, due to lack of a highly useable interface and limited processing power. These limitations mean that to date, some researchers have concluded that much of the interactive capability of LRCDs contributes to the 'lean-back' experience by making it easier for users to find more entertainment without more effort (Vinayagamoorthy et al. 2012). For users, the researcher Hommerberg (2012) considers the main opportunity of LRCDs such as smart TVs lies in the opportunity to be guided towards content they might not otherwise have encountered. For example, smart TVs may remember users' viewing history and use this information to proactively recommend specific channels or programmes. While preserving users' passive engagement with the device, this type of technology thus allows a more active and responsive viewing experience that is tailored to users' preferences.

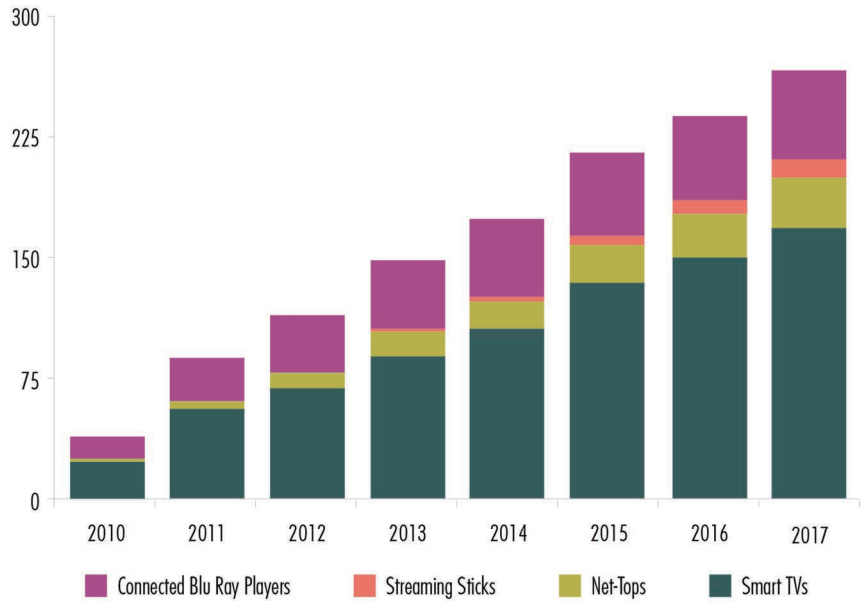
1.4.1. Consumer entertainment preferences will drive LRCD growth

The market for LRCDs is generally expected to grow, with increased sales of devices driven in particular by increased demand of smart TVs, games consoles, NTBs and connected Blu-ray players. NextMarket, a market research company, has considered the future of the ICLR, and concluded that:

> The connected living room streaming device market – which includes smart TVs, net-tops (streaming devices such as Apple TV or Roku), connected Blu-ray players, as well as a new class of streaming sticks[2] – is expected to grow from 114 million devices shipped worldwide in 2012 to 267 million by the end of the forecast period (NextMarket Insights 2013).

Their forecast of significant increase, which does not include games consoles, is illustrated in Figure 1.3. Added to this, Gartner, a technology research company, estimates that global sales of games consoles (the latest versions of which feature Internet connectivity) are forecast to grow from $15.9 billion in 2013 to $22.7 billion in 2015 (Gartner 2013). These growth forecasts were supported by interview evidence gathered during this study, suggesting that the LRCD market will grow and evolve significantly over the next few years (BBC 2014; Decipher Media Research 2013; iSEC 2013).

Figure 1.3. Forecast of increase in global shipments of LRCDs (millions)



Source: NextMarket Insights (2013).

The increased demand for LRCDs seems to be driven by consumers' expectations of appearance, capability and accessibility. Research by Ofcom, the communications regulator, identifies the reasons for consumers buying a smart TV are 'they needed a new TV and decided to buy one with the latest technology' (51%). The next most commonly cited reasons relate to 'liking the design of the set' (33%)

[2] Streaming sticks are devices that can be plugged into a TV to download programmes from the internet.

and 'wanting the best screen' (29%) (Ofcom, 2013). New TVs also are equipped with innovative service capabilities that, according to media research firm Decipher, enhance the user experience, making it similar to what they enjoy on their computer, tablet or mobile device (Decipher Media Research 2013). Improved connectivity also heightens TVs' accessibility to users, as new TVs are wireless (avoiding the need for the customer to physically connect them) and automatically request wireless passwords upon activation (inviting immediate connection) (Decipher Media Research, 2013).

1.4.2. LRCD use is growing in the UK, although estimates vary

There are varying opinions as to how widespread LRCDs are in the home, but the main observation is that UK homes have more devices that connect to the Internet, many of which are LRCDs. Ofcom's 2013 UK Communication Market Report showed that UK households have an average of three different types of Internet-enabled devices (however, these devices may not be Internet connected), of which the most popular are laptops, smartphones and games consoles, and that 7 per cent of UK households own a smart TV (Ofcom 2013). A survey by Microsoft (a software company) suggested that UK households have on average ten connectable devices, of which six will be connected to the Internet, with 63 per cent of families having some form of games console that connects to the Internet, 40 per cent having a set-top box, and a quarter having TVs connected to the Internet (Microsoft 2013). Decipher, a media research company, estimates from a survey of online households that in the UK a PlayStation 3 can be found in about 20 per cent of homes and an Xbox 360 in a further 22 per cent of homes, and that most of these consoles will be replaced with the new generation versions which often connect to the Internet by default (Decipher Media Research 2013).

In the UK, Decipher Media Research estimates that half of the boxes installed for Sky TV customers are Sky+ HD (high definition) boxes that are enabled for Internet connectivity, and of these about half are already connected to the Internet (Decipher Media Research 2013). This figure is expected to grow as Sky encourages more subscribers to use their Video on Demand (VoD) service (the ability to download videos to view when the user wishes), meaning that within two years Sky may have 6 million connected boxes in UK homes (Decipher Media Research 2013).

Market forecasting company NextMarket and software company Microsoft expect that second-screen devices such as tablets and mobile phones could influence the smart TV market by further increasing the popularity of smart TVs over Blu-ray and NTBs, particularly as they make it easier to discover further content (Microsoft 2013; NextMarket Insights 2013). The Apple TV service, for example, which operates through a NTB, is expected to grow in popularity as more people are attracted to the prospect of an Internet connected TV that can be controlled through their iPhones and iPads (Decipher Media Research 2013).

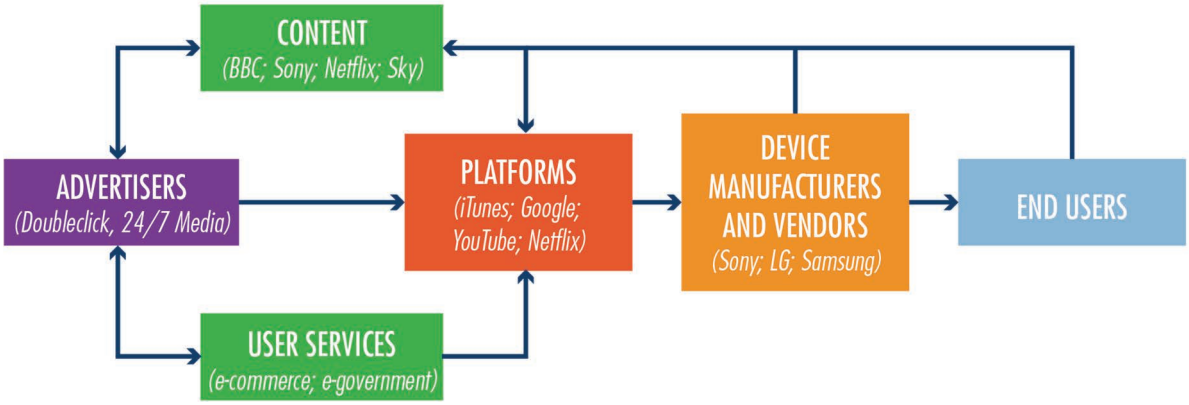
Despite the variations in specific findings from available studies, the general conclusion from a media researcher, broadcaster and security software company interviewed for this study is that, while not ubiquitous, the ICLR is increasingly common in the UK and growth is expected to continue (BBC 2014; Decipher Media Research 2013; Symantec 2013a).

1.5. A complex range of industry actors are engaged in the ICLR, with varying roles and motivations

1.5.1. LRCD actors interact in a value chain

The range of LRCDs and related service providers means that the playing field of industry actors for the ICLR is complicated. The main actors to consider are device manufacturers, service providers, platform providers and content generators (among which users of such services as Twitter can be counted as well) and, related to these, the advertisers. The service providers are in some cases also generating new content, including TV programmes. Underpinning all these actors are the providers of broadband services, without whom the market for LRCDs would not exist. Industry players interact in a value chain (a series of activities conducted to bring a valuable service or product to the market) to provide LRCD entertainment services to end users. While this network may vary slightly depending on the different devices and services that are being used, Figure 1.4 illustrates a generic value chain for the ICLR.

Figure 1.4. A generic value chain for the provision of ICLR services to end users



Source: RAND Europe analysis.

A key observation to make about the value chain is that the roles each party plays are becoming intermingled and the same player increasingly performs multiple roles. For example, Netflix, a company which specialised in providing a platform for end users to consume content commissioned by others, recently began to commission its own content. Netflix thus plays a role as both a content provider and a platform provider. Formal legal agreements might not exist between different players, potentially resulting in greater confusion about how obligations, e.g. with regard to consumer protection, are transferred between different market players. The issue of consumer protection becomes more confusing as a consequence. Figure 1.4 also does not reflect the nature in which end users become content aggregators through, for example, discussing on social media a television show during its broadcast via their second screen devices. Cloud service providers (a new type of market player) can also join this complex landscape but they do not necessarily fall into any of these readily defined types: they are neither service providers (in the traditional communication service provider sense) nor content creators, but they are becoming increasingly important in the ICLR as a place to store content but also manage authorised personal media

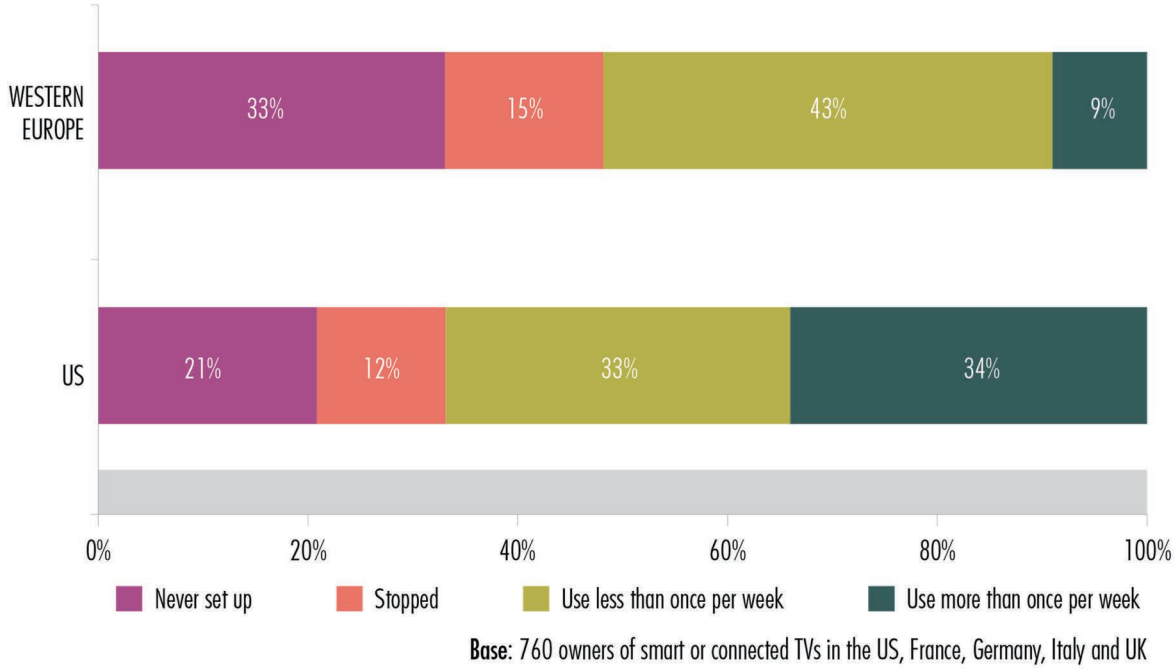
collections, for example via Apple's iCloud service. This value chain for service provision is enabled by a 'back chain', which describes how a range of personal data is collected about users at the device level directly (as was demonstrated by the LG Smart TV privacy news story reported by the BBC and others in late 2013; BBC 2013a), or about user choices as captured on platforms (so-called clickstream information) or through consumption of content. This is then integrated, and perhaps processed, by 'information aggregators' and 'resold' to content providers, advertisers (or the merchants they represent) and user service providers for market research, product design or personalised service purposes (European Parliament 2011). The ability to gather data on users and their behaviour offers opportunities that have yet to be exploited fully, but could include targeted advertising, entertainment recommendations for users and possibly new ways of selling goods to users.

1.5.2. User demand for new Internet enabled services is not yet clear

Companies which support the ICLR, in particular platform providers, content providers and device manufacturers, have an interest in gathering data on users and their behaviour, such as personal data and what entertainment they particularly enjoy. This data could be used to recommend content to users (which users may be prepared to pay for) or to better target advertising to suit users' real or predicted preferences. Given the industry benefits of improved data on user preferences, ICLR companies are keen to encourage more living room users to connect their entertainment devices to the Internet. It is also possible that LRCDs could be used in the future for developing new avenues of e-commerce, informed by user data and usage behaviour. By contrast, there is little evidence about what users are demanding as new services; at present the most popular services appear to be catch-up TV and the ability to download films. The development of new services is, in our view, presently driven by industry innovation rather than user demand.

However, a European Commission source suggests 91 per cent of connected TV users in western Europe are either not connected or using the service infrequently (see Figure 1.5), whereas Analysis Mason, a research and consultancy company, states from survey evidence that of the 20 per cent of people who claimed to own a smart TV, fewer than half had connected it to the Internet (Analysys Mason 2013; DG Internal Policies 2013). On the other hand, research by Ofcom suggests that of those who own a smart TV in the UK, 77 per cent have connected it to the Internet and used the connection (Ofcom 2013).

Figure 1.5. Use of connected functionality in TVs



Source: Directorate-General for Internal Policies (2013).

2. Security, privacy and industry challenges in the Internet connected living room

2.1. Introduction

Along with its range of benefits, the ICLR presents a number of potential challenges for users and industry alike. This chapter outlines the possible security and privacy concerns related to growing use of LRCDs.

The major security threats facing the ICLR are not new; instead, they are existing online threats that find a new 'means' of attack by exploiting LRCD vulnerabilities. LRCDs may store users' personal or financial data, making them ideal targets for online attackers seeking to inflict financial or psychological harm. The growing complexity and standardisation of LRCDs makes them particularly susceptible to these Internet enabled security threats.

LRCDs' collection of user data also attracts industry interest in the monetisation of personal data. While less sinister than security threats, the use of personal data by industry actors poses potentially significant privacy challenges to ICLR users.

A lack of appropriate awareness among users has the potential to exacerbate LRCDs' vulnerability to security threats and privacy breaches.

In the future, security and privacy concerns may spur industry to take a more active role in addressing user protection and digital rights management. The most powerful incentive may come from companies' desire to prevent reputational damage from well-publicised security breaches, as has occurred in the past.

2.2. There are no new threats, just old threats in new devices

To map and understand the security threats UK users could encounter in the ICLR, it is useful to distinguish these threats in terms of their ends, ways and means.[3] For the purpose of this study, the 'ends' denote the financial or psychological motives that prompt attackers to exploit different vulnerabilities in LRCDs (i.e., why they do it). The 'ways' refer to the ways in which these vulnerabilities can be exploited

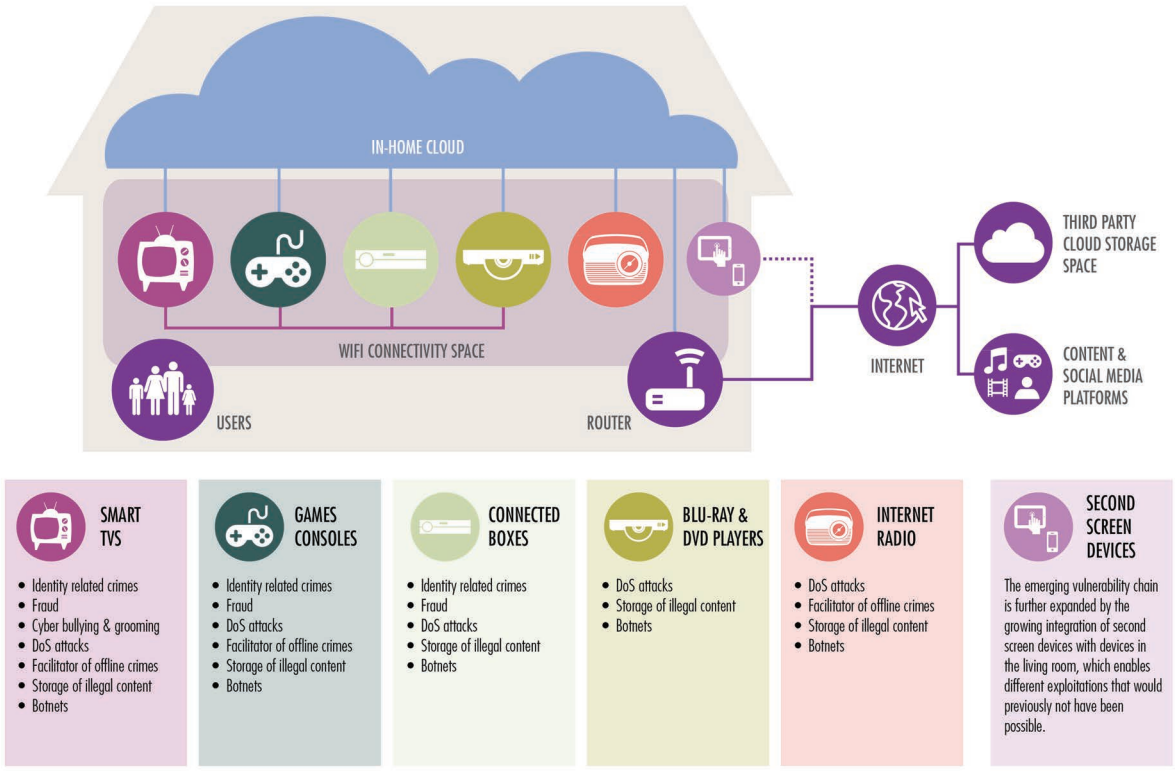
[3] Assessing challenges and threats in terms of their underlying ends, ways and means is a common approach in strategic threat analysis and therefore also applied in the context of this chapter.

by attackers (i.e., how they do it). Finally, the 'means' are the LRCDs most likely to display the vulnerabilities that are exploited by attackers (i.e., what devices they use to do it).

Significantly, many of the potential security challenges in the ICLR – such as identity-related theft and fraud, online fraud, cyberbullying and online grooming, and Remote Access Trojans (see Figure 2.1) – involve the same ends and ways that characterise security threats to PCs and tablets. Many UK users are already familiar with these threats in a personal computer context; for example, empirical data from a Home Office bulletin suggests that in recent years 33 per cent of UK adults had been negatively affected by a virus at least once a year (Smith et al. 2012). European Commission information shows that in total, some 11 per cent of UK Internet users have been victims of cyber-enabled identity fraud, the highest figure in the EU (European Commission 2013a). Researchers at Oxford University report that 6 per cent have had their credit card details stolen online (Dutton & Blank 2013), and Home Office figures show that 5 per cent have experienced financial loss from the fraudulent use of debit or credit card details (McGuire & Dowling 2013).

However, users might struggle to fully appreciate how known online security challenges will play out in the new context of the ICLR. Indeed, as will be outlined in the next chapter, the familiar ends and ways that have characterised online security threats take on unfamiliar guises when combined with the new means of LRCDs through which attackers can pursue their malicious ends.

Figure 2.1. Potential security challenges associated with LRCDs



Source: RAND Europe analysis.

Personal data accessed through the ICLR could contribute to identity-related crimes

In order to use or access content or social media platforms in the ICLR, users normally transmit personal details, including names, addresses, dates of birth and banking or credit card details, via their LRCDs as well as in the databases of the relevant platform providers. For example, to login to a service like Amazon Instant Video, the user name and password needs to be submitted and credit card information supplied (Amazon Instant Video 2014). An international team of university researchers (Arabo et al. 2012) has therefore suggested that both LRCDs and platform databases are likely to become increasingly attractive targets for financially motivated thieves, who exploit vulnerabilities to extract personal data in order to open bogus bank accounts, to extract cash or to create fake online profiles to get free access to premium online services .

While our research was only able to uncover one study, conducted by a team of university researchers led by Engebretson (Engebretson et al. 2013), into the ways in which cybercriminals could exploit LRCDs as means to commit identity theft or fraud, it seems likely that games consoles will constitute particularly attractive means to such criminals due to the associated potential for resale. Specifically, Engebretson and his colleagues (2013) suggest that the emerging second-hand games console market has the potential to lead to rising rates of identity theft. Their study also shows that it is possible to modify the software on a refurbished Xbox 360 to find the original owners' files, folders and credit card details on the hard drive; this method may already be employed by cybercriminals (Engebretson et al. 2013). While managing data storage is a standard and relatively straightforward feature of all major games consoles, we did not find evidence whether UK users are aware of the simple methods that exist to delete personal data from games consoles. Likewise, we did not find evidence whether users are aware of the need to delete this data before trading in their console. However, as long as the scope of the problem is not fully established, it is also unclear how it should be addressed.

In general, identity theft in the ICLR could become a much more significant problem for users in the future if biometric identification becomes a more popular LRCD feature. Indeed, as one academic explains, some LRCDs already have biometric online identification tools on board, which will identify users by scanning their iris or fingerprint, and it seems likely that such tools will become increasingly common features (Corcoran 2013). However, while the use of personal biometric data as a means of authentication has several advantages for consumers, such as improved child protection mechanisms, the academic expert also underlines that their introduction carries the risk of a rise in 'irreparable' identity thefts, as once compromised, biometric data cannot be easily modified to correct intentional inaccuracies, unlike a credit score, for example (Corcoran 2013).

While the illicit extraction of personal data from platform databases arguably poses a challenge to industry reputations (see Section 2.5.2), such instances can also have severe negative consequences for LRCD users. Engebretson and his research team (Engebretson et al. 2013), for example, have reported that in early 2012 cybercriminals gathered gamer tags (i.e., individual online gamer signifiers) from the Xbox online gaming platform, Xbox Live, and were able to extract user information of Xbox live account holders, including credit card details and account information for other online services. Their study (Engebretson et al. 2013) further reports that this was accomplished by searching for similar tags on the Internet and

rapidly testing password combinations. The compromised accounts were then hacked to enable fraudulent purchases.

The ICLR might become a place where users are defrauded

One security firm representative interviewed for this study (Lookout 2013) suggested that an increase in the use of smart TVs and games consoles for surfing the Internet is likely to see the extension of online fraud from one platform to another, namely from the PC to a smart TV screen. This change in online fraud will likely have little impact on the fraud's ends or ways. Cybercriminals will continue to trick individuals into sharing financial or other valuable information, for example via 'spoofing' (fooling people into entering valuable data, such as financial details, into a counterfeit website), 'phishing' (bogus but often convincing money transfer requests), or 'spear phishing' (highly personalised bogus e-mails). The 'lean-back' experience of the ICLR (as discussed in Section 1.3) may, according to a market researcher from Decipher Media Research (2013) interviewed for this study, be associated with lower attention levels of LRCD users, meaning that people are more likely to fall victim to online scams than in the context of using PCs.

Cyberbullying and online grooming may extend to LRCDs

'Cyberbullying' captures all forms of bullying by electronic means, which can be through games networks, social networking sites or other services, and usually serves the perpetrators as a source of 'fun' or 'revenge'. 'Online grooming' describes the use of digital technologies, such as social networking sites, chat rooms or online gaming platforms, to befriend minors with the aim of committing a sexual offence.

Cyberbullying and online grooming have been of growing concern among the media, parents, law enforcement and child protection groups for some time, and it is conceivable that they may migrate to the ICLR. However, we were not able to uncover evidence that would suggest that LRCDs used in the ICLR provide cyberbullies or online groomers with new attractive means to commit their crimes. Indeed, industry, security firm, and market research views gathered for this study (Decipher Media Research 2013; iSEC Partners 2013; Steam 2013) suggests that, at the moment, cyberbullying and online grooming constitute minor challenges in the communal environment of the ICLR. Instead, we were told that cyberbullying and online grooming are more likely to take place on Internet connected devices in children's bedrooms, where parents tend to have less oversight over the activities of their children.

Indeed, recent media coverage (Fahey 2012) has given rise to the impression that children may be increasingly exposed to cyberbullying and online grooming practices when using online gaming platforms. LRCDs could therefore provide perpetrators of cyber bullying and online grooming with new means to pursue their ends. Specifically, the anonymous live chat functions of some games console networks offer a way to behave in a manner towards minors that might not be socially acceptable and that might even constitute a crime, such as, for example, instances of hate speech. US law enforcement agencies have also noted the attractiveness of games console networks, which are predominantly used by minors, for those wishing to groom children online and, according to media reports (Fox News 2013; Semmes 2011), several US citizens have been convicted of sexual offences against children in cases where grooming took place over online gaming networks. As Microsoft's own public relations work (Lavin 2013) suggests, the latest generation of the Xbox games console enables players to search for others based on age and

language. Users would need to take care in activating settings to restrict or make available their age or language lest this capability become a concern.

Remote Access Trojans exploit sophisticated audio-visual capabilities in LRCDs

A Remote Access Trojan (RAT) is a piece of malicious software that is remotely installed on a device without the user being aware of its presence. According to the security firm Symantec (2013a), the result is that an attacker can gain almost complete control over the compromised device. The attacker can then do most things that someone physically sitting in front of the device could do, including extracting data stored on the device and recording audio and/or video footage using microphones and cameras built into the device. RATs are an increasingly frequent occurrence on PCs; Symantec has expressed concern about the spread to LRCDs, with smart TVs considered to be a good means for facilitating the ends of RAT attackers (Symantec 2013b).

These ends are usually financial or psychological. A BBC news report (BBC 2013c) uncovered that RAT attackers either threaten to release stolen or recorded data online unless a certain amount of money is paid by the victim, effectively blackmailing them, or they try and bully their victim by releasing the stolen or recorded data with the aim of permanently damaging the victim's reputation or causing psychological damage or distress.

As smart TVs and games consoles are increasingly incorporating microphones and cameras to facilitate online multiplayer gaming and videoconferencing, one academic vulnerability researcher (Sangani 2013) has argued that both types of devices constitute perfect means for RAT exploitations. At the 2013 Black Hat IT security conference, for example, security experts revealed theoretical attacks against several of Samsung's 2012 smart TV models, which allowed them to turn on the camera, take control over social media services like Facebook or Skype, and access files. While Samsung has patched the firmware of the smart TVs in question, RAT attackers can, according to Symantec (2013a) draw on a wide range of other hitherto undisclosed software vulnerabilities to compromise smart TVs. Likewise, it seems conceivable that RAT attackers could exploit vulnerabilities in games consoles in the future, although no evidence of such an attack seems to exist to date.

LRCDs might become affected by denial of service attacks

Rather than because of hardware failure, future technical faults of LRCDs could well be the result of malicious activities. Although it remains to be seen what techniques attackers will be able to draw on to 'find' smart TVs, which are, as one industry representative (Schultz 2014) notes, usually only indirectly connected to the Internet via a router and therefore 'hidden' to attackers from outside , smart TVs being hijacked by cybercriminals constitutes a conceivable scenario according to a group of university researchers led by Iyer et al. (2011). Indeed, security firms and informed media representatives (Common Vulnerabilities and Exposures 2012; Leyden 2012; Security Affairs 2013) have suggested that smart TVs could not only be the means (see below) but also the target of denial of service (DoS) or distributed denial of service (DDoS) attacks.[4] Such DoS / DDoS attacks would involve a smart TV being flooded with

[4] A DoS attack uses one electronic device and one Internet connection to flood a server with packets that overload the targeted server's bandwidth and/or processing power. In contrast, a DDoS attack draws on many devices and

massive data requests, which it cannot process, causing it to constantly reboot without user input or to not start at all. As a result, the TV would effectively be unusable. Although there are no known reports of such an event to date, DoS / DDos attacks on a smart TV could also be the overture to an online fraud scheme, where cybercriminals (falsely) offer to reinstate the functionality of the hijacked smart TV for payment of a fee.

The exploitation of data from the digital living room may enable offline burglary

A scholar having conducted extensive research on security implications of LRCDs, Al Falayleh (2013) suggests that cybercriminals may also be able to monitor the ICLR (using RATs, for example) and thus to establish when users are in or out of the house. These observations could then subsequently be sold to more 'traditional' criminals who are planning to commit crimes offline, such as burglary. In such a scenario, the ICLR offers a new way to plan burglaries, with smart TVs and games consoles constituting ideal means for cybercriminals to monitor user behaviour. However, according to a representative of Lookout (2013), a security firm interviewed for this study, even the usage patterns of less obvious devices, such as Internet radios, could be used as an effective means to find out when houses are unoccupied. However, this threat is currently debated as a theoretical possibility among security researchers from vulnerability research companies like McAfee (2013a), and there is no evidence of such an event actually having taken place.

The living room as an illegal content storage space

The availability of considerable amounts of digital storage space in the ICLR may, according to Al Falayleh (2013), attract cybercriminals in pursuit of inconspicuous opportunities to store pirated or other illegal content, which can subsequently be made available over the Internet. While no reliable data on the scale of this problem exists to date, smart TVs, connected boxes and games consoles have been identified by Lookout (2013) as particularly attractive means to distribute pirated and other illegal content, given their growing storage space and a broader range of ways in which they can be targeted. However, according to the same security firm (Lookout 2013), even devices that come with relatively small hard drives, such as Internet radios, could become attractive storage space for cybercriminals because they often have limited user interfaces, which makes it especially difficult for users to discover whether their devices are being exploited for the hosting of malicious, illegal or unauthorised content.

LRCDs could power botnets

Europol (2014) has reported for some time already that botnets have provided a platform for cybercriminals to perform DoS attacks, to host illegal or malicious content or to perpetrate other forms of misuse.[5] A team of university researchers led by Arabo (2012) has argued that cybercriminals might also

---

multiple Internet connections, often forming a so-called 'botnet' in order to overload the target's bandwidth and processing power.

[5] A botnet is composed of electronic devices with computing capabilities, which have been set up to communicate with each other via the Internet by a piece of malicious software without the device owners actually being aware of the existence of the communication and thus the botnet. Botnets are usually set up to forward transmissions, including spam or viruses, to other electronic devices connected to the Internet.

increasingly use LRCDs as means to create botnets or parts of botnets. Indeed, in recent years, security researchers from Lookout (2013) have become aware of at least two large-scale instances where LRCDs were found to be part of a botnet composed of more than 500,000 devices, underlining the attractiveness of LRCDs as means to create and to maintain a botnet. Significantly, even LRCDs that have relatively modest computing capabilities, such as Internet radios, are able to generate enough traffic to render a significant DoS attack. Moreover, as a researcher at Lookout (2013) interviewed for this study has suggested, they might be able to manipulate the targets of the botnet they are a part of in a way different from that of a PC, due to the different ways in which they interact with other devices.

In terms of cybercriminals' goals, two developments in particular are thought to encourage the use of LRCDs as a means to create and conserve botnets. First, as security firms Kaspersky and McAfee (McAfee 2013b; Raiu et al. 2013) have suggested, with virtual currencies (such as Bitcoin) on the rise, LRCDs may increasingly become part of botnets that help to mine virtual currency.[6] Second, security firm representatives interviewed for this study (iSEC Partner 2013; Lookout 2013; Symantec 2013a) suggested that in the future hacktivists or cyberterrorists could potentially draw on the computing power of botnets composed of LRCDs to launch large-scale cyberattacks on vital digital infrastructure.

2.2.1. LCRDs' growing complexity creates new vulnerabilities

While LRCDs already have the potential to serve as means to pursue the ends of cybercriminals and other attackers, creating substantial security challenges for users, the complexity of these devices may create new vulnerabilities and exacerbate old ones. Security researchers consulted for this study agreed that the more complex the design and capabilities of LRCDs become, the greater the risk of exploitation for misuse and crimes (iSEC Partners 2013; Lookout 2013; Symantec 2013a). There seems to be a widely shared understanding that, as the ICLR become more complex (see Figure 1.1), users will increasingly struggle to understand the vulnerabilities that these devices may be subject to and the way in which the vulnerabilities of these different devices might relate to each other. Indeed, as university researchers (Suomalainen et al. 2010) have suggested, a growing complexity of devices with their own distinct vulnerabilities, some of which have been presented in Section 2.2.3, makes the home network, which connects many of these devices, much more difficult to secure. Using the words of one Symantec (2013a) researcher consulted for this study, 'The market will expand before people understand the risks. That gap is where the risk lies.'

2.2.2. Standardisation of LRCDs' software ecosystems could result in the emergence of a vulnerability chain

Several security firms (iSEC Partners 2013; Lookout 2013; Symantec 2013a) believe that in the past the diversity of LRCDs and their foundational software ecosystems served as a 'natural' protection against the efficient exploitation of one vulnerability across different devices.[7] Conversely, they (iSEC Partners 2013; Lookout 2013; Symantec 2013a) argue that the homogenisation of software ecosystems could increasingly

[6] Virtual currencies like Bitcoin are mined or created through the use of spare computing power which users provide via a network, usually the Internet.

[7] The term 'software ecosystem' describes a collection of autonomous, but linked, software systems, which are developed in the same environment.

result in the emergence of a chain of similar or mutually reinforcing vulnerabilities across different devices. According to Symantec (2013a), recent industry tendencies to implement standard web technologies, such as HTML, CSS and Java, into smart TV apps, or to rely on Google's Android as a basis for smart TV operating systems, increasingly allow cybercriminals to 'capture' several types or models of devices (of which the installed user base may be huge) by exploiting one vulnerability. In this respect it is crucial to note that vulnerabilities exist across many of the software ecosystems LRCD manufacturers currently employ; during 2013, for example, Kaspersky security consultants (Raiu et al. 2013) have noted that Java vulnerabilities accounted for around 90 per cent of attacks across different devices, making it the most attractive software ecosystem target among cybercriminals. During the same year, Google's Android was in third place, with vulnerabilities accounting for around 2.5 per cent of all cyberattacks. According to one Symantec researcher interviewed for this study (Symantec 2013a), it is likely that the share of attacks on Android-based devices will continue to grow because Android is widely used and it is relatively easy to develop malicious code for this ecosystem.

Second screens extend the vulnerability chain

The emerging vulnerability chain is currently further expanded by the growing integration of second-screen devices with smart TVs and games consoles (see Section 1.2), which enables different exploitations that would previously not have been possible. For example, a vulnerability in a smartphone could be exploited to remotely connect it to a smart TV via Bluetooth. As a result, as told when interviewing a security consultant from Symantec (2013a), even those smart TVs that users have deliberately not directly connected to the Internet could become a means for the pursuance of the malicious ends of cybercriminals through exploiting vulnerabilities in second-screen devices to traverse to other devices on a home network.

Usage of the cloud expands the vulnerability chain

Decipher Media Research (2013) has uncovered that ICLR users store an ever-growing amount of personal data remotely in the cloud on services like Dropbox or Google Drive, and LRCDs are increasingly designed to access this data, which further expands the vulnerability chain. Thus, cloud storage space and content platform providers could, according to a senior McAfee (2013a) security researcher, make for increasingly attractive targets for cybercriminals, as one successful attack could provide a massive amount of sensitive user data (including account and financial details), the possession of which could constitute a useful first step for fraudulent activity or the blackmailing of the original data owners. However, cybercriminals are not the only reason why users may be increasingly at risk of losing data they assume to be safe in the cloud. An informed journalist (Mello 2013) has described several high-profile incidents of large-scale cloud storage providers becoming temporarily unavailable through outages or system or network failures and denying access to users' content.

2.2.3. Three critical issues: immature firmware, inconsistent patching and unaware users

The potential of the ICLR to be exploited has, to date, not translated into a change in the security behaviour patterns of industry and users. Indeed, there seem to be at least three issues that account for the emergence of security challenges in the ICLR:

- Immature firmware
- Inconsistent patches
- Poor user security behaviours.

Firmware used in LRCDs is prone to vulnerabilities

The manufacturers of LRCDs have a business imperative to develop and bring to market new models, loaded with features boasting the latest innovations, as quickly as possible. Based on previous analysis of how security relates to innovation in a European research study Robinson et al. from RAND Europe concluded that, as a result, security often comes as an afterthought (Robinson et al. 2007). Given the innovative nature of the LRCD market, as described earlier in Chapter 1, it might be assumed that similar dynamics might apply here and security comes a poor second.

The problem of more and more LRCDs being released without a sufficiently mature software ecosystem is aggravated by the presence of a growing number of 'non-traditional' Internet connected device vendors. Security experts (iSEC Partners 2013; Lookout 2013) consulted in this study referred to diverse security practices adopted by those involved in the LRCD value chain with varying levels of maturity related to the length of time firms had been designing and offering Internet-enabled devices and services.

Patches for vulnerabilities are often not provided rapidly

The absence of a regular patch cycle means, according to Vinayagamoorthy (2012) and a team of university researchers he has worked with, that the level of security in LRCDs depends on the pace at which customers upgrade their technology. As senior researchers from the security firm iSEC Partners (2013) have argued during an interview with us, from a manufacturer's perspective, upgrading a product may not always be a desirable option as there is always a risk of users temporarily or permanently damaging a running system in the process of attempting to install a firmware or software patch. However, for some devices, such as games consoles, which have a long life cycle of up to seven years, it is, according to Engebretson and his colleagues (2013), almost inevitable from a security engineering perspective that vendors will need to occasionally upgrade what is often older, legacy software.[8] In contrast, a smart TV has a typical lifespan of two to three years, which considerably lowers the pressure on manufacturers to offer firmware upgrades, with the implicit assumption being, according to various technology journalists (*Guardian* 2013b; Kerton 2012; Lawler 2012; Morrison 2012) that security vulnerabilities will be resolved when users purchase a new smart TV. However, in the meantime, users could be exposed to vulnerabilities that remain unfixed.

[8] This estimate is based upon past amounts of time between console generation's release dates, which stands at eight years for Xbox 360 to the Xbox One, and seven years between the PlayStation 3 and PlayStation 4 (Scharr 2013).

Poor user security behaviours create and increase vulnerabilities

UK users' growing familiarity with online threats in relation to using PCs or tablets (see Section 2.2) would suggest that there is also better user behaviour when it comes to responding to threats and challenges related to the use of LRCDs. However, parts of the UK population are still not aware of the ways in which they can fall victim to misuse in cyberspace. For example, the Home Office (McGuire & Dowling 2013) has estimated that 38 per cent of UK Internet users are unaware that clicking on suspect links can cause considerable harm to an Internet connected device and infringe upon the integrity of data stored on it. Some 42 per cent neither see any problems in downloading unknown programmes or files nor in using easy-to-guess passwords (McGuire & Dowling 2013). Not surprisingly, as a result, according to the Home Office (McGuire & Dowling 2013) 48 per cent of Internet users are not in the habit of protecting their own home network with a reasonably complex password, often resorting to the default password instead.

While evidence on users' perception of security challenges in the ICLR is still sparse, the findings presented in the work of Al Falayleh (2013) suggests that the figures provided above are not explicitly referring to user behaviour in the context of the ICLR; the nature of LRCDs and the 'trusted' environment in which they operate suggests that users may have an even lower awareness of the potential for security risks when using LRCDs (see Chapter 1). The Lookout researcher consulted within the framework of this study (Lookout 2013) highlighted that '… people are more likely to be trusting on a mobile device than on a PC because it doesn't seem as powerful. This will be worse when it is on your TV.' Another security consultant (Symantec 2013a) stressed that the ease of interaction with LRCDs means that the propensity of consumers to divulge sensitive information may be different than when accessing a webpage: 'People are more likely to give credit card information onto a device in the living room than a webpage.'

Users are also likely to perform relatively weakly when assessing potential security challenges in the ICLR because the connectivity of LRCDs often goes unnoticed. Evidence from some of the interviews conducted with market researchers and information security firms (Decipher Media Research 2013; iSEC Partners 2013; McAfee 2013a) for this study suggests that experts consider users to be poorly aware of the potential for connectivity, especially when LRCDs are connected by default out of the box.

In the PC world there are patch updating processes and policies that enable the user to exercise a degree of management over security (aided by either the software vendor or a third-party security provider). In contrast, updates for LRCDs, if provided by the vendor, may not be released as frequently and the user is not covered for liabilities resulting from the patch updating process. Indeed, Lookout (2013) consultants argue that it is often difficult for users to apply patches to LRCDs and the risk of something going wrong resulting in their device becoming useless is more pressing. At the same time, the lack of specific security solutions in the LRCD space means that it is more difficult for the user to be alerted or notified of the behaviour or presence of any unknown application or malicious software. Indeed, Al Falayleh (2013) suggests that there is often little user awareness of an ongoing attack.

2.3. ICLR industry actors also pose privacy and data protection challenges

While not a threat in the same way as the security concerns discussed earlier, the use of business models that revolve around the monetisation of personal data collected in the ICLR also poses significant challenges to users. Defined in greater detail in Chapter 1, these business models have potentially adverse implications for privacy and data protection in a number of ways. The failure to adhere to well-established principles for the protection of personal data, such as giving users the chance to exercise meaningful choice and consent to the ways in which their personal data will be used, while ensuring accountability and transparency for its use and permitting some degree of control by the data subject, has a potentially untoward effect upon privacy and the right to the protection of personal data.

Consumer rights organisations consulted for this study, both in the UK and at the European level (BEUC 2013; Office of Fair Trading 2013a), have expressed concern about LRCDs posing a challenge to users' rights to the protection of their personal data.[9] Specifically, engagement with the Office of Fair Trading (2013a) in the context of this study has revealed a growing concern about the 'aggressiveness' with which vendors of LRCDs and the providers of related services and platforms compete for users' data.

The concern is not surprising given that academic research (Clemons 2009; Zhan & Rajamani 2008) has established that the ICLR constitutes a potentially attractive place for hardware vendors and particularly media and social media platforms to collect personal data in order to offer products and services to individual users, with highly tailored messages, to deliver advertising and promotional pricing to consumers at exactly the right time, and to enable advertisers to constantly monitor the impact of their advertising and their promotional expenditures. A survey recently conducted by a German IT magazine (Heise 2014) has revealed that all major smart TV brands available on the UK market share extensive data about users' viewing habits with hardware vendors, TV stations and even Google, without users usually being aware of this data being shared.

While there are, of course, legitimate arguments for the way in which highly personalised advertising, for example, helps to make markets more efficient (by better matching supply and demand), the integrated audio visual technologies or motion detectors that LRCDs increasingly have on board could mean that the question of personal data and privacy becomes even more complex. For instance, university researchers (Konow et al. 2010) have discovered that the sensors in some devices could gather physical or locational information about users and their gestures, while also recording audio, pictures and video from their surroundings. This constitutes a broader challenge than being simply about control of access to personal data, but rather about privacy relating to the integrity of the personal physical space around an individual. People may increasingly experience their locational privacy or physical personal space being intruded upon or unnecessarily monitored.

Indeed, vendors are anticipated to have new means and ways at their disposal to deliver targeted advertising through more advanced analysis of viewer preferences, and to build complex profiles of customers based not only on submitted information but also on measurements picked up by physical sensors in the ICLR. For example, media coverage (Grotticelli 2012) suggests that United States Internet

[9] This is defined as the claim or right of individuals to exercise a measure of control over the collection, use and disclosure of their personal information (Adjei & Olesen 2011).

service provider Verizon has filed a patent for a 'detection zone' enabled by smart TVs, which allows for the delivery of advertising based upon consumers' conversations. While Verizon's patent application was, according to news reports at the time, still pending (Meredith 2013), Microsoft has also filed a patent for a technology that allows its motion-capture Kinect device to count the number of people watching digital content on an Xbox in one room with the aim of adjusting the price for that content on a per-person basis (Ingersoll 2012). In the medium term, the technology might also provide a basis for selecting advertisement to target audiences with much greater precision.

2.3.1. Users seem often unaware of the use of their personal data in the ICLR

To date, there is little empirical evidence of users' attitude towards the collection of personal data, i.e. data which on its own or in conjunction with other data can be used to determine an individual's identity, in the ICLR. Indeed, the limited scientific evidence available ((Hurwitz 2011) merely suggests that the majority of users do not object to one of the most common type of personal data collection in the ICLR, namely the amount and type of media consumed through content providers, such as Netflix. However, it remains questionable to what extent users are actually able to make an informed decision about the use of their private data in the ICLR. Thus, some of the evidence we generated during interviews with Decipher Media Research (2013) and the Office of Fair Trading (2013a) suggests that it is received wisdom that LRCD users rarely read privacy policies nor terms of service agreements when signing up for a service, rendering them effectively unaware of the way in which service providers, like content or social media platforms, can use their personal data (Vu et al. 2007). A variety of academic studies (Spears 2013) have also found that consumers lack knowledge of behavioural tracking practices and their implications.

A general lack of awareness of prevailing personal data collection practices in the ICLR also seems to shape the data privacy expectations and personal data protection behaviour of UK smart TV users. Thus what seems to be a low general awareness seems to translate into equally low levels of expectations and personal data guarding behaviours. The market expert from Decipher Media Research (2013) consulted for this study summarised the result of a large-scale survey of the UK smart TV market and the behaviour of UK users:

> When I bought my smart TV I was confronted with 20 pages of terms and conditions and I was asked to read it all and say OK to it. An ordinary consumer gets to 3 pages and gives up. The problem is that it is all very complicated. If you ask a focus group how much they care about these things, they would tell you that they care deeply about them; they care deeply about their privacy. But in practice they are not exhibiting the behaviour. We worry about these things in a very passive way.

2.4. Some types of users are more vulnerable in the ICLR than others

Different user groups are likely to show different levels of susceptibility to security and privacy challenges that they encounter in the ICLR. Significantly, while existing statistical data, academic research, and the experience of security industry experts offer a somewhat inconclusive picture, age does not necessarily seem to constitute a useful indicator to categorise users in relation to their susceptibility to security threats and privacy breaches in the ICLR. Instead, different technology adoption patterns among users and

different personality types seem to constitute better indicators for describing users and their susceptibility to security threats and the loss of personal data.

2.4.1. Age may not explain why different people exhibit different data sharing practices

No data have been collected so far about the correlations between age and user security behaviour and attitudes in the ICLR. However, some expectations can be inferred from research into general Internet usage behaviour data conducted for the Home Office, which suggests that UK children and teenagers seem to constitute a more vulnerable group when it comes to Internet-enabled and dependent security challenges (McGuire & Dowling 2013). Only 70% of users aged 15–24 use security software, while 92% of the users aged 65 and over used security software (although it remains unclear whether this software is kept up to date). Only 37% of users aged between 15 and 44 were aware of ISP security features, which compares to 47–57% of users aged 35–65 being aware of such features (McGuire & Dowling 2013). There seems to be a negative correlation between increasing age and susceptibility to malicious code among UK users. Some 43% of UK Internet users aged 16–24 had been affected by a computer virus, compared to 34% of users aged 25–34 and 26% of users aged 55–64 (Smith et al. 2012). Only 11% of users aged 16–24 are concerned about the insecurity of personal details when shopping online (Smith et al. 2012), and only 5% of users aged 16–24 were concerned about the possibility of losing money or having money stolen as a result of online banking or managing finances. However, academic researchers Read and Beale (2009) suggest that children generally seem to have a good understanding of what personal data should be shared with a stranger, even though their understanding of who constitutes a stranger might be confused.

2.4.2. Digital literacy could be a differentiator of user data privacy practices

Several academics and security experts have suggested that 'digital nativeness' might be a useful category to explain why some individuals are more susceptible to challenges to security and privacy than others (Bennet et al. 2008; Helsper & Eynon 2010; McAfee 2013a; Symantec 2013a). According to the founder of the concept (Prensky 2001), 'digital natives', who were born during or after the general introduction of digital technologies and who adopt new technologies swiftly and interact with them on an almost permanent basis, are more likely to recognise the security and privacy implications of using certain electronic devices. In contrast, 'digital migrants', who were born before the existence of digital technology and who usually adopt new technologies with considerable delay if they do at all, often fail to realise the security and privacy implications of a device, even after it has been used for some time. While the concept of digital nativeness may well capture part of the explanation of different user privacy practices, two UK scholars (Helsper & Enyon 2010) have suggested that breadth of use, experience, gender and educational levels are in some cases more important than generational differences in explaining the extent to which people can be defined as a digital native.

2.4.3. Personality could be a differentiator of user data privacy practices

One security consultant interviewed for this study also suggested that personality fundamentally shapes users' susceptibility to security and privacy challenges (Symantec 2013a). Following this line of reasoning,

users who are generally more willing to share personal details with third parties offline may also be expected to be more liberal when it comes to sharing this information in their ICLR on social media platforms and thus with potential attackers or on content platforms and thus with hardware vendors and service providers.[10]

2.5. Industry also faces challenges in the ICLR

While the ICLR holds a wide range of opportunities for industry – not least in terms of the market for personal data discussed in the sections above – two developments are also of potential concern. First, as one extensive academic enquiry into the matter (Pereira 2011) suggests, industry is likely to face new challenges with regard to enforcing digital rights management (DRM) in an ICLR that hosts ever more seamlessly integrated devices and streamed media content. Second, industry is at risk of incurring reputational damage resulting from the 'loss' of data collected in the ICLR and related debates about interference with the privacy of users (see Section 2.5.2).

However, media consumption in the ICLR may also render piracy increasingly unattractive, as original streamed content is offered at competitive rates and quality expectations are on the rise. The representative of Decipher Media Research (2013) we interviewed for this study argued that 'convenience pirates' would be particularly likely to regard low-cost streaming services as a more attractive alternative to illegal streaming services.

2.5.1. The ICLR might give rise to new digital rights management challenges

The growing complexity of the ICLR and LRCDs could expose industry to a range of new DRM challenges. Although research on the topic and its implications is still in its infancy, we uncovered a market research analysis (Greenfield 2012) that suggests that the seamless integration of ever more LRCDs might render the consumption of pirated content in the living room much more convenient in the future, with tablets or mobile phones being used for finding pirated content, which can subsequently be consumed on the 'big screen' Likewise, market research firm Ipsos MediaCT (2011) has suggested that if users decide to increasingly use their smart TVs to access the Internet, which is so far not the case, the potential for the consumption of streamed pirated movies and shows on smart TVs could also grow. At the same time, NTBs, like Roku (Markworth 2011), advertise the fact that users can set up 'private channels' on their devices, which also can be used to stream pirated content to other users, posing a potential challenge to industry when it comes to enforcing DRM. At the same time, the ever-growing popularity of VoD apps on smart TVs and games consoles may result in an increase in the illegal recording of streamed content and the sharing of accounts, and encourage a growing number of people to bypass geographical location restrictions often built into these apps (Pereira 2011).

There is also a trend towards modifying LRCDs with the aim of getting free access to services or content. As one security expert (Symantec 2013a) consulted for this study noted, in the past PlayStation users have

[10] Notably, in the latter instance the information might also end up in the hands of attackers who manage to gain unauthorised access to platform databases (see Sections 2.2.1 and 2.5.2).

created modified versions of their games consoles, so-called 'modded games consoles',[11] which allow them to play games from illegally copied media. Such modification of games consoles not only raises DRM concerns but also acts as a catalyst of security vulnerabilities. Indeed, as Engebretson and his colleagues (2013) have argued, modded games consoles are usually excluded from patching routines, which makes both the software and the devices less secure.

The ICLR could also help to reduce the demand for pirated content

While the seamless integration and modification of devices in the ICLR could result in an increase in the consumption of pirated content in this setting, other developments in the ICLR render a decline in the demand for pirated content equally conceivable. Market researchers and informed media representatives (BBC 2013b; Brown 2013; Tassi 2013) have noted that users are much less inclined to consume illegal copies of content whenever content providers offer an attractive balance between the amount and quality of content offered and the price that needs to be paid to consume this content.[12] Considering the totality of programmes offered by media platforms such as Netflix, the consumption of individual pieces of entertainment not only comes at a minuscule price but also arguably at greater convenience than the illegal streaming of content (Tassi 2013). Significantly, Netflix and other comparable VoD services have suggested that they have reduced BitTorrent peer-to-peer sharing of pirated content in Canada by an estimated 50 per cent over the course of three years (BBC 2013b; Brown 2013), and while these figures have so far not been confirmed by any independent sources they resonate with findings from other streaming domains. Thus, legal games streaming services, like Steam, which offer games at highly competitive prices, are assumed to have contributed to a reduction of games piracy and modding (Tassi 2013).

Netflix and similar services are also regarded by market experts (Tassi 2013) to have reduced the general appetite for pirated content by raising ICLR users' expectations regarding the quality of video transmission. Indeed, the two university researchers (Blaich & Striegel, 2009) have even suggested that with the proliferation of high-definition VoD content the use of DRM mechanisms is increasingly less important.

2.5.2. Reputational damage could become the most pressing industry concern

One large-scale academic study (Hurwitz 2011) has established trust building as a key condition for encouraging consumers to exchange personal data and to complete commercial transactions online. Conversely, industry loss of users' trust can cause severe reputational damage and huge financial losses. As

[11] Modding usually consists of re-flashing or replacing the BIOS chip with a so-called 'modchip' that allows the user to play pirated games and to boot games from other, usually copied, media than the game would normally be delivered on. A modded games console also allows for the installation of a larger hard drive, thus eliminating the need for a CD or DVD. As a result, games can be backed up and played from the new hard drive.

[12] As one market expert consulted for this study (Decipher Media Research 2013) pointed out, this applies in particular to so-called 'convenience pirates', who not only have appetite for media content but also money at their disposal to spend on consuming such content legally. However, they are dissatisfied with the services digital content platforms provide, specifically as regards DRM practices and the movability and storability of digital media files, and their pricing policies. Indeed, they feel that commercial digital content services are inconvenient and overtly expensive, which prompts them to resort to pirated content.

was discussed earlier (see Section 2.2), two of the security firm researchers interviewed for this study (iSEC Partners 2013; Lookout 2013) have argued that the presence of a growing number of 'non-traditional' LRCD vendors arguably increases the risk for an entire industry to be exposed to negative publicity resulting from the public provision of insecure devices and platforms.

Companies with an established track record in manufacturing LRCDs and similar devices are also not immune to the new set of potential reputational and financial challenges emerging from the ICLR (Decipher Media Research 2013; iSEC Partners 2013). This was illustrated on 26 April 2011, when Sony announced that the personal data of over 77 million Sony PlayStation Network users had been stolen. According to news reports (*Guardian* 2011a; Rick 2011; Seybold 2011; Stuart & Arthur 2011), Sony temporarily shut down the Network and moved the physical storage centres as a mitigation measure (Seybold 2011). Even though the incident constituted one of the largest identity thefts in history at the time (CBC 2011), Sony did not divulge the precise nature of data theft until one week later, when the company announced that user names, addresses, dates of birth and log-in details had been stolen (CBC 2011). Moreover, in May 2011, it was discovered that the Sony PlayStation Network had also been hacked on a previous occasion, with an additional 25 million users' details being compromised (*Guardian* 2011b).

Besides the obvious vulnerabilities of Sony's security architecture, the Sony breaches also highlighted the fact that Sony had been storing potentially sensitive user data in an unencrypted format. The incident further illustrated that the exposure of user passwords could result in the hijacking of other online service accounts, as the hackers were able to use PlayStation Network passwords to access e-mail accounts and then use them for malicious purposes (Stuart & Arthur 2011). Despite a large forensic investigation that implicated the online 'hacktivist' group Anonymous (*Guardian* 2011a), Sony could not positively identify the source of the breach and offered 30 free days of PlayStation Plus, the premium PlayStation Network service, to PlayStation users as a compensatory measure. In addition, Sony immediately replaced the PlayStation Network servers and updated its terms and conditions to prevent class action lawsuits being lodged against them as a result of data losses (Rick 2011).

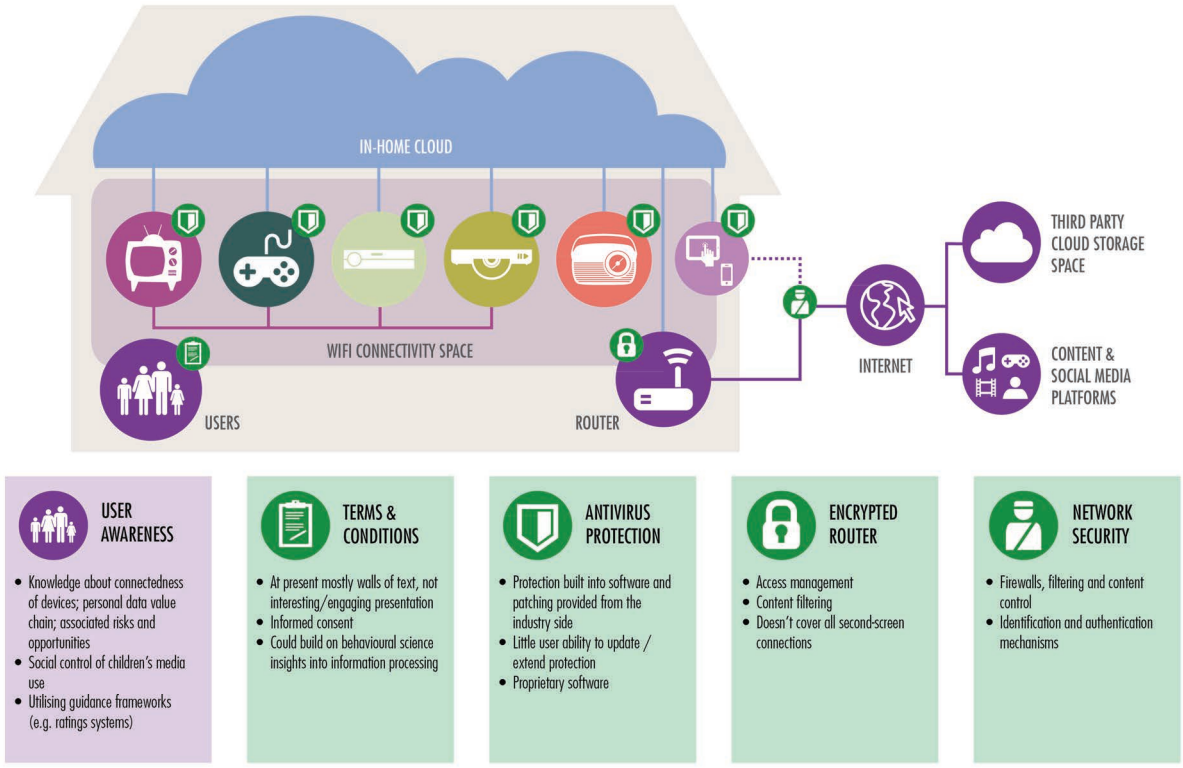
In the public domain Sony was widely criticised for an allegedly indifferent approach to the protection of user data. Moreover, Sony faced lawsuits from individuals and government agencies, with the UK Information Commissioner's Office (2013) fining Sony £250,000 as a penalty for compromising users' data. In the United States, the House Subcommittee on Commerce, Manufacturing, and Trade held a May 2011 hearing titled 'The Threat of Data Theft to American Consumers' to discuss the scale of the breach and the consequences for the protection of US citizens' privacy and security (Hearing Before the Subcommittee 2011). The negative publicity effect of the 2011 Sony PlayStation Network data loss incidents clearly underlines the need for industry to be vigilant when it comes to protecting the personal data of LRCD users.

3. Protecting users and industry in the Internet connected living room

3.1. Introduction

In response to the vulnerabilities examined in Chapter 2, there is a need to consider both technical and behavioural tools to strengthen security and privacy in the ICLR (as illustrated in Figure 3.1). These layers of technology and behaviour interact with one another, and technological protection measures will only function as intended if users have the appropriate skills and understanding to deploy them correctly.

Figure 3.1. Protection and awareness in the ICLR



Source: RAND Europe analysis.

Consumers and companies have a wide range of technical measures at their disposal to protect themselves and the content they consider private or copyrighted in the ICLR. Tools to confront vulnerabilities, protect against attacks and enable user control of accessibility exist at each level of the vulnerability chain outlined in Chapter 2. Available solutions can be found at the device-, platform-, service- and network-level of the ICLR. While the level of maturity and sophistication of these measures is often below those available for more widely embedded technologies, such as computers or mobile phones, there are some signs that industry processes may be evolving to support enhanced security in the ICLR domain.

Even when adequate technical tools exist, appropriate user behaviour is necessary to ensure that they function successfully. In the absence of easy-to-use and intuitive interfaces, users may be unable to benefit from a level of protection that reflects their preferences. By making solutions and incentives available for users to engage with their LRCDs more conscientiously, industry can help encourage responsible security behaviours.

Improved awareness mechanisms, including appropriate informed consent measures, are also critical in ensuring that users and the general public understand the balance of risks and rewards in the ICLR. Awareness should extend to the full range of security and privacy risks associated with LRCDs, including an understanding of business models in the personal data value chain and recognition of the full implications of enhanced connectivity.

3.2. Inadequate tools limit protection from emerging threats

Connected devices often include a range of default security options. These include measures for user authentication, identity management and protection against external attacks. Other tools are configured more as processes, such as the frequency with which devices get replaced or the cycle of security patches installed by companies. A third group of tools depend and act on the user's behaviour patterns and preferences. These include content control and parental overview as well as the device set-up guidance provided by companies.

3.2.1. Technology: as the availability of dedicated user-controlled security software is limited, LRCDs depend on a variety of other tools

Security providers aim to keep systems safe through automatic or manual security updates, similarly to traditional computing and mobile devices. For instance, some smart TV companies (including Samsung's) have security modules to prevent malicious apps from running (Samsung D Forum 2014). However, there are sometimes important differences between how this is done on LRCDs compared to PCs and other connected devices. One example of vulnerability in default security devices was found by technology journalists writing for TechRadar in the Opera browser running on Wii consoles: as the browser did not have a phishing filter, users could be exposed to phishing attacks when accessing the Internet via their Wii consoles (Rivington 2007). Similarly, another computer technology journalist for a German magazine, Eikenberg (2014), found that encryption security features (where the software checks the trusted provenance of safety certificates) were lacking on several models of smart TV operating systems, allowing external individuals to obtain login data for apps and access browsing sessions. This results in an overall

lower level of transparency and reduced user control over the security of LRCDs. While users performing risky interactions despite warnings is among the most salient concerns for traditional computer security, these concerns are somewhat less relevant for LRCDs, although users' willingness to engage with security setting on devices that often have a limited interface, as described in Chapter 2, can present limitations. Rather, as concluded by academic researchers Krol et al. (2012), their lower level of security often appears to be determined by the availability of appropriate tools for protection.

Furthermore, several LRCDs, such as Internet radios, lack an appropriate easy-to-use interface that would enable users to access and manage such built-in security settings. Consequently, the set of tools available to the user of a LRCD often depends mostly on the properties of the device purchased and its default settings, with little scope for the user to use upgraded security from a third party. In addition, even for devices for which protection mechanisms exist, several academic studies (e.g. Al Falayleh 2013; Herfurt 2013; Kuipers et al. 2014) indicate that their reliability may be limited.

Users have at their disposal a more restricted range of user-managed security tools, such as antivirus, antimalware software or removal tools, on LRCDs. While applications running on these devices, such as browsers, might have their own security plug-ins, most connected devices rely on other factors for security, such as replacing devices, automatic security patches and network-level security tools.

Encryption capabilities are under-utilised

Devices use encryption to maintain the confidentiality of the data being transmitted. Academics Iyer et al. (2012) stress that encryption used together with authentication and identity management can be a powerful tool in preventing large-scale security breaches, especially when these elements are designed in a way to support each other. An example of harm cited by Iyer et al. (2012) and SafeNet technology commentator Ocampo (2011) that could have been potentially prevented by encryption is offered by the Sony Playstation breach in 2011, which has been imputed to a lack of links between authentication and encryption. However, despite their widespread availability (for instance in LG connected systems, see LG 2014), an interviewee from a security company suggested that built-in or optional encryption capabilities are often not activated by manufacturers or users (Symantec 2013a).

DRM technologies developed for PCs might not be suitable for LRCDs

DRM tools are important to protect content and assure digital rights. At present, there are seemingly few fundamental differences between the tools utilised for DRM on PCs and on those devices found in the ICLR. However, the adequacy of such measures to protect content consumed in a connected living room setting might be inferior. One area where DRM technologies and solutions are challenged by the development of LRCDs is the maintenance of digital rights protection across a complex value chain that is emerging in the market for these devices and services (see Chapter 1 of this report). The wide range of players involved in the market, which includes app developers, platform providers and ISP companies as well as hardware manufacturers, means that there are even more channels through which DRM has to be considered. For example, upon a compromise of cryptographic protocols used to protect content, the means to revoke the compromised code or update the available tools to close the vulnerability could involve several of the above-mentioned actors at the same time, resulting in a potentially higher level of diversity than in a PC-orientated domain.

Table 3.1 summarises the most commonly used DRM methods:

Table 3.1. DRM instruments

Instrument	Relevance for LRCD
Encryption	Non-legal copies of software or content (e.g. DVDs, games) cannot be played on the device.
Limited number of plays/installations	It could be difficult for users to transfer games between their devices or re-install their systems following a security update if these actions go beyond the permitted number of installations.
Blocking URLs associated with P2P sharing or streaming of illegal content	Addresses can be blocked at the ISP level, e.g. filtering obligations of ISPs in the UK. However, the blocking of these sites is not without some controversy.
Denying content compatibility on devices with weak DRM mechanisms	LRCDs using this system may be at a competitive disadvantage compared to devices with DRM mechanisms judged to be more reliable by content providers.
Audio watermarking technologies	Embedded features in LRCDs, such as Cinavia, can detect if content is pirated by searching for inaudible sound codes produced by legitimate vendors, and then cancel the playback of content that lacks the watermark. This also may hinder the playback of legitimately copied or converted files.
'Always on' DRM	This mechanism relies on constantly authenticating the product via a constant online connection, meaning that products (e.g. games such as Sim City) can only be used when the device is connected to a server. However, this protection method is vulnerable to accidental losses of connectivity which can diminish the user experience, as well as denial of service attacks. According to the Xbox Wired official blog, negative user feedback on this type of DRM was one of the reasons why Microsoft revised its original plans to deploy always-on DRM on the Xbox One (Mattrick 2013).

Finally, noting the recent LG data collection case (*Guardian* 2013a), device manufacturers have the capability to include software that reads files stored on hard drives connected to the device. These could enable monitoring of digital-right-infringing content consumed through LRCDs, such as in the case exposed by a blogger in connection with LG smart TVs, but is also understandably seen as a privacy concern (DoctorBeet's Blog 2013).

Network-level security

With limited user control of the security settings of individual devices, network-level security settings, including firewalls, filtering and content control, are important in determining the level of protection available to the ICLR. Network-level solutions have also been identified by a security company interviewee as the 'next level' protection mechanism for the living room, accompanying (or superseding) those for authentication and patching (Symantec 2013a). These both refer to the home network, which can be managed through a router, and the overall network, managed by the ISP.

In some cases, network-level protection appears to be the preferred option against risks and vulnerabilities. For instance, a blogger who uncovered the recent LG smart TV data collection practice advised that users should disable access to certain tracking and profiling sites at the home router level – the only potential solution to limit access to the files stored on the devices connected to the TV (DoctorBeet's Blog 2013). Further upstream, network-level mechanisms such as security at the cloud level and other, network-level security features geared towards PCs might be applicable to content delivery systems through LRCDs, such as the filtering services being offered by UK ISPs.

3.2.2. Authentication: new technologies for intelligent user identification

Authentication allows a user to prove their identity to the system network or platform they are accessing and hence be permitted to perform a set of actions. One of the most widespread authentication mechanisms is the insertion of a secret security 'key' (usually a password) that links the user's account to their identity. Often a single authentication can prove identity to several services. For instance, academic security researchers Engebretson et al. (2013) discovered that once a user accesses their Xbox Live service, messages sent from their account are assumed to be from that particular user. While these features are useful in supporting service usability (the argument is made that re-authentication for every action would be inconvenient), they also rely significantly on a single approach to delivering security.

Secure systems on LRCDs and platforms and networks accessed through these devices include those that enable users to access and manage security settings (for example setting and resetting passwords and security questions). Keeping authentication mechanisms secure is crucial in preventing unauthorised access to devices and denying unauthorised users the capability to assume the credentials of another person, thus playing an important role in fraud prevention. However, innovation in services and the expanding uses of living room technologies by potentially vulnerable groups of consumers such as children, digital migrants or the elderly (see also Section 2.4 of this report), and in sensitive settings (e.g. for home monitoring services for the elderly) also underscore the need for such mechanisms to go beyond PIN-based authentication mechanisms and leverage the technological possibilities enabled by new settings and interfaces. Recent areas of academic research in authentication systems, for instance the work conducted by Ben Hadj Mohamed et al. (2012) and Anido et al. (2013) include, for instance, biometrics, voice recognition or three-dimensional motion recognition.

3.2.3. Identity management questions underscore the discrepancies between data-hungry companies and the privacy of users' data

Identity in information systems, as opposed to authentication discussed above, is defined by Windley (2005) in his book on digital identities as the collection of traits, attributes and preferences linked to the user, ultimately resulting in the online representation of a specific (human) individual. There is an increasing overlap between identity management and authentication. Identity management concentrates on control of user access to system resources, usually by associating rights and restrictions with an identity, e.g. users comment on content from Netflix on their Facebook accounts without the need for re-authentication between the services. Cavoukian (2006), a researcher from the Canadian Information Commissioner's Office, has emphasised that interoperable identities, while increasing usability and ensuring a more convenient user experience, may increase exposure to vulnerabilities in terms of identity theft and fraud. Technology sector journalists Lennon and Geller (2013) and operations management researchers such as Clemons (2009) stress that at the same time, implementing interoperable identity management makes it possible for services to gather more information (both data and meta-data) about the characteristics and behaviour of the user for profiling and targeting purposes. As explained in Section 1.5 (and supported by the academic literature, e.g. Clemons 2009), this user data is a key attraction for private sector actors, which are looking to build monetisation of personal data into their business models.

Identity management is increasingly relevant in the ICLR as in the PC-oriented world, where several of the devices provide access to platforms that can act as managers between multiple online personas and communities constructed for the same user, as discussed throughout Chapter 1. For example, consumers can login to a variety of websites using their Facebook credentials and easily share web content across multiple platforms (e.g. between Twitter and Facebook). However, an added level of complexity for identity management emerges from the social practices surrounding the use of these devices. According to computer security researchers Suarez-Tangil et al. (2013), if TVs, DVD players and games consoles are often used in the presence of more than one person, determining and managing identities in such a setting becomes more difficult. For instance, according to MIT's Sollins (2011) security settings, content controls, child protection tools and data gathering can be more or less appropriate based on the composition of the group that uses the device; e.g. when the group comprises largely children, a higher level of protection may be necessary, while adult users may approve of data gathering for certain purposes.

While it is easy to concentrate on the vulnerabilities resulting from cross-platform identities and a reduced number of prompts for user authentication, these measures enable a better user experience by increasing the usability of technologies. However, as explored in Section 2.3, and supported by the academic literature which we uncovered during the course of this review, e.g. Adjei and Olesen (2011), some limitations in the capability of these tools to efficiently protect users stems from a view held by academics that researchers and developers of user-centric identity management systems have mainly focused on making existing identity control architectures interoperable, as opposed to putting privacy at the core of the identity management system design.

In this context, another challenge is making sure that users understand the identity control policies of the services with which they are engaging. Increasingly seamless cross-service identification makes it more

difficult for users to realise which services they are signed in to at any time and what data is collected by these services.

3.2.4. Industry processes support potential security improvements

The main resources that provide security on LRCDs, as discussed in Chapter 2, are represented by the rate at which users upgrade their devices to more up-to-date (and supposedly, more secure) models; patches issued by manufacturers; and, to a certain extent, the characteristics of the software running on these devices.

While the maturity of security tools (especially those over which the user has a degree of control) appears to be at an early stage of development, the current generation of Internet connected devices exists in a dynamic market; as companies keep improving their devices, consumers replace their devices at an accelerating pace. This trend has been confirmed by the academic literature (e.g. Vinayagamoorthy et al. 2012).

At the same time, even though the overall availability of dedicated security software remains limited, manufacturers do also offer patches that integrate and update the features of the devices already on the market. For example, the instructions for Sony's update process for its Bravia range of TVs describe a complex and irreversible range of steps involving downloading an update to the firmware to a USB drive, extracting the file and then installing it (Sony 2014). However, as pointed out by information security researchers Engebretson et al. (2013), the frequency and availability of these patches may not be consistent across devices. Their efficiency, however, also depends on the willingness and skills of users to update and install more secure software or update the settings on their devices.

In addition, another software-based support option that can help increase security levels even as user-controlled antivirus and antimalware tools remain limited stems from the operating systems running on the devices. LRCDs often run on proprietary software or specially adjusted variants of the Linux Open Source Software distribution. According to an interviewee from a platform provider, this strategy is supposed to offer a much less attractive target for malicious attacks (Steam 2013). According to technology journalist Chickowski (2013) writing for information security portal DarkReading, the diversity of software environments, while not stemming from security concerns, has offered a certain degree of resilience as attackers would need to develop many different versions of malware to attack a large number of different devices.

3.3. Secure user behaviours may be either constrained or enabled by default security and content control settings

In securing the ICLR, a crucial factor is users' awareness level of potential risks and the extent to which they use security tools and settings. Awareness in this context includes knowledge of communication by companies about security (both via user manuals and through other channels) as well as the provision of parental and content control tools at the device and network level.

3.3.1. Security guidance in user guides

User manuals for LRCDs will typically have a dedicated section on setting up and managing the device. However, while these documents, for instance those provided by Nintendo or Microsoft, often give warnings on the potential health hazards of using the devices (such as repetitive motion injuries or motion sickness in the case of games consoles) stemming from compliance with safety standards (Nintendo 2014a), they do not always contain additional information on security features or how to best set and monitor configurations in these when setting up the machine (Microsoft 2014a).

3.3.2. Protecting devices by disconnecting them

In the absence of dedicated security tools, consumer advice provided by the popular press are that users should not to use the capabilities of their devices or alternatively employ strategies to reduce vulnerabilities by hampering the connectivity of the device (*Telegraph* 2014). For example, following the experimental demonstration of vulnerabilities in Samsung smart TVs at the Black Hat Security Conference in 2013, the news website CNN Money received a statement from Samsung that users, if concerned, could '…unplug the TV from the home network when the Smart TV features are not in use' (CNN 2013). According to security company McAfee and technology journalist Bode (2012) writing for the specialist magazine Broadband Reports, these methods are already used by a significant portion of smart TV owners (Bode 2012; McAfee 2014). For instance, McAfee advises games console users to: 'Disable game consoles' Internet access to remove the probability of downloading a virus and opt for local game use only' (McAfee 2014). This directly goes against the grain of why these devices are popular: multiplayer gaming. Similarly, as reported by technology magazine HD Guru, Samsung advised users, as an added precaution in addition to changing the settings to disable the camera, to rotate the webcams of their smart TVs towards a blank surface: 'Should the TV owner choose not to use these features, the camera and microphone can be disabled. Users can check if the camera and microphone are activated from the TV's settings menu. As an added precaution the camera can be rotated and tucked into the bezel of the TV. Once tucked away, the camera only captures a black image' (HD Guru 2012). This approach, however, would be ineffective against the sophisticated threats outlined earlier, as it only limits the use of some functionalities of the device: data extraction, for instance, would still be possible.

3.3.3. Content control and parental control mechanisms are often limited by behavioural patterns and supported by social practices

One of the most pressing concerns related to connected devices is the potential risks that children are exposed to through them, as investigated by London School of Economics researchers (Livingstone et al. 2011) among others. At the same time, controlling and reviewing young users' consumption of online and broadcast content has been an issue that policymakers and actors along the value chain have been engaging with since these technologies have become mainstream.[13] In some countries (including the UK),

[13] An example is the EU's inclusion of 'Making the Internet a safer place for children' among the goals of the Digital Agenda flagship initiative or the establishment of the UK Council for Child Internet Safety. See European Commission (2013b) and UK Council for Child Internet Safety (2012).

content filtering technologies have been put in place at the network level. Limiting or blocking access to websites promoting or facilitating illegal activities has been advocated by digital rights holders and law enforcement agencies among others, but certain aspects of this are opposed by civil liberties organisations, such as the Open Rights Group (see e.g. Open Rights Group 2014). These concerns remain relevant in the context of the ICLR, where devices make access to both of these types of content available to users. Measures to exercise control include content control mechanisms and parental control options that can be set up at the device or network level.

Network-level content management and filtering

Academic literature, e.g. Fernandez Villamor and Yelmo (2011), describe how protocol-specific authorisation management mechanisms installed at the network level can make access decisions based on previously defined policies and user identities. These authorisation management mechanisms could, for instance, determine what content to make available on the TV for an adult user as opposed to a child. In order to differentiate between users, these mechanisms build on identity management resources (see Section 3.2.3) – linking rights to user profiles. We discovered an example of this called 'Oversee' which was developed in 2011 as part of a Research and Development project run by a consortium of Spanish companies, universities and research centres related to telecommunications security in conjunction with Ericsson Research.

Fernandez Villamor and Yelmo (2011) proposed to extend the control of network-level mechanisms beyond simple connection to user profiles to include more complex actions to serve child protection objectives. They could, for example, distinguish between social networking 'friend' requests arriving from adults or children, permitting children to interact with others their age but not with unknown adults.

On the other hand, another technique is the filtering of content. This is defined as based on routing certain types of traffic, as chosen by the user, through a physical component (router) or through software that analyses and filters content. This type of filtering evaluates content according to the user requesting it, the nature of the content itself and the resource involved, to determine whether to allow the action based on a preset policy or the profile of the user that is logged on to the device or service. Through this mechanism, the filtering also depends on the identification of the user (see Sections 3.2.2 and 3.2.3). The person in control of the policy sets categories of content that can be allowed or forbidden, or sets a predetermined list of addresses to be included or excluded (white lists and blacklists, respectively). Such lists can be constructed ad hoc, or based on rating systems that are made available to the public.[14] Computer science researchers Fernandez Villamor and Yelmo (2011) and Matsuno (2012) also suggest that these tools have their limitations: they cannot analyse encrypted content, and they pose privacy hazards by interposing an additional chain in the content's route.

Content filtering is not only implemented for the means of child protection. In the UK the most prominent instances of network-level content filtering beyond family-friendly filters are the filters adopted by UK ISPs. This filtering technology was originally introduced under the British Telecom Anti-Child-Abuse Initiative to block sites related to illegal content (such as child sexual abuse images) further

[14] See for example RTA (2014) or SafeSurf (2014).

upstream, in 2004. Since then, as reported by University of Amsterdam researchers Nooren, Leurdijk and van Eijk (2012), its reach has also been extended to target sites associated with P2P sharing of illegally copied DRM content through a High Court order.[15] The Cambridgeshire-based Internet Watch Foundation (IWF) also maintains a blacklist of potentially criminal web pages, which in 2009 the government strongly encouraged all UK ISPs to use (Expert Reviews 2009).[16]

Parental control services

Although most parents in the UK trust their children's ability to use the Internet safely, they are also concerned about potential risks that young users may encounter online.[17] Ofcom's research into parental attitudes towards managing children's Internet use (Ofcom 2014) suggests that parents use a range of strategies from communication and supervision (including social media monitoring), to the use of technology-based controls (through ISPs, preinstalled operating systems or third party software) to manage their children's access to the Internet, including access of Internet through games consoles and other devices. While network-level content filtering offers tools to monitor and block certain categories of content and access to specific websites, researchers studying parent–adolescent interactions (Padilla-Walker & Coyne 2011) found that parents still prefer retaining a high level of control over their children's media usage, wanting to set content control guidelines themselves rather than following defaults set by ISPs or manufacturers.

Symantec (2009) reported that the parental control options on LRCD devices targeted to younger audiences, such as games consoles like models of the Xbox, Playstation and Nintendo Wii, are equipped with options for content access, but also behavioural options such as the length of time a user is allowed to play. At the same time, opportunities for parents to better protect their children from cyberbullying on online gaming platforms are present. For instance, Sony informs its customers that the PlayStation Network offers parents the option to create a 'Sub Account' for under-18s, which prevents the transmission of text and voice chats via the console (Sony 2014).

Similarly, the Xbox website informs users that Xbox Live has a variety of parental settings that can regulate messages that children receive and require approval for any friend requests made through the Live network (Microsoft 2014b).

However there are devices that do not present an easy-to-manipulate interface (such as Internet radios and DVD/Blu-ray players). Anthropological research conducted by Bernhaupt et al. (2008) found that in-person control of device use and media consumption can often supplement or be used in place of automated content filtering options, which could be a way of supplementing these controls or replacing them in the absence of easy-to use software and interfaces.

---

[15] High Court case HC10C04385 (BAILII 2011).

[16] The most recent publicly available data which we could find from 2009 suggested that 95% of all UK ISPs used the IWF blacklist.

[17] 52% of parents of 3–4s, 72% of parents of 5–7s, 83% of parents of 8–11s and 89% of parents of 12–15s said they are confident in their child's ability to use the Internet safely (Ofcom 2014) At the same time, around a quarter of parents said they were concerned about cyberbullying and their children downloading harmful content such as viruses. One in six parents was concerned about inappropriate content, and one in five reported being worried about their children giving out personal information.

In-person control of media use

The academic literature looking at children's Internet and media consumption (e.g. Bernhaupt et al. 2008; Livingstone et al. 2011; Ofcom 2014) has underlined that in addition to technical tools, informal monitoring of children's technology use is an important practice, often seen by parents as a corollary or a substitute for technology-based measures. These practices, based on being present while the child uses a device, are especially relevant in the living room context, where content is often consumed in a shared setting. Academic researchers on digital identities, such as Sollins (2011), also stress that social measures, such as advice from family and friends, can offer a solution to identity management problems raised by multiple people accessing content through a smart TV which may not be appropriate for all members of the group, or in the case of devices without an interface or the ability to change parental settings.

Empirical research conducted by Bernhaupt et al. (2012) illustrates that many parents prefer to monitor in person their child's media usage. Ofcom's research into the topic has found that in the UK in particular, young people's media and technology use is closely monitored by parents, using a mix of controls and mediation (Ofcom 2014). A London School of Economics research group on children's online behaviour has concluded that while no specific data are available for Internet connected technologies found in the living room, 87 per cent of UK children say that they are either not allowed to do some online activities (disclose personal information, upload, download, etc.) from a list or that they can while under parental restrictions (Livingstone et al. 2011). The same research reports that monitoring strategies for Internet use are adopted by 55 per cent of UK parents, making this somewhat common. However, positive support is a more favourable approach; used by more than 70 per cent of parents, this strategy involves giving children safety guidance or making rules about Internet use, such as limiting the time or places where Internet use is allowed. Some 54 per cent of UK parents say that they block or filter websites at home (compared to a European average of 28 per cent), while 46 per cent say they use technical tools to track the websites visited by their children (compared to a European average of 24 per cent) (Livingstone et al. 2011). These findings are far higher than in Europe generally, with the UK topping the country ranking for use of filters (Livingstone et al. 2011). It is worth mentioning, however, that an earlier study conducted for Ofcom found that the use of parental control devices is often limited by behavioural factors, such as parents finding their management complicated, forgetting to activate or update them, or children 'getting the upper hand' in decisions about their use (Jigsaw Research 2012).

Content labelling

Several platforms, like Microsoft's Xbox Live Zune video marketplace or Sony's Sony Entertainment Network (SEN), which deliver content to LRCD users rely on supplementary labelling and classification schemes. These systems often follow industry guidelines on labelling and categorising content (e.g. the content provided by YouView or the British Board of Film Classification (BBFC) ratings for age categories on films) and products (e.g. videogames) according to their appropriateness for age groups or whether they contain potentially offensive elements or violence (BBFC 2014). The Pan-European Game Information (PEGI) rates computer and video games according to the appropriate audience for each game (like movie ratings), displaying ratings on the packaging of products in an easy-to-understand label form. It is backed by public authorities such as the European Commission and was established with the explicit goal to help European parents make informed decisions on buying computer games (PEGI 2014). It is

currently used by 30 European countries, where it replaced national content rating systems for videogames. The PEGI system, similarly to the US Entertainment Software Rating Board (ESRB) age rating system, was developed by an industry association. Both PEGI and ESRB are also supported by the major console manufacturers, including Sony, Microsoft and Nintendo, as well as by publishers and developers of interactive games throughout Europe. In 2012 PEGI announced that they had launched a classification scheme for apps (PEGI 2012) which was intended to illustrate whether certain apps could be used to make in-app purchases, share personal or location information or allow social interaction.

Community-based content control

In addition to parental control and content filtering tools, the latest generation of consoles and their associated platforms are also offering ways of countering cyberbullying and online grooming reported on their platforms by the user community. Xbox Live, for example, has recently announced the launch of 'Enforcement United', which will in the future allow all members of the Xbox Live user community to report offensive or threatening behaviour to an Xbox management team (Xbox Enforcement United 2014). Similarly, as reported in a post on the Google official blog, the terms of service of several platforms that may be accessed through LRCDs (such as YouTube or social network services) offer opportunities to report offensive or illegal behaviour and have content removed (Google Policy Center 2014; YouTube 2014). These services support consumer and child protection goals by extending reporting and control over offensive content beyond the singular parent (who may not be able or willing to interact with parental controls to a level that mirrors their preferences about the content available to their children) and by involving industry such as platform providers for the content exchanged and hosted via their services.

3.4. Raising user awareness can improve security

With many security outcomes ultimately depending on the extent to which users behave in security/privacy-conscious ways, academic research, for instance Prensky (2001), suggests that raising user awareness and digital literacy in general is an important tool in preventing harm from attacks, breaches and incidents (see Chapter 2). Awareness should extend to the following areas:

- The business models in the personal data value chain (see Chapter 1)
- The capabilities/connectedness of the devices (see Chapter 1)
- The security and privacy risks associated with LRCDs (see Chapter 2).

Encouraging greater understanding of the capabilities, benefits and risks discussed in Chapters 1 and 2 for instance, based on the research of Smith et al. (2012) on harms and concerns in the ICLR, can be particularly useful in increasing the security and confidence of consumers. However, as with security and privacy on the Internet generally, academic research on awareness of risks and privacy challenges confirms that these are challenging areas for the layman to understand (see e.g. Hansen et al. 2008; Spears 2013). The potential ways for managing awareness and data protection overlap to a large extent with those that are relevant in the context of surfing the web, such as awareness-raising campaigns, clear and readable terms and conditions (such as the ones indicated by the review of behavioural science research applied to the area in Helberger (2013)), and tools that allow for a partnership-like approach to data control and

management. Industry also plays a crucial role in implementing and operationalising these tools, although consumer protection organisations and governments are useful interlocutors.

3.4.1. Media coverage of attacks and awareness raising about risks

One way that awareness increases is through media coverage of particular events. Media analysis conducted by academic researchers Löblich and Karppinen (2014) found that media coverage of communications technologies has increasingly focused on privacy and data protection issues in recent times. While the causal link between media coverage and changes in legislation on safety and security is unclear, in several cases adverse publicity has contributed to changes in company practices by highlighting the inadequate or unsatisfactory nature of their products or services. Such practices were analysed by researchers Hoadley et al. (2010) following Facebook's Privacy News Feed outcry. Internet surveillance and high-profile hacking cases have been identified by industry experts consulted for this study as suspected important future drivers of awareness amongst users about the potential risks of technologies that they have grown accustomed to using (Office of Fair Trading 2013a). At the same time, two of our interviewees – one from a company conducting market research and user studies connected to LRCDs and one policymaker – found it important that the public debate over surveillance (albeit in a different context) illustrates the extent to which companies are considered a crucial actor in ensuring ethical handling of data, potentially contributing to users' expectations about their role in protecting their customers (Decipher Media Research 2013; Office of Fair Trading 2013a). This applies also to LRCDs, as incidents involving these are often covered in the media, for instance as reported by technology journalists from the *Guardian* (2011b) and the specialised magazine *Broadcast Journal* (Grotticelli 2012). However, information about breaches, vulnerabilities and the potential of LRCD technology also flows from other stakeholders, most importantly manufacturers, consumer groups, social media and regulatory authorities. In relation to children's technology use, the LSE's research mentioned above (Livingstone et al. 2011) found that parents, teachers and friends from a peer group have also been found to be among the most important active mediators in safe Internet use, a trend that could be potentially similar for Internet access and safe use of devices in the ICLR.

3.4.2. Terms and conditions and privacy policies don't exploit all possibilities to communicate clearly

Documentation, such as terms and conditions and privacy policies, have a role in communicating to users the privacy and security risks and secondary uses of their data, as discussed in Chapters 1 and 2. Such documentation is provided under regulatory obligations (such as under the Data Protection Act 1998 and the Privacy and Electronic Communications (EC Directive) Regulations 2003). Following media attention on security and privacy issues in connected technologies, some industry representatives, including ISPs and manufacturers, have been active in raising awareness about engaging with the privacy policies or T&Cs of devices and services. An example of this is Google's push notifications that prompted users to consult changes in the privacy policies around the time it introduced a single privacy policy for all its Internet services in 2012 (Google 2012). Some companies, such as Google in the case of the aforementioned privacy policy update, have also made efforts to communicate these in easy-to-understand

terms for users with non-legal backgrounds. They also underline the importance to consumers of reading and understanding these, for instance using push notifications about updates.[18]

However users provide their consent based on highly complex textual information. Media researchers Luger et al. (2013) scored the terms and conditions of UK websites along the scale used to assess the complexity of texts for reading ability exams and after analysing a sample of T&Cs from the UKs big six energy providers found that they were far beyond what an average adult could be expected to understand. Therefore, even in the case that a user read the documents provided, it would appear unlikely that they manage to extract all relevant information from the text. Improving readability as a route for encouraging consumer understanding of T&Cs was drawn out in the interview conducted with the ICO for this study.

Academic research by Helberger (2013) and University of Amsterdam researcher Zuiderveen Borgesius (2013) stresses that the outcomes to date of these initiatives are limited in scope and effectiveness. One of the main reasons for this limitation drawn out by Zuiderveen Borgesius (2013) and Rotterdam university researchers Faure and Luth (2012) underpinned by the field of research of behavioural economics is that people most often do not read lengthy documentation, not even when they know that it contains important information that impacts on them (e.g. in the case of mortgage contracts or standard contracts). Marotta-Wurgler (2011) conducted academic research on the readership of end user license agreements (EULAs) of software products. The study analysed the clickstreams of almost 50,000 households, and concluded that the overall average rate of readership of EULAs was on the order of 0.1 per cent to 1 per cent. Even the users that did look at the terms did not do so long enough to read them effectively.

Finally, users' behaviour is subject to a series of behavioural biases. For instance, the work conducted by academic researchers into privacy-related behaviours suggests that users tend to underestimate the risk of identity fraud or other negative outcomes that come from not reading policies; at the same time, myopia in decisionmaking makes users value short-term outcomes (e.g. access to the services they want to use) more than potential future risks in the longer term (Acquisti 2009; Acquisti & Grossklags 2005). In sum, consent and understanding of terms and conditions cannot be taken for granted, even when all the relevant information is provided to the user.

Online service providers and retailers regularly strive to convey complex usage information about their products in a compelling and enticing way, using interactive approaches such as embedded videos, for example those that can be found on the Nintendo web page to describe their products (Nintendo 2014c) However, academic research conducted by Helberger and her team found that the same often does not seem to be true for information about privacy and terms and conditions related to the same products (Helberger 2013). Similarly, Helberger's study emphasises that while tools to make information easily understandable and attractive to users are often deployed in presenting product information to consumers, they are not employed to present terms and conditions and privacy policies (Helberger 2013). An example of this can be found in some of the websites relating to LRCDs, such as Apple TV's or

[18] Push notifications are pieces of information provided by the central server of a service even when the user is not actively engaging with the service. See, for example, Google 2012; however, it is worth noting that the changes brought to Google's privacy policy itself have not been uncontroversial and have, among others, resulted in a fine from the French and Spanish data protection agencies (see AEPD 2013; CNiL 2014).

Nintendo's, where user information about the devices is presented in personable, enticing and visually interesting ways (see, for example, Apple 2014a; Nintendo 2014b); privacy policies and the terms and conditions applicable to the same product, however, are accessible through a link positioned in a non-prominent position and presented via a 'wall of text' (see, for example, Apple 2014b; Nintendo 2011). The extent to which regulatory obligations drive industry to articulate policies in this way – 'drafted for lawyers by lawyers' – has been noted as general characteristic of the personal data-enabled economy by academic research (Robinson et al. 2009).

In conclusion, issues remain regarding the sufficiency of information provided to consumers and the behavioural outcomes of the ways people interact with terms and conditions, including in situations where it cannot be guaranteed that the user has read and understood the information he or she has 'consented to' or where the only alternative to not agreeing to a policy is for the consumer to not use the service.

4. Potential ways to increase the security of living room connected devices

4.1. Introduction

This chapter identifies some possible avenues available to address the security and privacy challenges in the ICLR. The choice of and whether the use of such tools is warranted will need to be driven by a good understanding of how the ICLR is evolving and how the roles and responsibilities of each player in the value chain play out. Careful consideration will need to be given to the right measures that will satisfactorily address the privacy and security challenges without losing sight of the opportunities offered by the ICLR.

At a basic level, it is important that key players in the LRCD landscape keep apprised of the evolution of the ICLR and adapt their roles and responsibilities accordingly to ensure that consumers are provided with appropriate security and privacy safeguards.

User behaviour plays a key role in securing the ICLR. There is significant scope to develop both technical and non-technical tools to encourage more conscientious use of connected devices.

Improved communication between all parties can help achieve transparency and reduce risk associated with use of LRCDs. Media campaigns and point-of-sale information can be productively utilised to spread awareness about potential security concerns, leading to strengthened security awareness and behaviours. Improving general understanding of personal information usage in the value chain can also help users give informed consent while offering industry opportunities for competitive advantage.

Looking ahead, partnerships offer a potential way forward to address the security and privacy challenges of LRCDs without undermining the positive impacts of innovation in this area. By working together, users, industry and regulators can work to strike the right balance between protection and opportunity in the emerging ICLR environment.

4.2. There is a need to follow the evolution of the LRCD value chain

As Chapter 1 has indicated, the types, nature and responsibilities of players in the ICLR is becoming increasingly diverse. This diversity suggests that responsibilities which were traditionally relatively clear are becoming more opaque. There would thus appear to be a need to observe the evolution of the ICLR value chain carefully to ensure that important issues such as fairness, consumer protection or enforcement of the right to the protection of personal data are well managed. Regulatory bodies, government departments

and consumer protection organisations would need to keep pace with these developments: they might need to engage with existing stakeholders on new issues (for example, speaking to traditional broadcast players about how to manage usage of personal data) as well as reach to new stakeholders (e.g. firms such as companies whose platforms are accessible through LRCDs) about issues like threats to consumers or the role that these challenges might play in affecting consumers' access to an open, fair and transparent marketplace.

4.3. A number of existing tools could be adapted to promote a more secure ICLR

As discussed earlier in the report, the ICLR provides a new 'means' for many existing online security and privacy threats. It is therefore possible that general tools already used to enhance Internet security could be adapted to effectively address the challenges which are emerging through increased use of LRCDs. Academic researchers Cave and Marsden (2008) provided a detailed categorisation of these existing Internet security tools in a study for the European Commission that considered which approaches were best to tackle some of the emerging challenges for regulation in the Internet age. Table 4.1 thus summarises some of the existing mechanisms with varying levels of government and industry involvement and identifies their relevance and advantages for the subject of this study.

While there is a wide range of possible soft measures and alternatives to top-down regulation, evidence from an interview conducted for this study with a consumer association highlighted a preference toward regulatory measures in incentivising privacy- and security-conscious practices by companies. Such a view is perhaps understandable given the perception in consumer organisations and the media that for some issues, strong regulatory intervention is the only effective solution – a similar view was voiced by our interview with a consumer organisation (European Consumers' Organisation (BEUC) 2013). One of the interviewees, a consumer organisation, emphasised the need for stronger enforcement of the existing rules and the potential for industry initiatives to support top-down efforts, but the interviews emphasised the role of regulators in setting up a framework (BEUC 2013). Industry, on the other hand, underlined the importance of making sure users understand how their data is collected and used and the role of industry associations in mediating security, privacy and consumer protection preferences. A cybersecurity firm consulted for this study held such a view, perhaps understandably given their role in mediating and enabling security aspects of such a market for personal data (McAfee 2013a).

Table 4.1. Internet security measures which may be adapted to support consumer protection in the ICLR (in order of severity of impact)

Type of measure	Examples in force	Relevance for LRCD	Advantages	Disadvantages
Self-Regulation	Content classification schemes (e.g. ESRB)	Supporting parents and carers in making decisions about rules for children's media consumption	Bottom-up (industry identifies viable solutions with limited government intervention)	Limited oversight from government to ensure consumer protection objectives
Industry guidelines	Office of Fair Trading (OFT) guidelines on in-app purchases	Protecting children and vulnerable consumers when accessing apps thorough LRCDs	Flexible guidance can evolve with technological progress	Redress mechanisms not always clear to consumer
Terms of service of platforms	YouTube, Facebook, Google Plus ToS	Filtering offensive / illegal content	Leveraging the collective power of user communities	Filtering decisions often not without controversy
National legislation	UK Consumer Bill; Consumer Rights Regulation; Consumer Contracts Regulation	Terms and conditions have to be communicated to the user	Implementing EU legislation	Legislation often concentrates upon provision of information not on comprehension /take-up
European legislation	Proposed Data Protection Regulation; Audiovisual and Media Services Directive; Consumer Rights Directive	Management and transfers of data exchanged through services and apps with cross-border relevance; Advertising, protection of minors, cultural diversity	Addressing cross-border issues; Levelling EU market playing field for all companies	May not be suitable for all national contexts; ongoing questions about how to address competitiveness (e.g. EU–US)

4.4. Secure user behaviour can be encouraged through both technical and non-technical tools

Tools to enable greater user control

The literature review and interviews conducted for this study offered insights into potential technical measures that could be leveraged to increase the level of awareness and protection of users in the ICLR. Overall, a review of the evidence suggests that there is need for more sophisticated security tools that give users greater control in managing the security of their devices. Chapters 2 and 3 outlined the need for

more frequent patching and the potential demand of LRCD-specific protection software that allows users to ensure a level of security that mirrors their preferences rather than relying on industry defaults. These could be complemented by approaches that improve the assessment and testing of the security levels of LRCDs broadening out the conformity statements to cover security. Such an approach is proposed by information security researchers, such as Kuipers et al. (2014).

Non-technical tools: privacy and security by design and 'nudges'

Privacy and security by design (the approach to systems engineering that takes privacy and security into considerations throughout the design process) appear to be particularly pressing issues for the ICLR since the availability of traditional security tools for these devices appears to be limited (see Section 2.2 and Section 3.3.2). Privacy and security aspects can also be supported and enhanced by 'nudges': strategies that aim to incentivise users to behave in more security-conscious ways, such as described by academics investigating the applications of behavioural science, for instance Thaler and Sunstein (2008); or Acquisti (2009).

One of the interviewees from the consumer protection policy area highlighted that security- and privacy-oriented 'nudges' have been implemented in games console networks, such as the Xbox One (Office of Fair Trading 2013a). For instance, some consoles don't let users play new games until their security patches are up to date. In the case of the Xbox One, this creates incentives for the user to engage with the settings of the device: the design constrains the user to interact and implement settings in the device before being able to use it for its intended purpose. Furthermore, two interviewees from information security firms agreed with the importance of smart defaults for security and privacy options and that these should be taken into account in the design phase (iSec Partners 2013; Lookout 2013). These interviewees also conveyed the opinion that these ideas would potentially need a government-led approach for their implementation and enforcement (iSec Partners 2013; Lookout 2013), supporting research (e.g. the work of Sollins 2011) suggesting that industry seems to take only limited advantage of the technological possibilities to increase security for the end user and rarely considers the context in which the devices are used when implementing security measures (Sollins 2011).

4.5. Information sharing enhances awareness and response to potential risks

Many of the findings in this study illustrate how users are unaware of both the types of risk (fraud, etc.) that they might face in the living room and also the way in which their personal data is used to support the value chain. Examples of practices in other areas are illustrative of how these challenges might be addressed.

Communicating security: media campaigns and point-of-sale information about risks

Consumer organisations have been instrumental in informing users about the potential and risks associated with services that can be accessed through Internet connected technologies. These themes include behavioural advertising (Your Online Choices 2014) and awareness of data control and ownership (Naked Citizens 2014). Some of the innovative tools provided by these organisations include checklists on

accessing online services (Surfer Haben Rechte 2014), such as streaming. However, it has been pointed out in the academic literature that simply informing consumers in the absence of supplementary prompts and appropriate settings within the connected environments is most often not sufficient to prompt them to modify their behaviour (Helberger 2013).

Another potential channel to inform consumers in a more personalised and relevant setting could be represented by retailers. While manufacturers and ISPs are currently responsible for most of the issues related to their products, retailers also build up their own relationships and engage directly with the consumer. Furthermore, retailers are often bound by regulations on selling products and services. Therefore, the authors of this study think that point-of-sale provision of knowledge on security and privacy could offer a useful venue for communicating this information to consumers.

Communicating to consumers about personal information usage in the value chain

As we have seen in Chapter 1, personal data is a key element of the business models in the ICLR. This is both a risk and an opportunity: better uses of personal data while respecting the rights of the consumer might result in a more dynamic ICLR marketplace, but failure to respect such safeguards might result in consumers withdrawing from participation or, even worse, direct consequences such as fraud or identity theft. A key mechanism is communicating to consumers in order to obtain meaningful informed consent for their personal data to be processed.

Informed consent relies upon the user not only reading but understanding the conditions on which personal information may be used by others in the value chain. The UK Information Commissioner's Office points to a legal definition of consent as being: 'Any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed' (Directive 95/46 of the EC 1995).

As discussed in Section 3.5.2, behavioural research indicates that the average user of LRCD might be less circumspect, rational and reasonably well informed than is presumed by the rules on information provision (Helberger 2013). Further limitations to the awareness of users may also be a result of the fact that many of them interact with their devices in a distracted manner as discussed in Chapter 1.

Communication with consumers might also become more effective by incorporating insights from behavioural science, informed by relevant concepts such as framing or managing behavioural biases in order to motivate them to engage with security settings through contextual 'nudges'. Insights into the realities of how people really make choices have been provided by academics, most popularly psychologists and economists Kahneman and Tversky (1984). Concern about the way in which policies and terms and conditions fail to do this has emerged to a certain extent from the interviews with a policymaker from the consumer protection area and documentation provided by consumer protection organisations such as The Federation of German Consumer Organisations (vzbv). However, some of these also reported documentation did not provide enough information to consumers (an approach that behavioural science underscores as less effective than presumed) (Huck et al. 2011; Office of Fair Trading 2013a; Vzbv 2011). Possible routes to addressing this gap might include not only increasing the amount of information that is provided to the users, but also making difficult language clearer, underscoring personal relevance of the

implication of data usage, leveraging understanding about users in order to effectively convey information and the use of multimedia techniques.

Furthermore, a study on digital identity management by Sollins (2011) advises that for conditions to adequately reflect the potential outcomes of the consumer's interaction with LRCDs, these documents should ideally include information on transferring data across domains, for instance across services hosted on the same platform; the potential for unintended exposure of data or identities; and the possibility of leakage of information from services secondary to the ones that the user is engaging with (for instance an advertising service loaded through a gaming platform). Finally, terms and conditions, privacy policies and security settings should be adapted to the technologies in question to ensure their accessibility for users with disabilities as suggested by technology journalists like Strechay (2011), writing for an accessibility magazine, and consumers could be reminded at suitable points in their interaction with these devices.

Communicating with industry about privacy as a competitive advantage

While legal obligations for manufacturers and content providers to increase the security and privacy of their products are one possible way of improving security and privacy, Helberger's (2013) literature review finds that another route includes offering increased security and privacy in the value added by the product. This might be part of a strategic response to a growing consumer demand for security or privacy (as researched by Acquisti (2009) for instance), although as has been noted it remains unclear how much value people place on their security and privacy, and whether this can be measured economically.[19] Alternatively, the increased focus on these aspects might be a response to several high-profile breaches that are perceived to threaten the market value of a firm. This trend has also featured in the interviews conducted for the study, with a security company pointing to privacy protections as a likely competitiveness factor between companies (Symantec 2013a).

This trend has been recently illustrated by the marketing of the Xbox One, which prominently features privacy options, a strategy also adopted by Microsoft for its other products, as covered by marketing sector magazine *Adweek* (Bachman 2013; Microsoft 2014c).

Using labelling and icons

Labels and icons are often used to convey complex information to consumers in an easily accessible visual summary, for instance regarding energy efficiency of household appliances as researched by Cave and Cave (2012). They have been used, for instance, to communicate information on the content of gaming products or the energy efficiency of consumer electronics, or to warn consumers of apps with in-app purchase options or summarise information about video games (see e.g. PEGI 2014). Following the examples of these fields, labelling could appear as a potentially useful tool to help consumers understand the characteristics of their LRCDs. In particular, they could be used to channel information regarding connectivity and data management. Privacy labels are used in some cases on websites to signal their adherence to industry standards.

However, the study team has found that labels such as privacy certificates that appear on the websites of several manufacturers and service providers (such as the ESRB privacy certification) offer a lesser degree of

[19] See ongoing research by RAND Europe (Robinson et al., forthcoming).

assistance to the consumer than labels in other areas. While they convey the authority of the certification entity, the consumer does not learn more about the potential privacy implications of the products he or she is interacting with, as the label is limited to a symbol and does not include information. Furthermore, industry initiatives are subject to a bias in setting qualifying conditions. Industry may be incentivised to play down how their devices, networks and platforms use personal data, lest consumers withdraw or refuse to sign up, undermining their market. In conclusion, connectivity and privacy labels may offer a useful support to industry initiatives towards better communication with users about privacy and security. However, the study team suggests that these labels would ideally have to include information on the product (e.g. types of data collected) and not be limited to a certificate (e.g. 'privacy approved').

4.6. Effective partnerships offer an opportunity to address challenges without losing benefits

The need to work together is one way in which we might be able to implement effective policymaking while maintaining a suitable balance as indicated earlier in this chapter. Two examples of partnerships come to mind in this regard: partnerships when creating guidelines and partnerships for data management.

Partnerships when creating guidelines

An example of how a partnership-like approach shared between different stakeholders resulted in guidelines is represented by the recently adopted UK guidance on in-app purchases (see text box).

In-app purchases: an example of child protection objectives and tools shared by parents, platforms and developers

While children's behaviour in the context of app-based platforms and games is not a LRCD-specific topic, there is a growing need to ensure that their actions are subject to parental oversight, as demonstrated by the US Federal Trade Commission in the recent ruling against Apple (Federal Trade Commission, 2013). In this case, Apple was ordered to refund purchases made by children without parental consent both in a private ruling and by the Federal Trade Commission, to the scale of a minimum $32 million. Subsequently, Apple changed its platform permissions settings to require informed consent by the account owners to enable purchases.

In-app purchases have also been on the radar of the UK Office for Fair Trading (OFT). The principles and responsibilities outlined by the UK OFT's investigation into these apps and games read as applicable and relevant guidance for LRCD-related platforms and applications to child protection priorities (Office of Fair Trading 2013b). According to the principles, in-app commerce should conform to the following guidance: the consumers should be provided with clear, accurate material information about the business and the product, provided up front, before the consumer begins to play, download or sign up.

Furthermore, the commercial intent of the business should be clear and distinguishable from gameplay, and alternatives offered to monetary transactions (e.g. waiting or completing in-game tasks to obtain credits instead of purchasing them). Thirdly, the apps should not include practices that are aggressive, or which otherwise have the potential to exploit a child's inherent inexperience, vulnerability or credulity. This includes strategies aimed at making children persuade others to make payments for them. Finally, payments should not be taken from the payment account holder unless authorised and unless the account holder has given explicit informed consent.

These principles in sum, offer guidelines to platforms and app developers to take into account child and consumer

protection objectives while designing the games. These are further supplemented by parental guidelines and responsibilities, potentially resulting in a balanced approach to offering in-app services.

Partnerships for data management

Another example of public–private partnership between industry, government and consumers has resulted in the creation of transparent data management practices to empower users in the control of their data a key tenent of the right to the protection of personal data. Midata, which focuses on the banking, finance and energy sectors, is an example of such an initiative. Its aims, as specified by the Department for Business, Innovation and Skills (2013), are to:

- Get more private sector businesses to release personal data to consumers electronically.
- Make sure consumers can access their own data securely.
- Encourage businesses to develop applications (apps) that will help consumers make effective use of their data

Industry (both device manufacturers and those that offer services available on them) could potentially benefit from the extension of similar initiatives that would encourage businesses to voluntarily cooperate with their user base and develop apps (in the ICLR context it would potentially be extensions on already existing applications) that allow greater transparency to users.

References

Acquisti, Alessandro. 2009. 'Nudging Privacy: The Behavioural Economics of Personal Information.' *IEEE Security and Privacy* 7 (6): 82–85.

Acquisti Alessandro & Grossklags Jan. 2005. 'Privacy and rationality in individual decision making.' *IEEE Security and Privacy* 3(1): 26.

Adjei, Joseph K., & Henning Olesen. 2011. 'Keeping Identity Private.' *Vehicular Technology Magazine, IEEE* 6 (3): 70–79.

AEPD. 2013. La AEPD sanciona a Google por vulnerar gravemente los derechos de los ciudadanos [in Spanish]. AEPD website. As of 4 August 2014: http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2013/notas_prensa/common/diciembre/131219_NP_AEPD_POL_PRIV_GOOGLE.pdf

Al Falayleh, Mousa. 2013. 'A Review of Smart TV Forensics: Present State & Future Challenges.' *The International Conference on Digital Information Processing, E-Business and Cloud Computing (DIPECC2013)*, 50–55.

Amazon. 'Amazon Instant Video User Guide.' As of 4 August 2014: http://www.amazon.com/gp/feature.html/ref=amb_link_359558142_4?ie=UTF8&docId=1000739191&pf_rd_m=ATVPDKIKX0DER&pf_rd_s=center-3&pf_rd_r=18JQ89DEP8K7GBVM5N1X&pf_rd_t=1401&pf_rd_p=1395801862&pf_rd_i=1000739191#HowToWatch

Analysis Mason. 2013. 'Most Smart-TV Owners Do Not Connect Their TVs to the Internet: Manufacturers Must Respond.' 28 May. As of 4 August 2014: http://www.analysysmason.com/About-Us/News/Insight/smart-TV-May2013/

Anido, Luis E., Sonia M. Valladares, Manuel J. Fernandez-Iglesias, Carlos Rivas & Miguel Gomez. 2013. 'Adapted interfaces and interactive electronic devices for the smart home.' *Computer Science & Education (ICCSE), 2013 8th International Conference on*, 472–77.

Apple. 2014a. 'What is Apple TV?' As of 4 August 2014: http://www.apple.com/appletv/what-is/

Apple. 2014b. 'Privacy.' As of 4 August 2014: http://www.apple.com/privacy/

Arabo, Abdullahi, & Fadi El-Moussa. 2012. 'Security Framework for Smart Devices.' *International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, 82–87. As of 4 August 2014: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6246103

Arabo, Abdullahi, Ian Brown & Fadi El-Moussa. 2012. 'Privacy in the Age of Mobility and Smart Devices in Smart Homes.' *Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Conference on Social Computing (SocialCom)*, 819–26.

Bachman, Katy. 2013. 'New Microsoft Privacy Campaign Promotes Consumer Control.' *Adweek,* 22 April. As of 4 August 2014: http://www.adweek.com/news/advertising-branding/new-microsoft-privacy-campaign-promotes-consumer-control-148781

BAILLII. 2011. 'High Court case HC10C04385.' As of 4 August 2014: www.baillii.org

BBC. 2008. 'IPTV Overview.' BBC Future Media and Technology. As of 4 August 2014: http://www.bbc.co.uk/blogs/bbcilabs/assets/bbc_tvp_what_is_iptv.pdf

BBC News. 2013a. 'LG investigates Smart TV "unauthorised spying" claim.' BBC website, 20 November. As of 4 August 2014: http://www.bbc.co.uk/news/technology-25018225

BBC News. 2013b. 'Netflix studies piracy sites to decide what to buy.' BBC website, 16 September. As of 4 August 2014: http://www.bbc.co.uk/news/technology-24108673

BBC. 2013c. 'Webcams taken over by hackers, charity warns.' BBC website*,* 20 June. As of 4 August 2014: http://www.bbc.co.uk/news/uk-22967622

BBFC. 2014. 'Content Classification Guidelines.' BBFC website, 13 January 2014. As of 4 August 2014: http://www.bbfc.co.uk/www.bbfc.co.uk/new-classification-guidelines

Ben Hadj Mohamed, A., T. Val, L. Andrieux & A. Kachouri. 2012. 'Using a Kinect WSN for home monitoring: Principle, network and application evaluation.' *Wireless Communications in Unusual and Confined Areas (ICWCUCA), 2012 International Conference on*, 1–5.

Bennet, S., Maton, K. & Kervin, L. 2008. 'The 'Digital Natives Debate: A critical review of the evidence.' *British Journal of Educational Technology* 39(5): 775–86.

Bernhaupt, R., B. G. Boutonnet, Y. Gimenez, C. Pouchepanadin, and L. Souiba, 2012 ‚A set of recommendations for the control of IPTV-systems via smart phones based on the understanding of users practices and needs,' paper presented in *Proceedings of the 10th European conference on Interactive tv and video*, Berlin, Germany.

Bernhaupt, R., M. Obrist, A. Weiss, E. Beck & M. Tscheligi. 2008. 'Trends in the living room and beyond: results from ethnographic studies using creative and playful probing.' *Computers in Entertainment* (CIE) 6(1), 5.

European Consumers Organisation (BEUC). 2013. Representative interviewed by authors, 12 December 2013.

Blaich, Andrew, & Aaron Striegel. 2009. 'Is High Definition a natural DRM?' *Computer Communications and Networks, 2009. ICCCN 2009. Proceedings of 18th International Conference on*, 1–4.

Bode, Karl. 2012. '50% of Connected TVs Aren't Connected.' DSL Reports, 21 February. As of 4 August 2014:
http://www.dslreports.com/shownews/50-of-Connected-TVs-Arent-Connected-118464

Borgesius, Zuiderveen. 2013. 'Consent to Behavioural Targeting in European Law – What are the Policy Implications of Insights from Behavioural Economics?' Amsterdam Law School Research Paper No. 2013–43.

Brown, Jesse. 2013. 'Netflix CEO says torrent piracy in Canada down 50 per cent.' Macleans's, 17 September. As of 4 August 2014:
http://www2.macleans.ca/2013/09/17/netflix-ceo-says-torrent-piracy-in-canada-down-50-per-cent/

Cave, Jonathan, & Chris Marsden. 2008. 'Quis Custodiet Ipsos Custodes in the Internet? Self-Regulation as a Threat and a Promise.' *36th Research Conference on Communication, Information and Internet Policy*.

Cave, Jonathan & Ben Cave. 2012. 'Nudging eConsumers: Online Ecolabelling as Part of the Green Internet.' Working paper. As of 4 August 2014:
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2141967

Cavoukian, Ann, & Marc Chanliau. 2013. *Privacy and Security by Design: A Convergence of Paradigms*. Ontario: Information and Privacy Commissioner of Ontario.

CBC News. 2011. 'PlayStation data breach deemed in "top 5 ever".' CBC website, 27 April. As of 4 August 2014:
http://www.cbc.ca/news/technology/playstation-data-breach-deemed-in-top-5-ever-1.1059548

Chickowski, Ericka. 2013. 'Too Smart For Their Own Good: Attacking Smart TVs.' Dark Reading, 2 August. As of 4 August 2014:
http://www.darkreading.com/applications/too-smart-for-their-own-good-attacking-s/240159378

Clemons, Eric K. 2009. 'Monetizing the Internet: Surely There Must be Something other than Advertising.' *System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on*, 1–10.

CNN. 2013. 'Your TV might be watching you.' CNN website, 1 August. As of 4 August 2014:
http://money.cnn.com/2013/08/01/technology/security/tv-hack/index.html

CNiL. 2014. 'La formation restreinte de la CNIL pronounce une sanction pécuniaire de 150,000€ à l'encontre de la société GOOGLE Inc' [in French]. CNiL website. As of 4 August 2014:
http://www.cnil.fr/linstitution/missions/sanctionner/Google/

Common Vulnerabilities and Exposures. 2012. 'CVE-2012-2210.' As of 4 August 2014:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2210

Corcoran, Peter M. 2013. 'Biometrics and Consumer Electronics: A Brave New World or the Road to Dystopia? [Soapbox].' *Consumer Electronics Magazine, IEEE* 2 (2): 22–33.

Decipher Media Research. 2013. Representative interviewed by authors, 5 December.

Department for Business, Innovation and Skills. 2013. *Providing better information and protection for consumers*. 12 December. As of 4 August 2014: https://www.gov.uk/government/policies/providing-better-information-and-protection-for-consumers/supporting-pages/personal-data

Directorate-General for Internal Policies. 2013. *The Challenges of Connected TV*. As of 4 August 2014: http://www.europarl.europa.eu/RegData/etudes/divers/join/2013/513988/IPOL-CULT_DV(2013)513988_EN.pdf

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 , 23/11/1995 P. 0031 – 0050

DoctorBeet's Blog. 2013. 'LG Smart TVs logging USB filenames and viewing info to LG servers.' 18 November. As of 4 August 2014: http://doctorbeet.blogspot.co.uk/2013/11/lg-smart-tvs-logging-usb-filenames-and.html

Dutton, William H., & Grant Blank. 2013. *Cultures of the Internet: The Internet in Britain*. Oxford: Oxford Internet Institute.

Eikenberg, Richard.2014. 'Spion im Wohnzimmer: Privacy und Sicherheit bei Internet-fähigen TVs.' *c't magazine* (4): 77–78.

Engebretson, Patrick, Ashley Podhradsky, D.L. Grahek & A.J. Bierschbach. 2013. 'Security Analysis of Xbox 360 Vulnerabilities.' International Institute of Informatics and Systematics. As of 4 August 2014: http://www.iiis.org/CDs2013/CD2013SCI/SCI_2013/PapersPdf/SA191HO.pdf

European Commission. 2013a. *Cyber Security Report*. Brussels: European Commission.

European Commission. 2013b. Digital Agenda for Europe. Website. As of 4 August 2014: http://ec.europa.eu/digital-agenda/en/self-regulation-better-internet-kids

European Parliament. 2011. *Does it help or Hinder? Promotion of Innovation on the Internet and Citizens Right to Privacy*. As of 4 August 2014: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2011/464462/IPOL-ITRE_ET(2011)464462_EN.pdf

Europol. 2014. 'Notorious Botnet Infecting 2 Million Computers Disrupted.' As of 4 August 2014: https://www.europol.europa.eu/content/notorious-botnet-infecting-2-million-computers-disrupted

Expert Reviews. 2009. 'Home Office clueless over its own anti-child porn measures.' 17 March. As of 4 August 2014: http://www.expertreviews.co.uk/software/249655/home-office-clueless-over-its-own-anti-child-porn-measures

Fahey, Rob. 2012. 'A decade on, Xbox Live must face its biggest challenge.' *Games Industry International*, 16 November. As of 4 August 2014: http://www.gamesindustry.biz/articles/2012-11-16-a-decade-on-xbox-live-must-face-its-biggest-challenge

Faure, M.G. and H.A. Luth, 2011. 'Behavioural Economics in Unfair Contract Terms. Cautions and Considerations.' *Journal of Consumer Policy* 34(3) : 337, 342.

Federal Trade Commission. 2013. *Statement of Maureen K. Ohlhausen in RE Apple Inc., No. 122-3108.* 15 January. As of 4 August 2014: http://www.ftc.gov/sites/default/files/documents/cases/140115applestatementohlhausen.pdf

Fernandez Villamor, Antonio M., & Juan C. Yelmo. 2011. 'Helping Users Deal with Digital Threats: The Online User Supervision Architecture.' *Security & Privacy, IEEE* 9 (6): 29–35.

Fox News. 2013. 'Experts: Child predators use Xbox to find victims.' Fox website, 17 October. As of 4 August 2014: http://q13fox.com/2013/10/17/experts-child-predators-use-xbox-to-find-victims/#axzz2qNEdFym8

Gartner. 2013. 'Gartner Says Worldwide Video Game Market to Total $93 Billion in 2013.' Website, 29 October. As of 4 August 2014: http://www.gartner.com/newsroom/id/2614915

Google. 2012. 'Updating our privacy policies and terms of service.' Google Official Blog web page. As of 4 August 2014: http://googleblog.blogspot.be/2012/01/updating-our-privacy-policies-and-terms.html

Google Policy Center. 2014. 'Hate Speech.' As of 4 August 2014: https://support.google.com/youtube/answer/2801939?hl=en

Greenfield, Richard. 2012. 'Our Key Question for CES 2012: Are Smart-TVs Going to Napsterize the Video World? Is Bundling Sustainable?' *BTIG Research*, 6 January.

Grotticelli, Michael. 2012. 'Verizon patents targeted advertising that watches TV viewers.' Broadcast Engineering website, 5 December. As of 4 August 2014: http://broadcastengineering.com/company-news/verizon-patents-targeted-advertising-watches-tv-viewers

Guardian. 2011a. 'As PlayStation Network tries to get back online, Sony points to Anonymous.' *Guardian* website, 4 May. As of 4 August 2014: http://www.theguardian.com/technology/2011/may/05/playstation-network-sony-anonymous

Guardian. 2011b. 'Sony suffers second data breach with theft of 25m more user details.' *Guardian* website, 3 May. As of 4 August 2014: http://www.theguardian.com/technology/blog/2011/may/03/sony-data-breach-online-entertainment

Guardian. 2013a. 'Information commissioner investigates LG snooping smart TV data collection.' *Guardian* website, 21 November. As of 4 August 2014: http://www.theguardian.com/technology/2013/nov/21/information-commissioner-investigates-lg-snooping-smart-tv-data-collection

Guardian. 2013b. 'What is the lifespan of a laptop?' *Guardian* website, 12 January. As of 4 August 2014: http://www.theguardian.com/environment/2013/jan/13/lifespan-laptop-pc-planned-obsolescence

Hansen, Marit, Andreas Pfitzmann & Sandra Steinbrecher. 2008. 'Identity management throughout one's whole life.' *Information Security Technical Report* 13(2): 83–94.

HD Guru. 2012. 'Snooping HDTV? Samsung Responds to Criticism.' 30 March. As of 4 August 2014: http://hdguru.com/snooping-hdtv-samsung-responds-to-criticism/

Hearing Before the Subcommittee on Commerce, Manufacturing, and Trade of the Committee on Energy and Commerce House of Representatives. 2011. *The Threat of Data Theft to American Consumers*. 4 May. Washington, D.C.: US Government Printing Office.

Heise. 2014. 'Spion im Wohnzimmer: c't ertappt schnüffelnde Fernseher.' 25 January. As of 4 August 2014: http://www.heise.de/newsticker/meldung/Spion-im-Wohnzimmer-c-t-ertappt-schnueffelnde-Fernseher-2096578.html

Helberger, Natali. 2013. 'Form Matters: Informing Consumers Effectively.' *Amsterdam Law School Research Paper* No. 2013–71.

Helsper, E.J., & R. Eynon. 2010. 'Digital natives: where is the evidence?' *British Educational Research Journal* 36 (3): 503–20.

Herfurt, Martin. 2013. 'Security concerns with HbbTV.' Martin Herfurts's Blog, 1 June. As of 4 August 2014: http://mherfurt.wordpress.com/2013/06/01/security-concerns-with-hbbtv/

Hoadley, Christopher M., Heng Xu, Joey J. Lee & Mary Beth Rosson. 2010. 'Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry.' *Electronic Commerce Research and Applications* 9(1): 50–60.

Hommerberg, Anders. 2012. *My Social TV: Integrating Social Media with the TV Experience*. Uppsala: Uppsala University.

Huck, Steffen, Jidong Zhou & Charlotte Duke. 2011. *Consumer Behavioural Biases in Competition: A Survey*. Office of Fair Trading. As of 4 August 2014: http://www.oft.gov.uk/shared_oft/research/OFT1324.pdf

Hurwitz, Joshua B. 2011. 'The Influence of Trust and Privacy Risk-Taking on User Acceptance of Electronic Services that Collect Personal Information.' *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 55 (1): 1110–114.

Information Commissioner's Office. 2013a. 'Data Protection Act 1998 Monetary Penalty Notice. Name: Sony Computer Entertainment Europe Limited.' 14 January. As of 4 August 2014: http://www.ico.org.uk/news/latest_news/2013/~/media/documents/library/Data_Protection/Notices/sony_monetary_penalty_notice.ashx

Information Commissioner's Office. 2013b. Representative interviewed by authors. 10 December.

Ingersoll, Geoffrey. 2012. 'New Microsoft Patent Uses Kinect and Mobile Cameras to Count People in Your Living Room.' Business Insider website, 6 November. As of 4 August 2014:

http://www.businessinsider.com/microsoft-patent-uses-kinect-and-mobile-cameras-to-count-people-in-your-living-room-2012-11

Ipsos MediaCT. 2011. 'TV gets smart: Assessing Internet Television.' As of 19 February 2014: http://www.ipsos-mori.com/DownloadPublication/1426_IpsosMediaCT_TV-gets-smart_Jun2011.pdf

iSEC Partners. 2013. Representative interviewed by authors. 18 December.

Iyer, Manimozhi, Senthilmurugan Sanmugam, Jitendranath Mungara & Janakiraman Janakiraman. 2011. 'Enhancement Security in Smart TV Web Application.' *Innovative Systems Design and Engineering* 2 (4): 12–22.

Jigsaw Research. 2012. *Parents' views on parental controls*. As of 4 August 2014: http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/oct2012/Annex_1.pdf

Kahneman, Daniel, & Amos Tversky. 1984. 'Choices, Values, and Frames.' *American Psychologist* 39 (4): 341–50.

Kerton, Derek. 2012. 'Smart TVs: Not Such a Smart Idea.' *Techdirt*, 21 February. As of 4 August 2014: http://www.techdirt.com/blog/innovation/articles/20120221/03352017827/smart-tvs-not-such-smart-idea.shtml

Konow, Roberto, Wayman Tan, Luis Loyola, Javier Pereira & Nelson Baloian. 2010. 'Recommender System for Contextual Advertising in IPTV Scenarios.' In: *Proceedings of the 14th international conference on computer supported cooperative work in design*, 617–22. Shanghai.

Kovach, Steve. 2010. 'What is a Smart TV?' *Business Insider*, 8 December. As of 4 August 2014: http://www.businessinsider.com/what-is-a-smart-tv-2010-12

Krol, Kat, Matthew Moroz & M. Angela Sasse. 2012. 'Don't work. Can't work? Why It's Time to Rethink Security Warnings.' *Risk and Security of Internet and Systems (CRiSIS), 2012 7th International Conference on*, 1–8.

Kuipers, Rikke, Eeva Starck & Hannu Keikkinen. 2014. 'Smart TV Hacking: Crash Testing Your Home Entertainment.' Codenomicon. As of 4 August 2014: http://www.codenomicon.com/resources/whitepapers/codenomicon-wp-smart-tv-fuzzing.pdf

Lavin, Mike. 'Matchmaking on Xbox One with Smart Match.' *Xbox Wire*, 30 July. As of 4 August 2014: http://news.xbox.com/2013/07/games-smartmatch-feature

Lawler, Ryan. 2012. 'The Incredible Shrinking TV Replacement Cycle.' *Gigaom*, 5 January. As of 4 August 2014: http://gigaom.com/2012/01/05/tv-replacement-cycle/

Lennon, Christopher & Harold S. Geller. 2013. 'The Pipe Dream Becomes Real: Advertising Workflows Come of Age.' *SMPTE Motion Imaging Journa*l 122 (8): 32–37.

Leyden, John. 2012. 'Samsung's smart TV's "wide open" to exploits.' *The Register*, 12 December. As of 4 August 2014: http://www.theregister.co.uk/2012/12/12/smart_tv_pwned

LG. 2014. 'Data Encryption.' LG website. As of 4 August 2014: http://www.lg.com/us/mobile-phones/lggate/Data_Encryption

Livingstone, S., L. Haddon, A. Görzig & K. Ólafsson. 2011. 'Risks and Safety on the Internet: The Perspective of European Children.' LSE, London: EU Kids Online.

Löblich, M., & K. Karppinen. 2014. 'Guiding Principles for Internet Policy: A Comparison of Media Coverage in Four Western Countries'. *The Information Society*, 30(1): 45–59.

Lookout. 2013. Representative interviewed by authors, 12 December.

Luger, E., S. Moran & T. Rodden. 2013. 'Consent for All: Revealing the Hidden Complexity of Terms and Conditions.' *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Paris, France: ACM.

Marcus, J., I. Godlovitch, P.A. Nooren, D. Elixmann, B. van den Ende & J. Cave. 2013. 'Entertainment x.0 to Boost Broadband Deployment.' Study for the European Parliament ITRE Committee, 156.

Markworth, Tom. 2011. 'What Are Private Channels?' Roku, 24 August. As of 4 August 2014: http://blog.roku.com/blog/2011/08/24/what-are-private-channels/

Marotta-Wurgler F. 2011. 'Will Increased Disclosure Help? Evaluating the Recommendations of the ALI's Principles of the Law of Software Contracts.' *The University of Chicago Law Review* 78(1): 165.

Matsuno, Yutaka, Kenji Taguchi, Yoshihiko Nakabo, & Akira Ohata. 2012. 'Iterative and Simultaneous Development of Embedded Control Software and Dependability Cases for Consumer Devices.' *SICE Annual Conference (SICE), 2012 Proceedings of*. 675–80.

Mattrick, Don. 2013. 'Your Feedback Matters – Update on Xbox One.' *Xbox Wire*, 19 June 2013. As of 4 August 2014: http://news.xbox.com/2013/06/update

McAfee. 2013a. Representative interviewed by authors, 16 December.

McAfee. 2013b. *McAfee Labs Threats Report: Third Quarter 2013*. McAfee website. As of 4 August 2014: http://www.mcafee.com/uk/resources/reports/rp-quarterly-threat-q3-2013.pdf

McAfee. 2014. 'Online Safety and Security.' McAfee website. As of 4 August 2014: http://www.mcafee.com/us/campaigns/fight_cybercrime/cru/information/safeguard_your_device.html#gaming_consoles

McGuire, Mike, & Samantha Dowling. 2013. *Cyber Crime: A Review of the Evidence. Research Report 75: Summary of Key Findings and Implications*. London: UK Home Office.

Mello, John P. 2013. 'Microsoft's Tough Friday: Software giant battles hackers, malware, and a cloud outage.' *PC World*, 23 February. As of 4 August 2014: http://www.pcworld.com/article/2029190/microsofts-tough-friday-software-giant-battles-hackers-malware-and-a-cloud-outage.html

Meredith, Leslie, 2013 'Verizon Denies Plan to Spy on Customers.' NBCNews.com website, 19th June 2013. As of 4th August 2014: http://www.nbcnews.com/id/52258055/ns/technology_and_science-tech_and_gadgets/t/verizon-denies-plan-spy-customers/

Microsoft. 2013. 'New research reveals 1 in 3 UK families use tech to communicate within the home'. Microsoft website. As of 4 August 2014: https://www.marketingsociety.com/the-library/new-microsoft-research-technology-and-home

Microsoft. 2014a. *Xbox 360 Operations Manual*. As of 4 August 2014: http://www.videogameconsolelibrary.com/images/Manuals/05_MS_360_s_en-Manual.pdf

Microsoft. 2014b. 'Set Parental Controls for Xbox 360 and Xbox Live.' As of 4 August 2014: http://support.xbox.com/en-GB/xbox-360/security/xbox-live-parental-control

Microsoft. 2014c. 'Get More with Xbox One.' As of 4 August 2014: http://www.xbox.com/en-US/xbox-one/get-the-facts

Morrison, Geoffrey. 2012. 'How long do TVs last?' *CNET*, 23 February. As of 4 August 2014: http://reviews.cnet.com/8301-33199_7-57383293-221/how-long-do-tvs-last-morrisons-mailbag/

Naked Citizens (homepage). 2014. As of 4 August 2014: https://www.nakedcitizens.eu/

NextMarket Insights. 2013. *Connected Living Room Market Forecast 2013–2017*.

Nilsson Helander, Karin. 2013. *Smart TV: a More Interactive Way of Watching TV*. Thesis, Umea University.

Nintendo. 2011. 'Club Nintendo Privacy Policy.' As of 4 August 2014: http://www.nintendo.co.uk/Legal/Club-Nintendo-Privacy-Policy/Club-Nintendo-Privacy-Policy-625948.html

Nintendo. 2014a. *Nintendo 3DS XL: Operations Manual*. As of 4 August 2014: http://www.nintendo.com/consumer/downloads/SPR_EN_NA.pdf

Nintendo. 2014b. 'Wii U.' As of 4 August 2014: http://www.nintendo.co.uk/Wii-U/Wii-U-344102.html

Nintendo. 2014c. 'Wii U Tutorial.' As of 4 August 2014: http://www.nintendo.co.uk/Support/Tutorials/Tutorials-648600.html

Nooren, Pieter, Andra Leurdijk & Nico van Eijk. 2012. 'Intended and Unintended Effects of Policy Measures Aimed at Promoting Net Neutrality: An Examination of the Value Chain for Video Distribution.' Amsterdam: TNO/Institute for Information Law, University of Amsterdam.

Ocampo, Dean. 2011. 'PlayStation: You're doing it wrong. While doing it right.' SafeNet, 2 May. As of 4 August 2014: http://data-protection.safenet-inc.com/2011/05/playstation-youre-doing-it-wrong-while-doing-it-right/

Ofcom. 2013. *Communications Market Report 2013*. As of 4 August 2014: http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr13/2013_UK_CMR.pdf

Ofcom. 2014. *Ofcom Report on Internet Safety Measures*. As of 4 August 2014: http://stakeholders.ofcom.org.uk/binaries/internet/internet-safety-measures.pdf

Office of Fair Trading. 2013a. Representative interviewed by authors, 17 December.

Office of Fair Trading. 2013b. *Children's Online Games: Report and Consultation*. As of 4 August 2014: https://www.gov.uk/cma-cases/children-s-online-games

Open Rights Group. 2014. 'Internet Censorship in the UK', Open Rights Group website. As of 4 August 2014: https://www.openrightsgroup.org/issues/censorship

Oulasvirta, Antti, et al. 2012. 'Long-term effects of ubiquitous surveillance in the home.' *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*. Pittsburgh, Pennsylvania, ACM, 41–50.

Padilla-Walker, L. M., & S.M. Coyne. 2011. "Turn That Thing Off!" Parent And Adolescent Predictors of Proactive Media Monitoring. *Journal of Adolescence* 34(4): 705–15.

PEGI. 2012. 'PEGI for Apps' presentation given at the PEGI Congress. 29 November. As of 4 August 2014: http://www.pegicongress.com/congress/Presentations_files/Simon%20Little%20-%20PEGI%20for%20Apps%20-%20PEGI%20Congress.pdf

PEGI. 2014. 'What Do the Labels Mean?' Guidance on the categories in the PEGI ratings system. PEGI portal. As of 4 August 2014: http://www.pegi.info/en/index/id/33/

Pereira, Carlos Filipe Zambujo Lopes. 2011. *Security on Over the Top TV Services*. Thesis, University of Lisbon.

Poole, Erika S., W. Keith Edwards & Lawrence Jarvis. 2008. 'More than Meets the Eye: transforming the user experience of home network management.' *Proceedings of the 7th ACM Conference on Designing Interactive Systems*. Cape Town, South Africa, ACM, 455–64.

Prensky, Marc. 2001. 'Digital Natives, Digital Immigrants.' *On the Horizon* 9 (5): 1–6. As of 4 August 2014: http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf

Raiu, Costin, & David Emm. 2013. *Kaspersky Security Bulletin 2013*. London: Kaspersky Lab.

Read, Janet, & Russell Beale. 2009. 'Under My Pillow: Designing Security for Children's Special Things.' In Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology, 288–92. Swindon: British Computer Society.

Rick, Christophor. 2011. 'New Sony Terms of Service Ban Class Action Lawsuits, Is that Legal?' *Gamers Daily News*, 15 September. As of 4 August 2014: http://www.gamersdailynews.com/story-25130-New-Sony-Terms-of-Service-Ban-Class-Action-Lawsuits-Is-that-Legal.html

Rivington, James. 2007. 'Wii and PS3 vulnerable to hacks and phishing.' *Tech Radar*, 19 August. As of 4 August 2014: http://www.techradar.com/us/news/gaming/consoles/wii-and-ps3-vulnerable-to-hacks-and-phishing-161313

Robinson, Neil, Maarten Botterman, Lorenzo Valeri, David S. Ortiz, Andreas Ligtvoet, Rebecca Shoob & Edward Nason. 2007. *Security Challenges to the Use and Deployment of Disruptive Technologies*. Santa Monica, Calif.: RAND Corporation. TR-406-EC. As of 4 August 2014: http://www.rand.org/pubs/technical_reports/TR406.html

Robinson, Neil, Hans Graux, Maarten Botterman & Lorenzo Valeri. 2009. *Review of the European Data Protection Directive*. Santa Monica, Calif.: RAND Corporation. TR-710-ICO. As of 19 February 2014: http://www.rand.org/pubs/technical_reports/TR710.html

Robinson, Neil, Dimitris Potoglou, et al. Forthcoming. *Assessing the Public Perception of Security and Privacy*. As of 4 August 2014: http://www.rand.org/randeurope/research/projects/pact-security-privacy.html

RTA (homepage). 2014. As of 4 August 2014: http://rtalabel.org

SafeSurf (homepage). 2014. As of 4 August 2014: http://www.safesurf.com

Samsung D Forum. 2014. 'TV Apps Security.' As of 4 August 2014: http://www.samsungdforum.com/Support/TVAppsSecurity

Sangani, K. 2013. 'Uninvited Guests.' *Engineering & Technology* 8 (10): 46–49.

Scharr, Jill. 2013. 'PlayStation 4, Xbox One and the Lifetime of a Game Console.' *Toms Guide*, 18 November. As of 4 August 2014: http://www.tomsguide.com/us/current-gen-consoles-timeline,news-17869.html

Schultz, Jaeson. 2014. 'Attack Attribution and the Internet of Things.' Cisco, 31 January. As of 4 August 2014: http://blogs.cisco.com/security/attack-attribution-and-the-internet-of-things/

Security Affairs. 2013. 'Researcher Demonstrated SmartTV Hacking on Samsung Models.' 23 July. As of 4 August 2014: http://securityaffairs.co/wordpress/16535/hacking/researcher-demonstrated-smarttv-hacking-on-samsung-models.html

Semmes, Anne W. 2011. 'A Predator Is Lurking: FBI agent offers Internet safety tips to kids and their parents.' *Greenwich Citizens*, 7 April. As of 4 August 2014: http://www.greenwichcitizen.com/news/article/A-predator-is-lurking-FBI-agent-offers-Internet-1325686.php

Seybold, Patrick. 2011. 'Press Release: Some PlayStation Network and Qriocity Services to be Available This Week.' Playstation Blog, 1 May. As of 4 August 2014: http://blog.us.playstation.com/2011/04/30/press-release-some-playstation-network-and-qriocity-services-to-be-available-this-week/

Smith, Kevin, Deborah Lader, Jacquelien Hoare & Ivy Lau. 2012. *Hate Crime, Cyber Security and the Experience of Crime among Children: findings from the 2010/11 British Crime Survey*. London: Home Office Statistical Bulletin.

Sollins, Karen R. 2011. 'Challenges to Privacy in Social Networking Mashups: Social TV as a Case Study.' *Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on*, 1–6.

Sony. 2014. 'Set Up the Right Account for You.' As of 4 August 2014: http://uk.playstation.com/psn/support/ps3/detail/linked235311/item235321/Set-up-the-right-account-for-you/

Sony. 'Sony Support –KDL32W650A Improve your TV Functionality.' As of 4 August 2014: http://www.sony.co.uk/support/en/content/cnt-dwnl/prd-tvhc/bravia-kdlw-kdlx-firmware-update-v4401eua/KDL-32W650A

Spears, Janine L. 2013. 'The Effects of Notice versus Awareness: An Empirical Examination of an Online Consumer's Privacy Risk Treatment.' *System Sciences (HICSS), 2013 46th Hawaii International Conference on*, 3229–38.

Steam (Valve Corporation). 2013. Representative interviewed by authors, 11 December.

Strechay, Joe. 2011. 'Apple TV (2nd generation): Apple Continues to Set the Accessibility Standard.' *AFB AccessWorld Magazine* 12 (4).

Stuart, Keith, & Charles Arthur. 2011. 'PlayStation Network hack: why it took Sony seven days to tell the world.' The *Guardian*, 27 April. As of 4 August 2014: http://www.theguardian.com/technology/gamesblog/2011/apr/27/playstation-network-hack-sony

Suarez-Tangil, Guillermo, et al. 2013. 'Evolution, Detection and Analysis of Malware for Smart Devices'. *IEEE Communications Surveys & Tutorials* 99: 1–27.

Surfer Haben Rechte (homepage). 2014. As of 4 August 2014: http://www.surfer-haben-rechte.de/

Suomalainen, Jani, Pasi Hyttinen & Pentti Tarvainen. 2010. 'Secure Information Sharing between Heterogeneous Embedded Devices.' *Proceedings of the Fourth European Conference on Software Architecture: Companion Volume*, Copenhagen, Denmark, ACM.

Symantec. 2009. 'Parental Controls for Games.' January. As of 4 August 2014: http://securityresponse.symantec.com/norton/familyresources/resources.jsp?title=ar_parental_controls_for_games

Symantec. 2013a. Representative interviewed by authors, 12 December.

Symantec. 2013b. 'Creepware – Who's Watching You?' 10 December. As of 4 August 2014: http://www.symantec.com/connect/blogs/creepware-who-s-watching-you

Tassi, Paul. 2013. 'Whatever Happened to the War on Piracy?' *Forbes,* 24 January. As of 4 August 2014: http://www.forbes.com/sites/insertcoin/2014/01/24/whatever-happened-to-the-war-on-piracy/

TechTarget. 2005. 'Set-top Box.' April. As of 4 August 2014: http://searchnetworking.techtarget.com/definition/set-top-box

Telegraph. 2014. 'Should I Be Protecting My Smart TV?' *Telegraph* website, 24 March. As of 4 August 2014:
http://www.telegraph.co.uk/technology/advice/10714754/Should-I-be-protecting-my-smart-TV.html

Thaler, Richard H., & Cass R. Sunstein. 2008. *Nudge: Improving Decisions about Health, Wealth, and Happiness*. New Haven, CT: Yale University Press.

UK Council for Child Internet Safety. 2012. Website. As of 4 August 2014:
https://www.gov.uk/government/policy-advisory-groups/uk-council-for-child-internet-safety-ukccis

Vzbv (Verbraucherzentrale Bundesverband). 2011. *Information gut, alles gut? Empfehlungen für wirksame Informationen* [in German]. November. As of 4 August 2014:
http://www.vzbv.de/mediapics/verbraucherinformationen_wirksam_empfehlungen_vzbv.pdf

Vinayagamoorthy, Vinoba, Penelope Allen, Matt Hammond & Michael Evans. 2012. 'Researching the User Experience for Connected TV: a Case Study.' *CHI '12 Extended Abstracts on Human Factors in Computing Systems*, Austin, Texas, ACM.

Vu, Kim-Phuong L., Vanessa Chambers, Fredrick P. Garcia, Beth Creekmur, John Sulaitis, Deborah Nelson, Russell Pierce & Robert W. Proctor. 2007. 'How Users Read and Comprehend Privacy Policies.' In: *Human Interface and the Management of Information. Interacting in Information Environments*, 802-11. Berlin: Springer.

Windley, Peter. 2005. *Digital Identity*. Sebastopol, CA: O'Reilly Media, Inc.

Xbox Enforcement United. 2014. 'FAQ.' As of 4 August 2014:
https://enforcement.xbox.com/United/Learn/FAQ

Your Online Choices (homepage). 2014. As of 4 August 2014: http://www.youronlinechoices.eu/

YouTube. 2014. 'Terms of Service.' As of 4 August 2014:
https://www.youtube.com/static?template=terms

Zhan, J., & V. Rajamani. 2008. 'The Economics of Privacy-Privacy: People, Policy and Technology.' *Information Security and Assurance, 2008. ISA 2008. International Conference on*, 579–84.

Appendix A – Methodology

The research team used a two-tracked approach for the research methodology: a literature review and a series of semi-structured interviews with key stakeholders were undertaken simultaneously to gather information, place the study in a wider context and identify knowledge gaps and areas for further investigation.

A.1 Literature review

The aim of the literature review was to investigate a broad stratum of sources, which would place LRCDs in a broader technological context. The literature reviewed was clustered around technologies looking at the three dimensions of market scale, susceptibility to threats and consumer protection mechanisms. We initially considered a wide variety of technologies, though as the research progressed it became apparent that certain technologies were less prevalent in the literature, such as Internet connected radios and cameras. Conversely, smart TVs and games consoles produced far more hits from the search terms used, and the large presence of smart TVs and games consoles in the literature reviewed reflects this.

Three online databases were used for the search: Google Scholar, IEEE Explore and ACM. A tiered approach was used in identifying key search terms, whereby a selection of structured search strings requested 'hits' on the technologies, markets, vulnerabilities and protection tools that concern LRCDs. Based upon the first set of search results, the research team revised a second set of 24 search strings to broaden or narrow the scope of potential literature reviewed. These are shown in Table A.1.

Table A.1. Summary of search terms

Generic Search Strings	TV Search Strings
Market scale (((“connected” OR “interactive” OR “smart” OR “social”) AND (“living room*” OR “consumer electronics”)) AND (“growth” OR “market forecast*” OR “market share*”)	Market scale (((“connected” OR “interactive” OR “smart” OR “social”) AND (“tv” OR “television”)) AND (“growth” OR “market forecast*” OR “market share*”)
Threats and vulnerabilities (((“connected” OR “interactive” OR “smart” OR “social”) AND (“living room*” OR “consumer	Threats and vulnerabilities (((“connected” OR “interactive” OR “smart” OR “social”) AND (“tv” OR “television”)) AND

electronics")) AND ("crime" OR "fraud" OR "identity theft" OR "malware" OR "privacy" OR "security" OR "threat*" OR "vulnerabilit*"))

Consumer protection mechanisms
(((("connected" OR "interactive" OR "smart" OR "social") AND ("living room*" OR "consumer electronics")) AND ("child protection" OR "consumer awareness" OR "consumer protection" OR "content control*" OR "lifecycle management" OR "metadata" OR "parental control*"))

("privacy" OR "security" OR "vulnerability*"))

Consumer protection mechanisms
((("connected" OR "interactive" OR "smart" OR "social") AND ("tv" OR "television")) AND ("child protection" OR "consumer protection" OR "content control*" OR "content filter*" OR "lifecycle management" OR "update*"))

TV Apps Search Strings	TV Accessories Search Strings
Market scale (("lg smart tv" OR "lovefilm instant" OR "netflix" OR "ott app*" OR "panasonic smart viera" OR "philips smart tv" OR "samsung smart hub" OR "sony entertainment network" OR "toshiba cloud tv" OR "tv app*" OR "youview") AND ("growth" OR "market forecast*" OR "market share*")	Market scale (("apple tv" OR "blu-ray player*" OR "connected media player*" OR "digital video recorder*" OR "dvd player*" OR "google tv" OR "net-top box*" OR "raspberry pi" OR "roku") AND ("market growth" OR "market forecast*" OR "market share*")
Threats and vulnerabilities (("lg smart tv" OR "lovefilm instant" OR "netflix" OR "ott app*" OR "panasonic smart viera" OR "philips smart tv" OR "samsung smart hub" OR "sony entertainment network" OR "toshiba cloud tv" OR "tv app*" OR "youview") AND ("malicious content*" OR "malware*" OR "privacy" OR "security" OR "targeted advertising" OR "vulnerabilit*"))	Threats and vulnerabilities (("apple tv" OR "blu-ray player*" OR "connected media player*" OR "digital video recorder*" OR "dvd player*" OR "google tv" OR "net-top box*" OR "raspberry pi" OR "roku") AND ("bypassing of control*" OR "privacy" OR "security" OR "vulnerabilit*"))
Consumer protection mechanisms (("lg smart tv" OR "lovefilm instant" OR "netflix" OR "ott app*" OR "panasonic smart viera" OR "philips smart tv" OR "samsung smart hub" OR "sony entertainment network" OR "toshiba cloud tv" OR "tv app*" OR "youview") AND ("authentication" OR "child protection" OR "consumer protection" OR "content control*" OR	Consumer protection mechanisms (("apple tv" OR "blu-ray player*" OR "connected media player*" OR "digital video recorder*" OR "dvd player*" OR "google tv" OR "net-top box*" OR "raspberry pi" OR "roku") AND ("child protection" OR "consumer protection" OR "content control*" OR "content filter*" OR "firmware update*" OR "lifecycle management" OR "metadata" OR "parental control*" OR "patching cycle*"))

"content filter*" OR "parental control"))

Radio Search Strings	Game Consoles Search Strings
Market scale (("wi-fi radio*" OR "internet radio*" OR "pandora" OR "tunein") AND ("market growth" OR "market forecast*" OR "market share*")	Market scale (("game console*" OR "playstation 4" OR "wii u" OR "xbox one") AND ("market growth" OR "market forecast*" OR "market share*")
Threats and vulnerabilities (("wi-fi radio*" OR "internet radio*" OR "pandora" OR "tunein") AND ("privacy" OR "security" OR "targeted advertising" OR "vulnerabilit*")	Threats and vulnerabilities (("game console*" OR "kinect" OR "playstation 3" OR "playstation 4" OR "wii" OR "wii u" OR "xbox 360" OR "xbox one") AND ("bullying" OR "bypassing of control*" OR "fraud" OR "privacy" OR "security" OR "vulnerabilit*")
Consumer protection mechanisms (("wi-fi radio*" OR "internet radio*" OR "pandora" OR "tunein") AND ("consumer protection" OR "firmware update*" OR "lifecycle management" OR "patching cycle"))	Consumer protection mechanisms (("game console*" OR "kinect" OR "playstation 3" OR "playstation 4" OR "wii" OR "wii u" OR "xbox 360" OR "xbox one") AND ("child protection" OR "consumer protection" OR "firmware update*" OR "lifecycle management" OR "parental control*")
Cameras Search Strings	**Enabling Technologies Search Strings**
Market scale (("connected camera*" OR "dropbox" OR "flickr" OR "picasa" OR "wi-fi digital camera*" OR "wireless camera*") AND ("growth" OR "market forecast*" OR "market share*")	Market scale (("biometrics" OR "cloud" OR "marlin" OR "miracast" OR "steam") AND ("living room*" OR "consumer electronics")) AND ("growth" OR "market forecast*" OR "market share*")
Threats and vulnerabilities (("connected camera*" OR "dropbox" OR "flickr" OR "picasa" OR "wi-fi digital camera*" OR "wireless camera*") AND ("privacy" OR "security" OR "targeted advertising" OR "vulnerabilit*"))	Threats and vulnerabilities (("biometrics" OR "cloud" OR "marlin" OR "miracast" OR "steam") AND ("living room*" OR "consumer electronics")) AND ("crime" OR "exploitation" OR "fraud" OR "identity theft" OR "privacy" OR "security" OR "threat*"))
Consumer protection mechanisms (("connected camera*" OR "dropbox" OR "flickr" OR "picasa" OR "wi-fi digital camera*" OR "wireless camera*") AND ("authentication" OR	Consumer protection mechanisms (("biometrics" OR "cloud" OR "marlin" OR "miracast" OR "steam") AND ("living room*" OR "consumer electronics")) AND ("consumer

"consumer protection" OR "identification"))	awareness" OR "consumer protection" OR "patching cycle*"))

In total, 231 articles were identified through our systemic search, with the literature covered spanning from 2006 to 2013. These articles were saved in the reference manager application EndNote, where the team screened each article's abstract. To determine the degree of relevance to the project, a systematic mapping exercise was undertaken, whereby each article's abstract was screened against a fixed set of criteria. The criteria comprised the main question the article attempted to address, with the researchers only selecting references which addressed one of the following:

1) The market for LRCDs
2) Potential benefits of LRCDs for users and industry
3) Potential challenges to users' security and privacy
4) Potential challenges to industry
5) Tools and mechanisms to protect users and
6) Mitigation of risks to which industry could be exposed.

Fifty-six articles were deemed relevant enough to be reviewed in depth, and this group of articles formed the majority of the literature-based body of evidence used in the study. In addition, the team also examined approximately 150 'grey papers' from the technology policy community, newspaper articles, as well as research reports from Ofcom and other government agencies.

Table A.2. Summary of literature review

Number of databases	3
Number of search strings	24
Abstracts screened	231
Articles reviewed in depth	56

Through the literature review and subsequent mapping exercise, the research team was able to identify 'knowledge gaps' in the literature that could be addressed through more targeted research using other resources, including newspaper articles and key stakeholder interviews. Figure A.1 summarises the outcomes of the mapping exercise.

Figure A.1. Summary of mapping exercise

What main question does it relate to?							Does this study mention a specific technology?							Does this study mention a specific threat?						
The market for LRCDs	Threats and vulnerabilities in LRCDs	Protection tools	Consumer protection	Description of technological solutions	Other	Net-top box	TV	Gaming	Video	Platforms	Apps	Enablers	Other	Privacy/data protection	Profiling	Malicious attacks	Vulnerable consumers	Harm to minors	Financial fraud	Other
90	60	20	32	41	1	10	91	18	6	4	8	20	3	48	12	18	16	11	8	68

A.2 Key stakeholder interviews

In parallel with the literature review, the project team sought out key stakeholders with significant expertise in our main areas of enquiry. Several organisations were suggested by Ofcom, and others were selected by the team on the basis of reputation and experience in the research area. The value chain determined the types of interviewees the project team contacted, although most organisations declined to be interviewed. While every organisation contacted received three reminders regarding the interview invitation, many organisations did not respond, or declined interviews with the research team after they became aware of the subject of the study.

Table A.3. List of organisations who received an invitation to participate in an interview

Institution	Industry / Service / Mandate
Apple	Platform provider
BBC	Service provider
BEUC	Consumer representative
BlackBerry	Platform provider
BT	Service provider
Child Exploitation and Online Protection Centre	Government agency
Decipher Media Research	Research firm

Dropcam	Hardware vendor
Europol EC3	Law enforcement
Gigaom	Research firm (blog)
Google	Platform provider
Information Commissioner's Office	Government agency
iSEC Partners	Vulnerability research firm
LG	Platform provider
Lookout	Vulnerability research firm
LOVEFiLM Instant	Service provider
McAfee	Software vendor
Metropolitan Police Central e-crime Unit	Law enforcement
Microsoft	Platform provider
Netflix	Service provider
Nintendo	Platform provider
Office of Fair Trading	Government agency
Panasonic	Hardware vendor
Philips	Hardware vendor
Phone Pay Plus	Regulator
Plex	Software and hardware vendor
ReVuln	Vulnerability research firm
Roku	Platform provider
Samsung	Hardware vendor
Sky	Service provider
smartclip UK	Advertising technology company
Sony PlayStation	Platform provider
Sony Smart TV	Hardware vendor
Symantec	Vulnerability research firm
The Authority for Television on Demand	Regulator
The Consumer Protection Association	Consumer representative
Toshiba	Hardware vendor

Valve Corporation	Platform provider
Virgin Media	Service provider
Wind River	Platform provider
Xumo	Advertising technology company
YuMe	Advertising technology company

There was an implicit bias in the sectors who agreed to be interviewed, as large manufacturers and service providers proved unwilling to respond to interview invitations, particularly after they had learned about the nature of our research. Information security and research firms, on the other hand, were generally willing to discuss the research topic with the study team. Despite a positive response rate of only 26 per cent, the interviews secured were all of high quality, and interviewees were able to offer key insights into all aspects of the value chain.

Table A.4. List of organisations interviewed

Institution	Industry / Service / Mandate
BBC	Service provider
BEUC	Consumer representative
Decipher Media Research	Research firm
Information Commissioner's Office	Government agency
iSEC Partners	Vulnerability research firm
Lookout	Vulnerability research firm
McAfee	Software vendor
Office of Fair Trading	Government agency
Plex	Software and hardware vendor
Symantec	Vulnerability research firm
Steam (Valve Corporation)	Platform provider

Forty-two organisations received interview invitations, and the research team successfully secured interviews with 11 organisational representatives. The interviews took place in person or on the phone. They were conducted on a semi-structured basis, with the interviewer following a protocol for the study, but also asking auxiliary questions and allowing for new lines of questioning depending on the expertise of the interviewee. Each individual interview protocol was tailored according to both the expertise of the interviewee and the emergent findings. Both note taking and audio recording were used during the

interviews, with interviewees being assured of non-attribution and anonymity when using direct quotes, unless they gave the researchers explicit permission otherwise. Audio files were destroyed upon completion of the transcription of the interviews.

Appendix B – Descriptions of LRCDs and services

A brief summary of the LRCDs and the services they can offer is provided below.

Examples of devices

Smart TV: A TV that integrates some of the features of a computer with those of a TV. Smart TVs usually offer interactive functions and can download apps (Kovach 2010). The connection to the Internet is either direct through a cable in the back of the TV or through a connected box. It is also possible for smart TVs to communicate with other devices such as computers, smartphones and tablets (Hommerberg 2012; Nilsson Helander 2013).

Internet-enabled TV: The term 'Internet-enabled TV' covers any television set connected to the Internet via a third-party device, such as a set-top box, a games console or a laptop/PC. The set-top box might be provided with services such as Sky On Demand, Virgin TiVo, BT Vision or Talk Talk. Games consoles used include Microsoft's Xbox Live, Sony's Playstation 3 and the Nintendo Wii. Laptops/PCs are connected through a cable run from an output port to an input port on a compatible TV (Ofcom 2013).

Set-top box: Set-top boxes mean that users can enjoy connected TV even without owning a smart TV. A set-top box is a device that allows a TV user to interface with the Internet and to receive digital television broadcasts (TechTarget 2005).

Games console: A games console plugs into a TV to allow users to play video games, and increasingly also offers greater connectivity and ability to share content between devices. Games consoles are designed primarily for purchasable games content to be played on them, either in offline 'single-player' mode, or online through a dedicated network with other players. Increasingly, games consoles are the primary device for users to consume other types of media besides games, such as on-demand television, Internet browsing and music. The newest devices include Sony's PlayStation 4, Microsoft's Xbox One, and Nintendo's 3DS and Wii U.

WiFi: WiFi, otherwise known as a wireless network, is a means of Internet connectivity that dispenses with the need for direct, cabled access to a router; WiFi allows wireless communication with the Internet and other devices. Higher-performance WiFi devices will also start to become available: 'While the vast majority of network connections in the living room today are 802.11n, this will shift in coming years as smart TVs, Blu-ray players and net-tops adopt 802.11ac dual-band connections' (NextMarket Insights 2013).

Second-screen devices: The user interface for a smart TV can be through a so-called second-screen device such as a smart phone or tablet computer; having been designed with inherent usability, and because it has a screen separate from the main display and much closer to the user, often with touch-screen capability, a second screen can rapidly be used to get more out of a smart TV.

Examples of the services and tools that can be enjoyed through LRCDs

Applications: Applications, commonly referred to as 'apps', are pieces of software that can be installed on a device that give additional functionality or features. Because different smart TVs use different platforms, not all apps work on all TVs; smart TVs often come with a set of apps installed and, depending on the model, users may be able to download further apps (Nilsson Helander 2013).

Internet Protocol Television (IPTV): IPTV refers to the IP networks that deliver services to smart TVs such as Live TV, on demand programming, and Interactive TV (ATIS 2005). IPTV services are usually delivered over a managed network such as Sky or BT Vision (BBC 2008).

Video on Demand (VoD): VoD is a service that allows users to stream or download video content over a network at a time of their choosing. In contrast to IPTV, VoD does not need to be delivered over Internet Protocol, but can be delivered to a set-top box from the broadcaster (BBC 2008).

Catch-up TV: Catch-up TV is a form of VoD that allows users to replay traditionally broadcast programmes up to a certain period after their on-air broadcast. BBC iPlayer and ITV's 4oD are platforms upon which catch-up TV is regularly watched.

Pay-per-view (PPV): PPV are telecasts that are delivered for a fee to the consumer at a specific time only. They are most commonly used for live events such as sporting or musical performances and are available through cable and terrestrial or digital satellites.

Internet Radio: While 'Internet radio' can refer to streaming music services such as Pandora or Spotify, which can be played on a variety of Internet connected devices, Internet radio in the context of this report refers to stand-alone hardware devices that are designed to receive Internet radio stations.