Ipsos MORI Scotland

CarnegieUK TRUST

CHANGING MINDS • CHANGING LIVES

Online Data Privacy from Attitudes to Action: an evidence review

Carolyn Black, Lucy Setterfield and Rachel Warren

Ipsos MORI Scotland for Carnegie UK Trust

CarnegieUK TRUST

CHANGING MINDS • CHANGING LIVES

ACKNOWLEDGEMENTS

Reviewed and edited for the Trust by Douglas White and Anna Grant

About Ipsos MORI Scotland

Ipsos MORI Scotland provides research focused on the distinct needs of policymakers and businesses in Scotland. We offer the full range of qualitative and quantitative research methodologies and have a detailed understanding of specific sectors in Scotland, their policy challenges and their research needs. The variety of research we conduct gives us a unique insight into many aspects of life in Scotland.

Contents

Foreword

Privacy is often cited as essential to freedom of expression and democracy and, as such, has an important impact on our wellbeing. But privacy is no longer confined to the physical space behind our kitchen curtains or the basic anonymity of who we voted for in the last election. As lines between the 'real' and 'connected' worlds continue to blur, online data privacy becomes an increasingly significant part of our individual privacy tapestry.

The challenge of understanding privacy in a digital age is complex. How we view data privacy can be highly individualised and the resulting motivations, perceptions and behaviour can be equally diverse. There is reason to believe that the implementation of the General Data Protection Regulation (GDPR), which starts to reassert citizens' right to control, as well as the significant media attention that recent data scandals have rightly received, will provide an important catalyst for conversation, recognition and action. Long-term implications on public understanding are as yet unclear.

However, despite the ever-growing significance of online data privacy, we often don't have a clear understanding of what the UK public really thinks about this issue or how they actually behave with their data. Public policy debates around how an individual's privacy is managed and protected online can be informed by instinctive responses to what 'feels' right or concerning. Better evidence about public attitudes and behaviour is needed. How we collectively think and act around online data privacy is having substantial societal, economic and political implications both in the UK and around the world, and it is important to note that it is not a zero-sum game. Both action and inertia have an impact as a lack of clear challenge can be taken as passive acceptance.

How do we ensure the voice of citizen is heard in the debate, when this voice is often widely dispersed, poorly organised and occasionally contradictory?

This report, commissioned by the Carnegie UK Trust and produced by Ipsos MORI, brings together a wide range of recent research studies which have explored people's attitudes and behaviours towards data privacy across different scenarios. Whilst many of the findings in this review may seem intuitive, others may be more surprising. It is important that this evidence has a role in the policy process, so decisions aren't driven by general assumptions or narrow experiences, but by an informed evidence-based understanding.

It is clear from the research that most people in the UK are concerned about their data privacy to some degree, but attitudes and actions towards data privacy can vary according to a multitude of factors, and the actions that the public take do not always reflect this level of concern. The purpose of this review was not to provide specific policy recommendations, but unpicking these points further could help to inform appropriate responses, as the solution to engaging communities on these issues will not be a 'one size fits all' approach.

The review also highlights a number of meaningful shortcomings within the existing data set, as well as challenges in drawing comparisons or trends. With more data about us being generated, shared and gathered every day, the implications for different societal groups merits further consideration and patterns need to be tracked over time.

We hope that this review will provide a robust, timely and neutral evidence base which policymakers, practitioners and academics can utilise, and from which they can draw informed opinions with regards to data privacy attitudes and actions.

Douglas White, Head of Advocacy, Carnegie UK Trust

1. Introduction

What are we exploring?

For many of us, our lives are increasingly lived online - whether through the extensive adoption of social media; constant internet access via smartphones and public WiFi networks; or the widespread digitisation of private markets and public services. While this has brought a great deal of convenience in day-to-day life, the impact of the collection and use of our personal data can have a cost. There has been much media coverage in the past few years covering high-profile data breaches. Many people have found revelations about the sheer amount of personal data that organisations hold on about us to be highly troubling. This year has seen the implementation of the General Data Protection Regulation (GDPR) across Europe, which is designed to help citizens regain a semblance of control. It is clear that online data privacy has never been more pertinent.

It is in this context that this research report seeks to address three overarching questions:

1. **What do people think about online data privacy?**
2. **What actions do people take in relation to their online privacy?**
3. **What trade-offs are people willing to make relating to their data privacy?**

Historical context

The issue of online data privacy can be contextualised within wider historical public policy, and legal and philosophical privacy debates. Concerns about privacy date as far back as Aristotle's distinction between the public sphere of political activity and the private sphere of family and domestic life. While privacy issues are highly culturally specific, issues relating to privacy such as gossip and surveillance have concerned almost all societies since antiquity. Technological advancement since the 19th century, and the rise of new information technologies in the 20th century, brought these debates to the fore, as the topic of privacy became increasingly prominent from the 1960s onwards.

How to define privacy has been the subject of considerable debate. Recent commentators on the issue have proposed numerous definitions of 'privacy' relating to different contexts. In the evidence reviewed, it is often not clear what is meant by online data privacy, as neither 'privacy' nor 'data' tended to be explicitly defined. However, based on the questions addressed in the literature (both in the UK and internationally), authors appeared to conceptualise online data privacy in terms of Gormley's definition of privacy as 'citizens' ability to regulate information about themselves' and Solove's definition 'control over personal information'.

As different individuals conceptualise privacy in different ways, it is important to note that participants in the studies included in this research report may have been using a different definition of privacy than that intended by those carrying out the study. Ken Gormley (1992) identifies four types of privacy definition: privacy as an expression of one's personhood and personality; privacy as autonomy; privacy as citizens' ability to regulate information about themselves; and multidimensional notions of privacy (Fuchs, 2011).

In his seminal work Understanding Privacy (2008), Daniel Solove goes further, arguing for six different privacy definitions: (1) the right to be left alone; (2) limited access to the self; (3) secrecy; (4) control over personal information; (5) personhood; and (6) intimacy. These definitions of privacy were, of course, developed before the exponential expansion of technology, particularly the advent and widespread adoption of social media and mobile internet devices, and therefore may have limitations in how effectively they can be used to address privacy in a digital landscape.

This report

In chapter two, we outline the research methods and comment on the process. In chapter three, the review begins by exploring what people think about their online data privacy, how that has changed over time and whether views of online data privacy differ by sociodemographic group. Chapter four examines the different types of online security behaviours the public do or do not exhibit, again exploring subgroup differences and change over time where possible. Chapter five explores whether the findings from chapters three and four correspond – does the public's behaviour reflect their reported attitude to online data privacy? The final chapter covers the overall conclusions of the review, in addition to setting out possible avenues for moving the evidence, and wider data privacy debate, forward.

2. Researching Online Data Privacy

The Carnegie UK Trust commissioned Ipsos MORI Scotland to undertake secondary analysis to review evidence of citizens' attitudes and behaviours towards online privacy in the UK. This included any variations by demographic group and context, as well as looking at cross-national comparative studies with the US and other European countries.

Methods

The methodology for this paper was a desk-based evidence review. The review encompassed both quantitative and qualitative empirical studies published by public, private and third-sector organisations, as well as academic papers. While we included a range of studies in terms of methodology and size – including but not limited to large-scale face-to-face, online and telephone surveys and focus groups – we restricted the dates of publication to the last three years to ensure that our findings were reasonably current, given the rapid and significant pace of change in the digital age. In total, we included 50 evidence sources in our review, which we were confident used rigorous data collection to produce robust data.

We followed several steps in compiling our source list to ensure the robustness and relevance of the data included. Firstly, we identified our search terms, which included 'data privacy', 'data security', 'attitudes to data privacy/security' and 'data privacy/security behaviours', then the search was limited to publications since 2014. While we focused primarily on UK-based studies, we also considered Pan-European studies and US-based studies in the same time-frame for a cross-national perspective. After compiling an initial list, we reviewed each study in terms of research quality to exclude any where there were concerns about the quality of the data collected. These were studies where we felt that leading questions were asked to participants, ultimately encouraging or prompting certain answers, and quantitative studies with insufficient numbers of cases for results to be significant.

Notably this review looks at individual's privacy attitudes and behaviours in relation to their own privacy and security, and did not include research investigating other privacy relationships such as parent to child, adult to older parent or peer to peer.

Comments on Researching

There were limitations to the data available to review both in terms of the methods used and the content of the data collected. In this section, we outline the issues encountered.

Inconsistencies in terminology and providing definitions

There was very little consistency in the language used across the different research studies reviewed. For example, while some literature uses very broad terms (e.g. concern around online data privacy), some focuses on very specific issues (e.g. concern about using specific social media sites or household appliances with internet connectivity), and some still uses alternative terminology which may engender a slightly different issue or response (e.g. concern about the recording of everyday activities on the internet).

A related challenge was that many studies did not explore concern at all, rather they looked at self-reported confidence. While this provides an interesting reflection of attitude, it is not an accurate reflection of whether online data security is a problem for them or not, as confidence can be misplaced. Furthermore, there was little attempt to define what was meant by the language used, or to preface questions within a particular context. This is problematic in a context where public understanding of the issues being investigated (the collection and use of personal data and the impact that this can have) is relatively low. For example, research by Doteveryone (2018) found that 83% of participants did not realise that information shared about them online by others is collected, while 62% did not realise that internet connection data is collected.

This lack of definition and consistency has two effects. First, it means that the data from different studies cannot be easily compared – we are not able to contrast like for like. Second, and perhaps more concerning, if there is no shared understanding among participants of what a question means – or what behaviours it is referring to – the questions essentially become subjective, and it is unlikely that you will get fully reliable data. For instance, one study asked if participants used 'different' passwords. This meant they had to interpret how many passwords 'different passwords' actually defined (a person who uses two different passwords across all their online accounts may think this counts as different passwords, whereas someone else may think it means a different password for every account).

Self-report data

It is important to note that the majority of behaviour recorded in the literature reviewed is self-reported. In survey research, participants can present themselves in a more positive light in order to provide the 'correct' answer as prescribed by society. If such a 'social desirability effect' is at play in this instance, then it is possible that the prevalence of 'secure' online behaviour may be lower than actually recorded.

The only studies that looked at knowledge were the 2018 Doteveryone Understanding report, as noted above, and some of the academic papers. While the academic papers can provide useful insight of why individuals might be acting in a specific way, there is the drawback that they often rely on convenience samples (often young, often educated – a particular issue when exploring online behaviour) meaning we cannot be sure the data is representative of the wider population.

Predominantly quantitative data

The review found that most of the studies on data privacy were quantitative, and there were very few qualitative studies which we could draw upon. Where possible, qualitative studies were included within the review. Given the general low level of understanding or conformity around many data privacy concepts or implications, there is a clear need and opportunity for more qualitative research to explore and interrogate why people think and behave the way they do.

Limited demographic breakdowns

While the data sources we reviewed were predominately quantitative, few of these explored demographic variations in depth, beyond age, though even this had its limitations. Studies included in the review generally include age 16 or 18 and upwards, and so much research does not include research with regards to privacy behaviours or attitudes of children, an absence also noted by contemporary researchers such as Livingstone (2018).

There has been much less research on the relationship between socioeconomic status and online data privacy views and behaviours. We also found a very limited number of ongoing studies and datasets that track the same attitudes and behaviours at regular intervals, which made it difficult to identify trends over time.

The key data sources used to explore these issues in the review were Ofcom and the Information Commissioners Office, as they fit the criteria of nationally representative data, with subgroup and trend data available for analysis. The 2015 Eurobarometer was also invaluable in providing country comparisons.

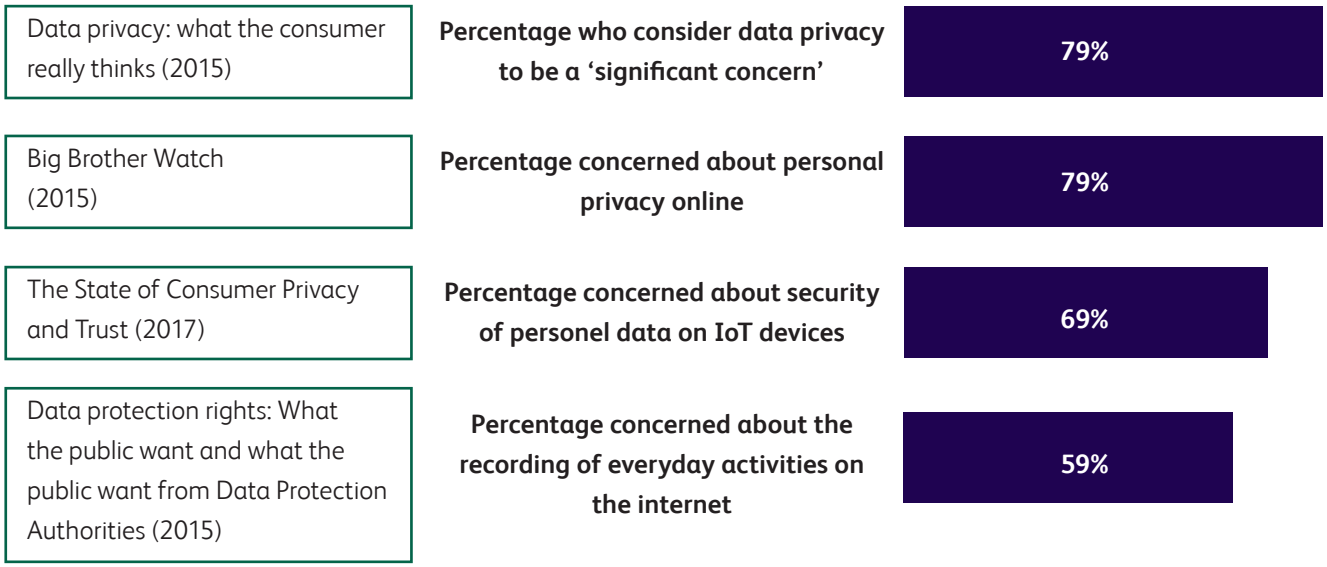
3. What Do People Think About Their Online Data Privacy?

How concerned are people about data privacy issues?

Views of online data privacy, whether attitudes around concern, control or confidence, vary depending on the context of the question asked. One of the most notable aspects of the literature, as noted in the previous chapter, is the lack of consistency across terminology and question wording. This means that there is a lack of consensus between studies, and therefore no conclusive answer on data privacy issues.

At the broadest level, a significant majority of people in the UK have some concern about data privacy. For example, the 2015 Big Brother Watch survey found that 79% of individuals are concerned about their personal privacy online, reporting that 49% of the individuals surveyed are fairly concerned, while 29% are very concerned (Big Brother Watch, 2015). Attitudes towards data privacy have also been explored through a variety of more specific measures in the literature, which has likely contributed to the degree of variation in the findings. Studies have variously reported that 69% of users in the UK and Ireland are concerned about the security of personal data on devices and appliances with internet connectivity (Gigya, 2017); that 59% of internet users in the UK express concern about the recording of everyday activities on the internet (Eurobarometer, 2015) and that 79% of individuals claim that online privacy is a significant concern (DMA, 2015).

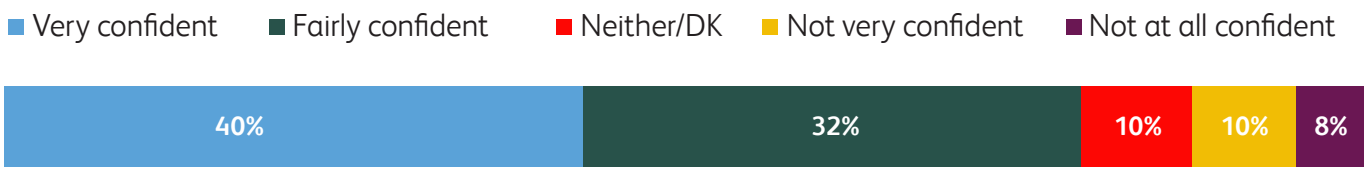
Figure 3.1 Level of concern about privacy online



Base: Data privacy: what the consumer really thinks: (1000 UK adults); Big Brother Watch (1,000); The State of Consumer Privacy and Trust: (2,001 US and 2,001 UK adults aged 18+); Data protection rights: What the public want and what the public want from Data Protection Authorities: Participants who are concerned about privacy (790).

While the studies above have asked participants how concerned they are about online privacy, other research has asked different questions around individuals' levels of confidence in managing their personal data. These alternative measures have, in some cases, produced a rather different picture of public attitudes. For example, 72% of people reported feeling confident they are in control of who has access to their personal data online (Ofcom, 2017).

Figure 3.2 Confidence in managing access to personal data online



Base: All adults aged 16+ who go online (1,553).

Change over time

A number of studies have highlighted that attitudes towards online privacy change over time. For example, the number of individuals who claimed that data privacy was a significant concern fell from 84% in 2012 to 79% in 2015 (DMA, 2015). Meanwhile, those who claimed to be 'unconcerned' about the collection and use of their data was the fastest-growing group during this time, rising from 16% in 2012 to 22% in 2015 (DMA, 2015). The evidence suggests that this trend was common across all age groups (DMA, 2015). This is, perhaps, surprising given that the reach of information technology became significantly more pervasive during this three-year period.

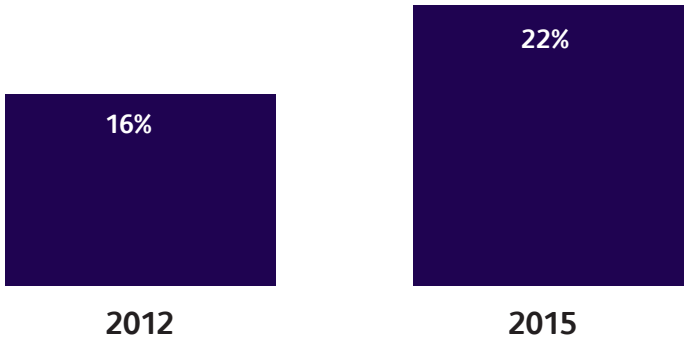
One interpretation of this trend is that individuals were not in fact any less concerned about data privacy infringement, but began to simply start to accept it as an increasingly inevitable aspect of modern life, and to display a growing degree of fatalism about it. While participants were more likely to believe that their personal data was open to use by commercial and governmental bodies, or to be conscious of the implications that may have for them, they became less likely to think they could do something about it. For instance, in a 2016 TRUSTe consumer privacy study, 30% of participants said that losing online privacy is part of being more connected online. The 2018 Doteveryone Attitudes report found that 43% of participants said that it does not matter if they trust organisations they engage with online if they need to use them for day-to-day life; while 52% said they wouldn't be able to get through all the things they need to do every day if they didn't use the internet. This is further illustrated in the quotation below:

> "It's very invasive. They have too much power but we all want to use those sites so we tick the box."

(Doteveryone Attitudes Report, 2018)

It is not yet clear, however, whether recent high-profile data breaches and scandals, alongside new laws to give more power to individuals, have begun to slow or reverse this trend towards citizens' acceptance of how their personal data is used.

Figure 3.3 Percentage who are 'unconcerned' about data privacy



Base: 1000 UK adults

Source: DMA, 2015

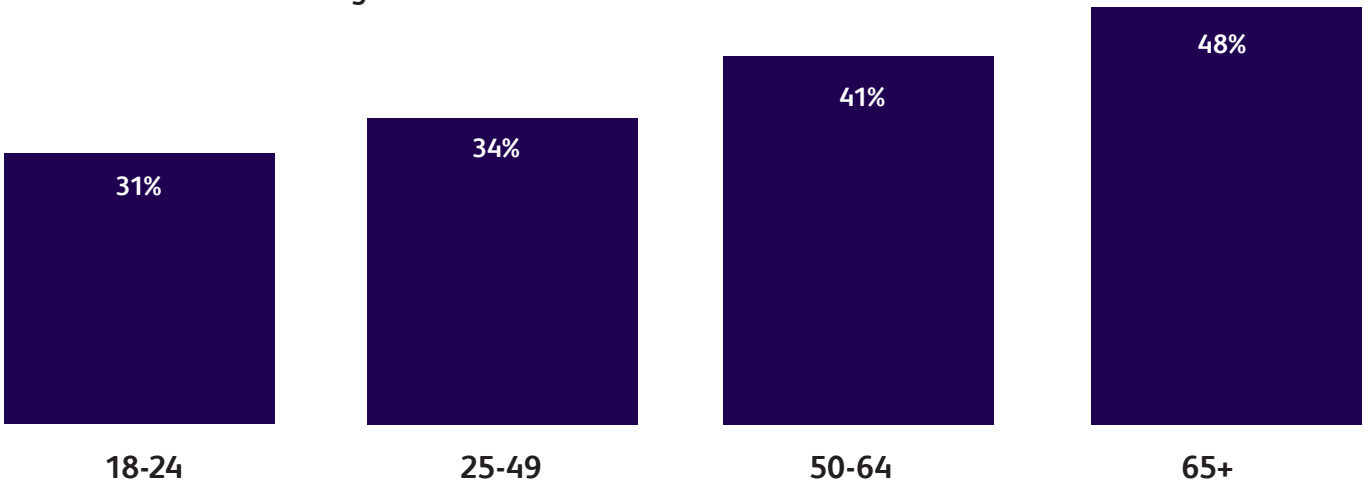
Do attitudes vary between different demographic groups?

While the amount of published evidence on demographic differences in the UK is limited, it seems that different groups have different attitudes to data privacy issues. The greatest focus of research to date has tended to be around the effect of age, with limited research on socio-economic group, gender, ethnicity or disability.

Age

The available data suggests that people's attitudes towards online data privacy do vary by age. Based on the studies which look at differences in attitudes by age, the general pattern appears to be that there are higher levels of concern about a variety of privacy issues among older people than younger people. For example, levels of concern about companies collecting personal data online and sharing it with other companies are closely correlated with age; with the proportion citing this as a concern increasing consistently through each age bracket, from 31% among 18 to 24-year-olds, to 48% among those aged over 65 (Rogers, 2017).

Figure 3.4 Percentage of participants concerned about companies collecting and sharing personal data online with other organisations



Base: 2,017 GB adults

Source: Rogers (2017).

In line with this, 18 to 24-year-olds make up the biggest proportion of those 'unconcerned' about data privacy at 30%, while 55 to 64-year-olds and 65+ consumers are less likely to be in this group (12% and 16% respectively) (DMA, 2015). As noted above, however, between 2012 and 2015, a growing number of people across all age groups reported themselves as 'unconcerned'.

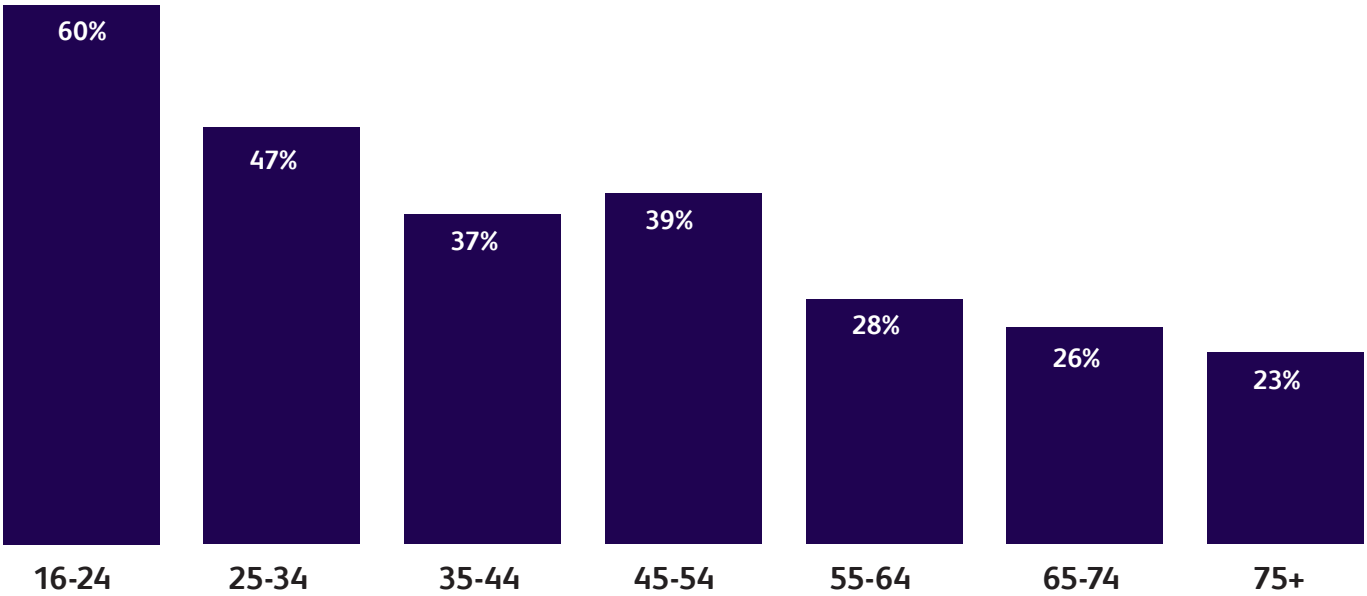
The generally higher levels of concern among older individuals was also borne out in the qualitative research:

> "They can find out everything about you. In another part of the world they know where you live, how much money you've got. You haven't got any private life now in my opinion because everybody can find out."

(Ofcom, 2015: Female, 82, Retired, Coventry)

Levels of confidence around data privacy issues also vary by age according to the available research. Younger people are much more likely to express a high degree of confidence about managing the security of their personal data, whereas older people are significantly more likely to report being not very or not at all confident in this area. While 60% of 16 to 24-year-olds and 47% of 25 to 34-year-olds say they are very confident in managing who has access to their personal data online, that figure is just 28% for 55 to 64-year-olds; 26% for 65 to 74-year-olds; and 23% for over-75s (Ofcom, 201&).

Figure 3.5 Percentage of internet users who are 'very confident' in managing who has access to their personal data online by age



Base: Adults aged 16+ who go online (1553) *Adults' media use and attitudes: Report 2017 (Ofcom 2017).*

Furthermore, internet users aged 65-74 and 75+ are more than twice as likely as internet users overall to say they are not at all confident that they can manage who has access to their personal data online (18% and 17% respectively compared to the average of 8%) (Ofcom, 2017).

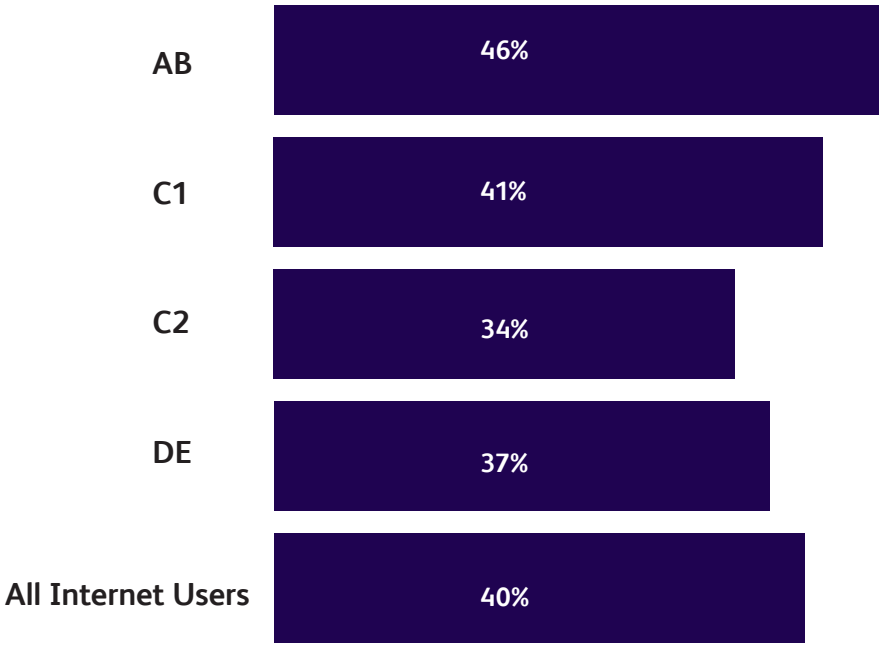
Gender

Findings on attitudes by gender are both limited in number and mixed in findings, presenting no clear patterns. While some studies have found women to be less confident[1] than men – with one study putting men's confidence levels in managing the security of their personal data at 44% and women's at just 37% (Ofcom, 2016) – others have challenged this, with one face-to-face survey finding women to be significantly more confident than men (Nurse and Williams, 2016).

Socio-economic status

Far fewer recent UK studies have looked at attitudes to data privacy by socioeconomic status. The review identified just a small number of studies that have done so in the last three years (Ofcom, 2016; Ofcom, 2017; Nurse and Williams, 2016). However, there is an emerging pattern: individuals of higher socioeconomic status are more concerned about, but more confident in dealing with, data privacy issues than those of lower socioeconomic status. Different measures of social status have been used across different studies. While one study looked at attitudes by level of education and whether participants used a PC in the workplace (an indicator of occupational status), the others explored attitudes by an overall measure of social grade. Internet users in AB households are more likely than internet users on average (46% compared to 40%) to say they are very confident in managing who has access to their personal data (Ofcom, 2017). It is important to note that higher confidence does not necessarily correspond to a greater ability to protect information online and this should be interpreted with caution. A total of 41% of those in C1 households, 34% of those in C2 households, and 37% of those in DE households said that they are very confident in response to the same question.

Figure 3.6 Percentage of adults who are 'very confident' in managing who has access to their personal data online by socioeconomic status



Base: Adults aged 16+ who go online (1553) *Adults' media use and attitudes: Report 2017 (Ofcom 2017).*

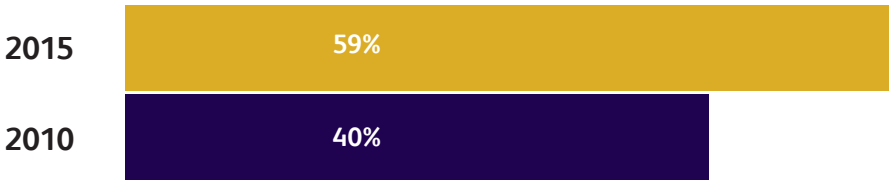
1 It should be noted that confidence does not necessarily equate to greater knowledge of data security.

Understanding citizens' concerns

There is some evidence from across the different research studies of the different types of data privacy issues that give citizens cause for concern.

One such area is the notably high, and growing, levels of concern about the recording of everyday activities on the internet in the UK, with 59% of users expressing concern about this in 2015; an increase of 19 percentage points since 2010 (Eurobarometer, 2015).

Figure 3.7 Percentage of UK participants concerned about the recording of everyday activities on the internet in 2015 and 2010.



Base: 1,328 UK adult

Source: Eurobarometer (2015)

This sense of unease about what is recorded as citizens go about their business online was also apparent in the qualitative research:

> "It's difficult, because I don't have a full understanding of how they use the data they have about me. I think that's the most intrusive thing, that some of the ads track your behaviour because of various sites you've visited, or Gmail just takes keywords out of your email."

(Ofcom, 2015: Male, 36, Web Officer, Cardiff)

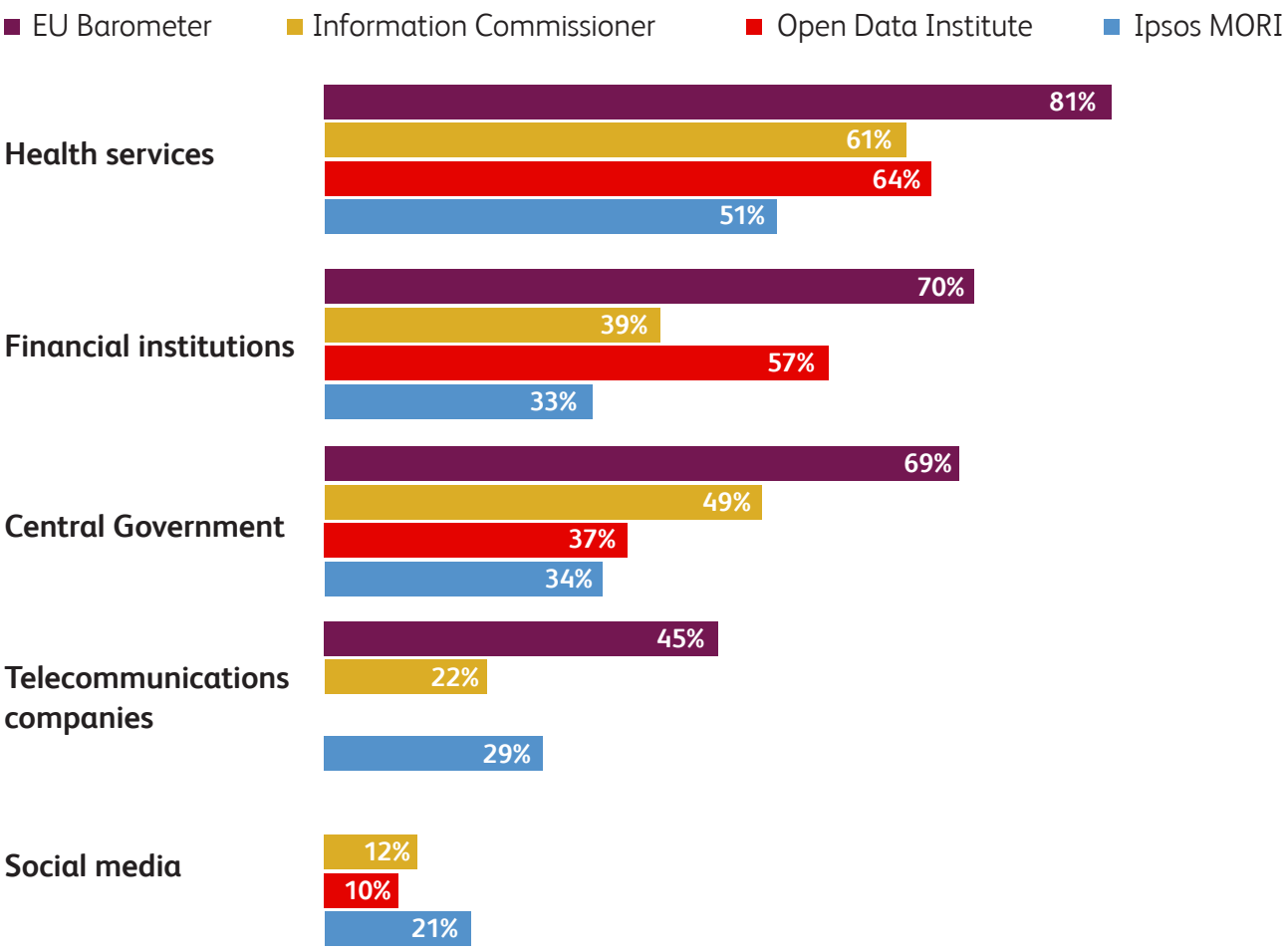
Qualitative research on attitudes to the use of health data also highlights that information asymmetry plays a role in determining the level of concern people feel:

> "It's a one-way mirror; they know everything about you but we don't know what they're doing with that."

(Ipsos MORI and Wellcome Trust, 2016: Patient, severe conditions)

Public concern also varies significantly depending the type of organisation data is shared with. Overall, citizens appear to be less concerned with public bodies than with private companies accessing their personal data. Users are most comfortable sharing data with public-sector organisations, with the NHS at the top of people's trust levels and the Central Government lower down. People are less comfortable sharing data with private companies such as telecommunications companies, with social media companies at the bottom of a trust ranking (Eurobarometer, 2015; ICO, 2015; ODI, 2018; Ipsos MORI, 2017).

Figure 3.8 Public trust in organisations accessing their personal data



This sentiment is illustrated in the below comment on health data:

> "I'm more than happy for academics or researchers to see (genetic data), but not private companies."

(Ipsos MORI and the Wellcome Trust, 2016: General Public, Sheffield)

While levels of trust overall are low for internet companies[2], they are notably lower among older users than younger users; with a mean trust score of 4.5/10 among 16 to 24-year-olds but only 3.4/10 among adults aged 55-75 (Ipsos MORI, 2014).

2 However, it is important to note that 'internet companies' was not defined in the research

How do attitudes in the UK compare to attitudes in other countries?

Overall, the evidence reviewed suggests there is a considerable degree of cross-national variation in attitudes to data privacy. Our findings indicate that levels of concern in the UK about data privacy issues are among the highest, if not the highest, in Europe, in line with those in the US.

How do UK attitudes compare to the EU as a whole?

Generally, the evidence suggests that people in the UK are more concerned about data privacy than individuals in most other European countries. A full 59% of UK citizens say they are concerned about the recording of everyday activities on the internet, which is notably higher than the European average of 45% (ICO, 2015).

Furthermore, there are other, more specific, contexts in which concerns about data privacy are notably high in the UK compared with other countries in Europe. These include: mobile applications, where the level of data privacy concern in the UK (63%) is second only to the Czech Republic (73%), and the use of payment cards, where only people in France, Ireland and the Czech Republic record higher levels of data privacy concern than those in the UK (Eurobarometer, 2015).

The trust ranking for different organisations is broadly consistent across the UK and the rest of Europe, though the evidence points to slightly higher levels of trust overall in Europe. As in the UK, individuals across Europe are least likely to trust internet service providers and social networking sites with their personal data, and express relatively higher levels of trust for public-sector organisations. Although in the UK just 22% of individuals trust internet service providers with their personal data (ICO, 2016), that figure is slightly higher in Europe as a whole, at 32% (ICO, 2015). Similarly, 11% of UK citizens trust social media companies with their personal data, compared with 22% in Europe (ICO, 2015).

As in the UK, attitudes to data privacy issues and data sharing in the rest of Europe are also highly context-dependent. The evidence suggests that across Europe, people are relatively more averse to the use of their data by private companies but more comfortable with the use of their data for medical purposes, or where they may get a personal benefit in return for sharing their data (Rand, 2015).

How does the UK compare to the US?

Research findings suggest that citizens in the United States display a broadly similar attitude to data privacy issues as UK citizens. In fact, the TRUSTe Consumer Privacy and Trust Surveys reported that the same percentage, 92%, of US and UK users worry about their privacy online (TRUSTe, 2016; TRUSTe, 2017).

Attitudes in the US towards social media and search companies holding data about individuals are broadly in line with the UK and EU, with 69% and 66% respectively not feeling confident in these types of companies keeping their data safe. However, there are higher levels of concern about public-sector organisations accessing personal data in the US (Pew Research Centre, 2015). In the UK, only 40% of citizens are not comfortable with government organisations accessing their personal data (Demos, 2017), whereas 54% of US citizens are not at all, or not too confident that their data will be kept secure by government agencies (Pew Research Centre, 2015).

4. What Actions Do People Take In Relation To Their Online Privacy?

How do people behave in relation to their online privacy?

The research analysed above suggests that the majority of citizens in the UK have at least some degree of concern about their online privacy.

However, the evidence reviewed for this study also suggests that a lower proportion of people are acting on this concern. Most citizens do make security checks before entering information into a website (Ofcom, 2017), but other precautionary actions are less common. For example, citizens in the UK do not commonly delete their browsing history or cookies, encrypt emails, use privacy software or read Privacy Policies or Terms and Conditions. The research also suggests that many people do not actively protect their location online; either through their mobile location services, or through social media activity. It is common, however, for citizens to give out minimal personal information when online, as a way of protecting their privacy.

This chapter addresses the different actions and tactics that people take to ensure their privacy online. As the literature covers a wide variety of behaviours, the actions addressed in this chapter have been divided into the following categories for ease of reference:

a) Internet browsing security measures

b) Reading privacy policies and terms and conditions

c) Password hygiene

d) Use of location services

e) Managing privacy on social media accounts

f) Providing false or limited personal information.

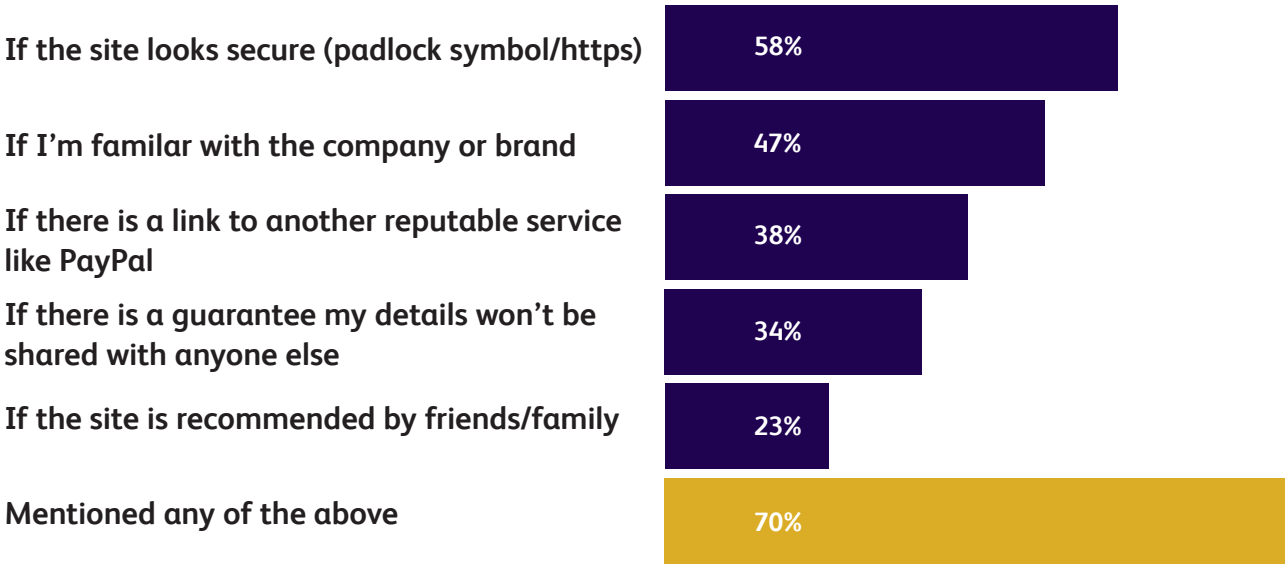
We first review each behaviour and then, where this information is available, go on to comment on any differences between demographic groups, alongside any notable differences between the UK and the United States, or European countries.

(a) Internet browsing security measures

This section includes how people assess the trustworthiness of internet sites they are browsing, how people manage their browsing history, use of public WiFi and the use of data privacy programmes. The Adults' Media and Attitudes Report 2017 found that most people (70%) make at least one recommended security check before entering any personal information into a website. These checks include: if the site looks secure (e.g. has a padlock symbol or https); if they are familiar with the company or brand; if there is a link to another reputable service/company; if there is a guarantee that their details

will not be shared; and if the site is recommended by friends or family. The two most common checks are: if the site looks secure (58%) and if they recognise the company or brand (47%) (Ofcom, 2017b). The Consumer Privacy Index found that 34% of people in Britain look for a 'privacy trust seal' before deciding whether or not to trust the site (TRUSTe, 2016).

Figure 4.1 Checks made before entering personal details into a website



Base: Adults aged 16+ who go online who say they register personal details online (1516) Source: Adults' Media Use and Attitudes Report, Ofcom (2017)

Qualitative research by Ofcom supports this finding. Participants stated that when judging if a website is secure or not, they take into consideration whether the site is popular and/or asked friends or family for advice if unsure (Ofcom, 2016a).

> "I think the trick is to stick to websites that a lot of people use. The way I see it is that if there are a thousand people using this website then chances are it's going to have to be quite secure."

(Adult Media Lives 2015: Male, 19, England).

> "I'm very cautious. If I'm not sure I call my daughter and explain what they're asking for. Then she will say "That's all right" or "Come out of it".

(Adult Media Lives 2014: Female, 70, Scotland).

Other studies also found that participants refrained from using an online service (39%) (ICO, 2016) or cancelled a transaction (23%) (TRUSTe, 2016a) after deciding that the website did not look trustworthy. However, these studies did not explore the reasons why the participants did not trust some websites or the factors they considered when making this decision.

Managing browser history:

Around half of participants (49%) report deleting cookies, cache or similar browsing history in the TRUSTe 2016 report, while just over a quarter of participants in the 2016 ICO report (28%) said they deleted cookies. Only 18% of participants in this study reported using a 'do not track' feature on their internet browser.

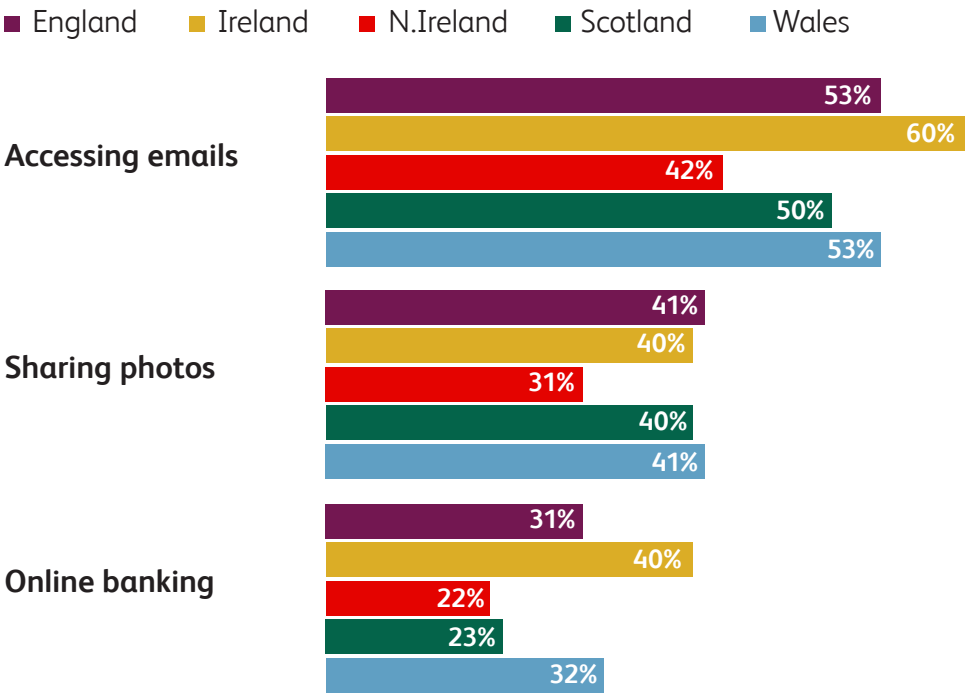
49% have deleted cookie, cache or similar browsing history (TRUSTe, 2016a)
28% deleted cookies from their internet browser (ICO, 2016)
18% use 'do not track' feature on browser (ICO, 2016).

A qualitative study by Marreiros et al (2015) explored people's behaviour around cookies and consent. It found that although most participants are aware of cookie notices, they rarely read them and instead either click accept regardless, or ignore them altogether.

Use of public WiFi:

Participants tend to use public WiFi to check their emails, more than to share photos or do online banking. That said, it was still fairly common for people to carry out these activities using public WiFi, despite some caution (White, 2017).

Figure 4.2 Online activities using public WiFi



Base: Adults who use the internet: England: 1,291; Ireland: 985; Northern Ireland: 1,005; Scotland: 725; Wales: 854
Source: Digitally Savvy Citizens: Data from across the UK and Ireland on how we manage information, security and privacy online (2017)

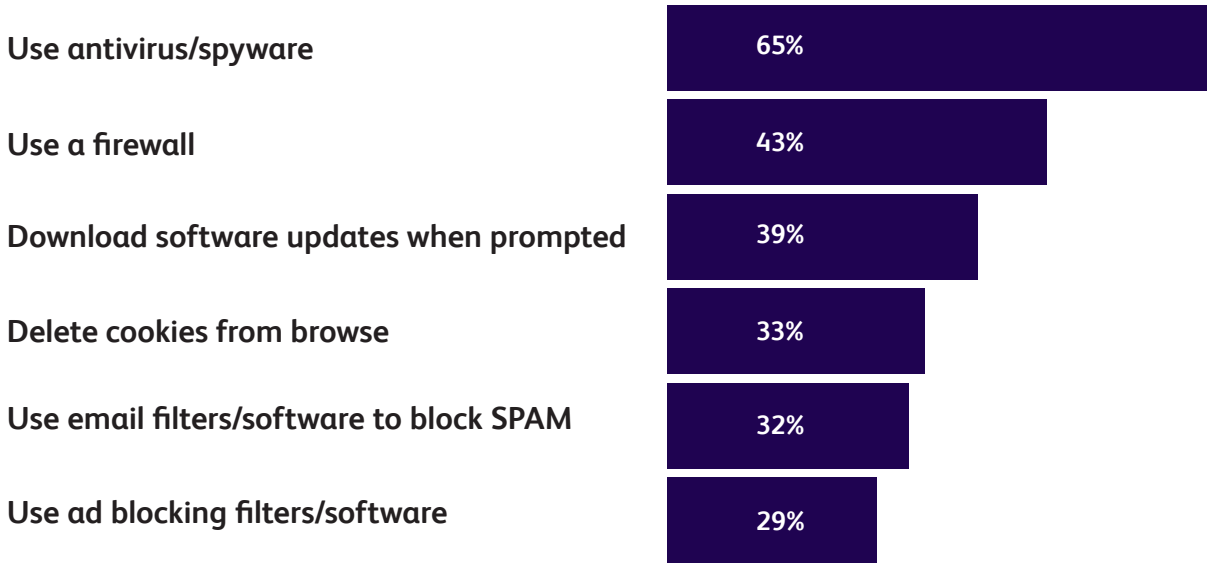
A qualitative study from Ofcom found that although most participants are reasonably confident about using their smartphone to do online banking or undertaking financial transactions, some were still cautious doing so while using public WiFi connections (Ofcom, 2016a).

Use of data privacy programmes/Privacy protection programmes:

While the use of anti-virus software and anti-spyware is common (Ofcom, 2017b; Scottish Government 2016), use and awareness of more technical encryption programmes for email, proxy servers or anonymity programmes such as 'Tor' are not (Williams and Nurse, 2013).

The Adults' Media Use and Attitudes Report found that 65% of internet users stated that they have installed anti-virus or anti-spyware software (Ofcom, 2017b). The ICO's Information Rights Research (2016) supports this finding, with 66% of their participants stating that they use such software (ICO, 2016). The Ofcom study also found that around two-fifths of internet users use a firewall (43%) and download the latest software updates (39%) (Ofcom, 2017b).

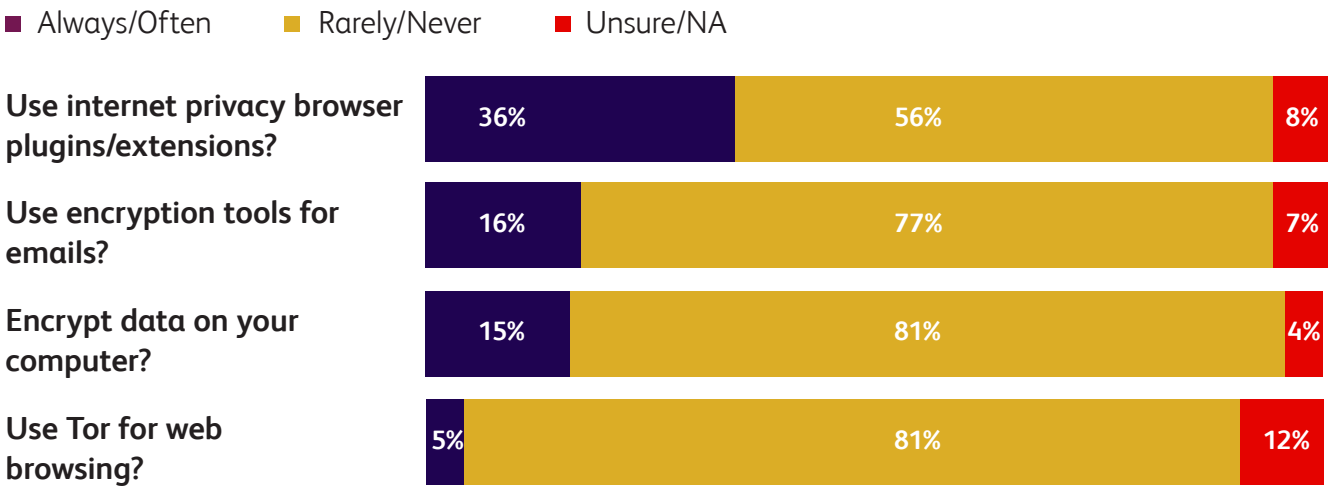
Figure 4.3 Security measures adopted



Base: Internet users aged 16+ (1553) *Source: Adults' media use and attitudes: Report 2017*

As well as the very small number who use Tor (5%), Williams and Nurse (2013) also found that a low number of participants encrypt data on their computer (15%) or use encryption when emailing (16%). The use of internet privacy plug-ins or extensions is more common, but still not highly used (36%).

Figure 4.4 Privacy programmes used. "How often do you…"



Base: All (102) *Source: Optional Data Disclosure and the Online Privacy Paradox: A UK Perspective (2016)*

b) Reading privacy policies and website terms and conditions:

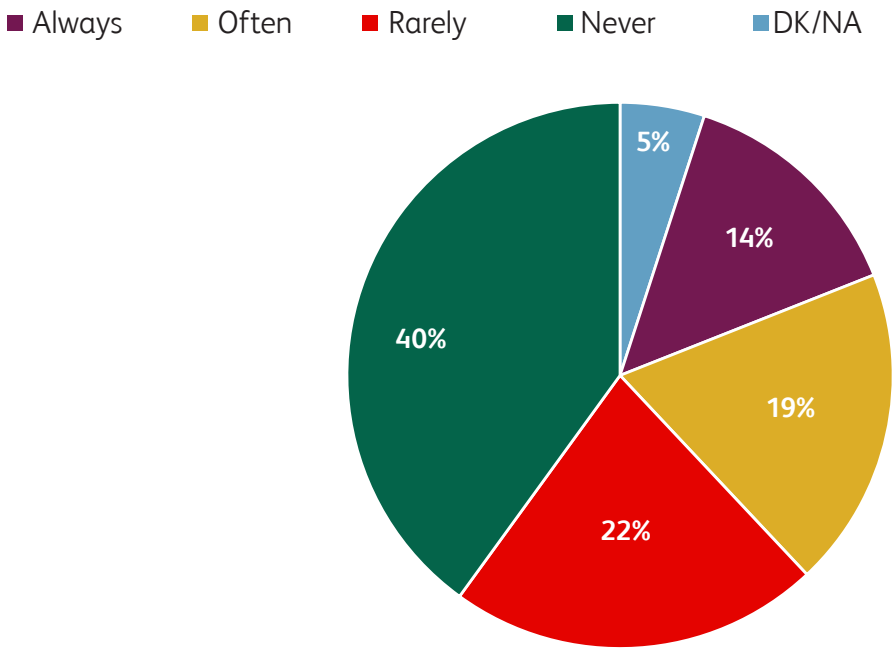
Only a small number of people report reading privacy policies[3] and website terms and conditions[4] fully, especially privacy policies. The GB Consumer Privacy Index reported that just 12% of participants ever read online privacy policy agreements (TRUSTe, 2016a), and the Eurobarometer found that only 13% of participants in the UK are doing so (European Commission, 2015).

More broadly, one study reported that a fifth of participants (20%) read terms and conditions thoroughly, whereas a higher proportion (45%) 'skim read' them (Ofcom, 2016b). Other research found that 40% of participants never read website terms and conditions (Williams et al, 2015). A more recent study by Doteveryone (2018) reiterated these findings. It reported that 58% did not read terms and conditions and, perhaps more worryingly, 43% thought that there was no point reading terms and conditions since companies 'do what they want anyway'. There was a clear consensus from participants in this study that companies need to do more to make terms and conditions understandable and clear (89%).

3 A Privacy Policy agreement is used by a website or app that collects personal information from users. This outlines what information is collected and how it is used

4 A Terms and Conditions agreement is the legal agreement that outlines the rules, requirements, and standards of using a website or an app.

Figure 4.5 How often do you read the terms and conditions on websites you use?

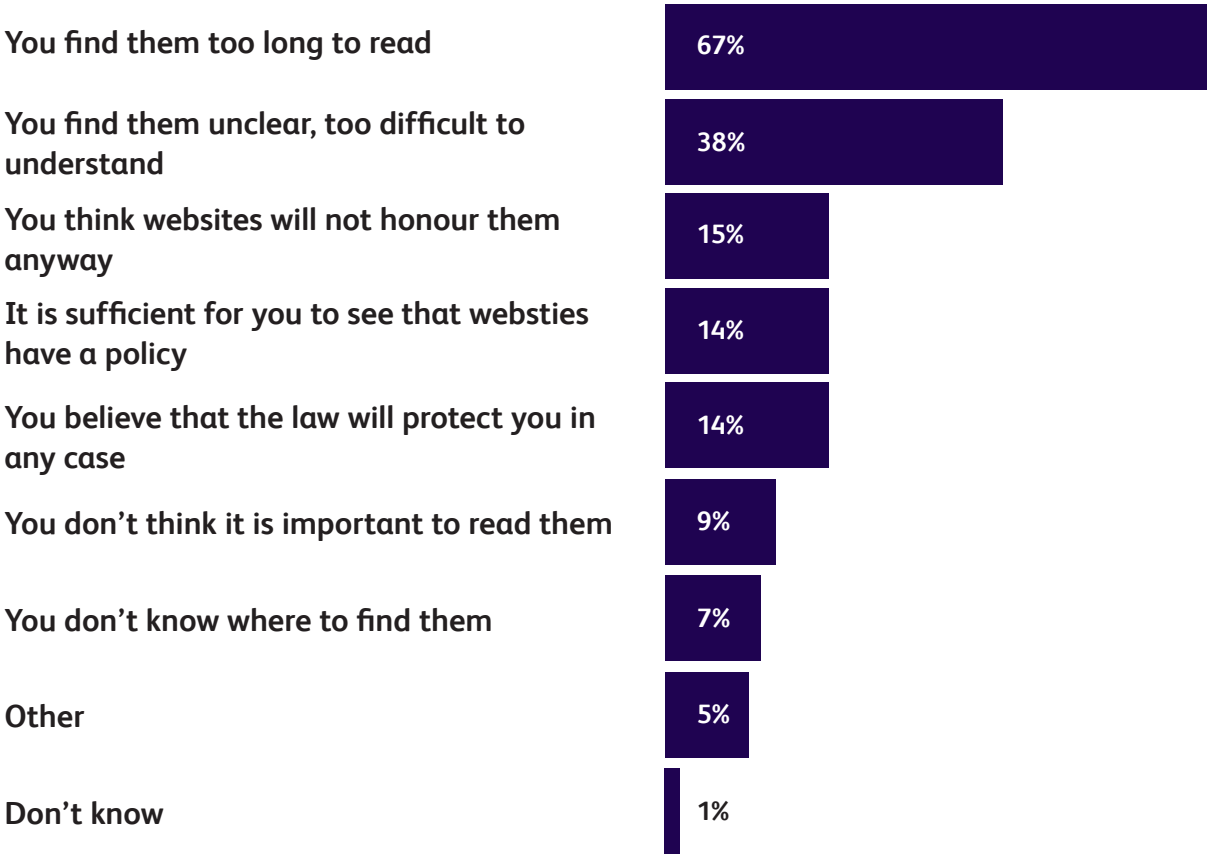


Base: All (102) *Source: Optional Data Disclosure and the Online Privacy Paradox: A UK Perspective (2016)*

The GB Consumer Privacy Index also asked about awareness of privacy policies and found that only a third of people (31%) are aware that they can read these. However, a much higher proportion of participants are aware of website terms and conditions and privacy policies when asked about together (93%) – suggesting that public awareness of more generic website terms and conditions is higher than it is of privacy policies per se (Ofcom 2016).

The 2015 Eurobarometer explored reasons why these policies are not being read. The most common reasons given are that people find the statements too long to read (67%), and they find them unclear or too difficult to understand (38%) (European Commission, 2015). This is further supported by Williams et al (2015) who found that the main reason given by participants for not reading policies was that they were too long and complex.

Figure 4.6 Reasons for not reading privacy statements/ policies



Base: Participants who do not fully read privacy statements (17,356 in EU 28 countries) Source: Special Eurobarometer 431: Data protection, Directorate-General for Communication, 2015

(c) Password hygiene

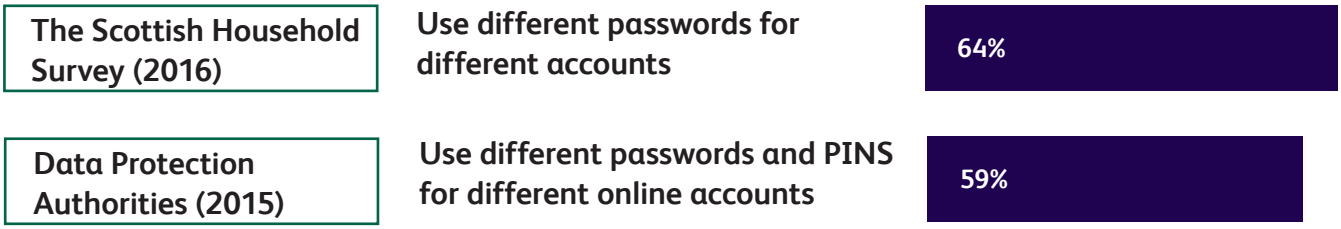
In order to keep online accounts secure, good 'password hygiene' is required. This refers to tactics such as: creating strong passwords (length, mixed characters, not using personal information e.g. name, birthdays); using different passwords for online accounts; and regularly changing passwords.

Password variation

A number of studies explored the proportion of participants who use 'different' passwords for their various online accounts. The Scottish Household Survey found that 64% of participants[5] use different passwords for different accounts, and the ICO information Track Rights Research found that 59% use different passwords and PINs for different online accounts.

5 In Scotland

Figure 4.7 Use of different passwords across different/all online accounts



Base: The Scottish Household Survey: Adults who use the internet 2,420; Data Protection Authorities All: 1,249 Source: Scottish Government (2016); Information Commissioner's Office (2016)

Although the proportions using different passwords seem higher than might be expected it is worth noting that these examples ask participants to make a judgement as to what constitutes 'different passwords'. For example, an individual who uses two or three passwords for all their online accounts may have stated that they use different passwords, and therefore be included, when the recommendation is to use a different password for every account[6].

This important detail is supported by evidence from the 2017 State of Consumer Privacy and Trust report, which highlighted poor 'password hygiene' as a concern as the majority of participants (70%) use seven or fewer passwords for all their online accounts (Gigya, 2017).

Strength of passwords used:

Another factor which contributes to password hygiene is the strength of the passwords used – i.e. the length, inclusion of mixed characters, cases and numbers.

The Adults' Media Use and Attitudes Report (Ofcom, 2017) stated that 54% use 'strong passwords'. Similarly, the 2016 Scottish Household Survey also found that over half of Scots (54%) reported that they use complex passwords. Again, both studies were based on self-report data, and what participants perceive to be a 'strong' or 'complex' password.

The Adults' Media Use and Attitudes Report (Ofcom, 2016) also explored the prevalence of using 'easy-to-remember' passwords and found that over a third (36%) agree with the statement: 'I tend to use easy-to-remember passwords like birthdays or names.'

Password security and mobile phones:

Digitally Savvy Citizens 2016 found that around two-thirds to three-quarters of people report protecting access to their mobile phone using a passcode. The figures varied depending on where citizens lived; this was more common in Scotland (76%) and Ireland (76%) than in England (70%), Wales (68%) and Northern Ireland (66%) (White, 2017).

6 https://www.getsafeonline.org/protecting-your-computer/passwords/

(d) Use of location services

Most mobile devices have a built-in location function or tracker, which can be used to provide localised services for the user of the device. However, this function potentially infringes individuals' privacy.

According to the GB Consumer Privacy Index, just over a quarter of participants (28%) turn off location services on their mobile phone (TRUSTe, 2016a), whereas the Digital Savvy Citizens report found that this percentage was higher, with around half of those in England (48%), Northern Ireland (47%) and Wales (54%) turning off location services, rising to 60% in Scotland and Ireland (White, 2017).

A total of 74% of social media users post their exact location online by 'checking in' when visiting places of interest (e.g. bars, theatres, cinemas, tourist attractions), although around one-third (36%) of those who do said that they always consider the privacy implications in advance (Ofcom, 2017b).

(e) Managing privacy on social media accounts

The level of protection used to preserve privacy on social media varies considerably between individuals.

Public accounts and changing privacy settings:

A small proportion of people report that they have public accounts or make their posts public. Digitally Savvy Citizens found that around a fifth of participants, in most jurisdictions, held public social media profiles, meaning that their names, photos and posts are publicly available[7]. Optional Data Disclosure and the Online Privacy Paradox found that 37% of people either always or often make their social media posts public (Williams and Nurse, 2016).

The evidence is inconsistent regarding how likely people are to actively change their social media settings. For example, the Adults' Media Use and Attitudes Report stated that two-thirds of Facebook (67%) and Instagram (67%) users, and just under half (47%) of Twitter users, have changed their privacy settings from the default setting (Ofcom, 2016b). However, the GB Consumer Privacy Index reported a much lower figure of 31% (TRUSTe, 2016a) when looking at social media more generally.

The Eurobarometer supports the higher figures, with 71% of participants[8] in the UK changing their social media privacy settings (European Commission, 2015).

Qualitative research by Ofcom explored the reasons why participants felt that it is important to ensure their social media profiles are private. One key reason is to reduce the impact of social media on future career prospects:

> "I'm applying for summer internships and placements and stuff for next summer, and the first thing that people do is look you up on social media, or get someone to look you up. I've made sure that everything I'm on is completely private."

(Adults' Media Lives 2016, Female 24, Scotland).

7 The research used the term 'social media' rather than breaking down the question into specific platforms which may gain different responses.

8 Participants who use social media

Personal details on social media accounts:

The Eurobarometer found that around three-quarters (78%) of participants (in the UK) who try to change their privacy settings find the process easy. People[9] who have not changed their privacy settings are most likely to say this is because they have not had time to look at the options (20%) or that they do not know how to do so (19%) (European Commission, 2015).

The 'Consumer Fears and Factors in The Fight Against Fraud' report found that 57% of participants provide their full name in social media profiles and 38% include their date of birth and age. However, only 1% reported that they include their address on their social media profiles (Equifax, 2017).

(f) Providing false or limited information

A tactic employed by some citizens is to provide companies with false or limited information as a means of protecting their online privacy. Adults' Media Use and Attitudes Report found that a quarter (25%) of internet users agree they give out inaccurate or false information online, in order to protect their online privacy (Ofcom, 2017).

Digital Savvy Citizens also found that between a quarter and 43% of participants (depending on where they live) use a name online that is different from their real identity (Scotland: 43%; Wales: 35%; England: 33%; Ireland: 29%; and Northern Ireland 25%).

Qualitative Ofcom research supports the suggestion that this behaviour is undertaken in order to protect online privacy, with people reporting they provide false information such as names, birthdays and email addresses.

> "I will only give what's publicly available: name, address. date of birth, well I won't necessarily give that correctly… In fact, I very rarely give the correct date of birth."

(Adults' Media Lives 2014: Male, 60, England).

> "I don't use my real name. I don't use my real age."

(Adult Media Lives 2016: Female, 55, England).

> "I use my Gmail address, but I just miss one of the characters out so I don't get any correspondence from them. It's the same as phone numbers, I just change one digit because I don't want to be getting texts galore from them."

(Adult Media Lives 2015: Male, 42, England).

9 In the UK

Higher proportions withhold information that is not a compulsory requirement, although these figures vary among the different reports. One study reported that 61% of participants agree with the statement: 'I always try to hide my personal data when using internet sources' (ICO, 2016). The Adults' Media Use and Attitudes Report 2016 reported a higher figure for similar behaviour, with the vast majority of participants (82%) agreeing with the statement: 'I tend to give the minimum amount of personal information required online' (Ofcom, 2016b).

Over a third (35%) of participants will avoid using a website altogether if they feel that too much personal information is required (ICO tracker, 2015).

Demographic differences in data privacy behaviour

Not all the studies explored variations in online privacy behaviours based on age, gender and socioeconomic status. Where this data was available, the greatest differences were noted between age groups/generations and in relation to socioeconomic status.

Age/generational differences:

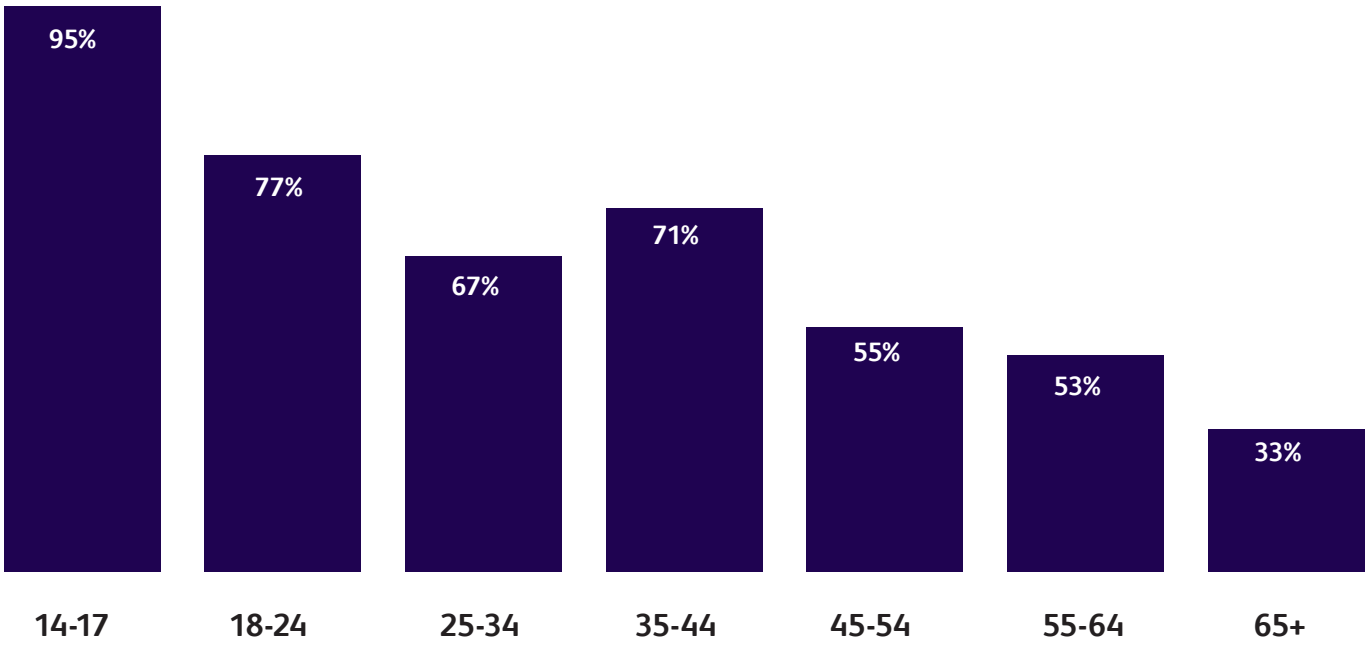
There are some differences in online privacy behaviour by age of participants. However, there is no clear trend across the studies in terms of which age group or generation demonstrate more secure behaviours and take action to better protect their online privacy.

That said, there are clear trends in relation to password hygiene. Younger participants are more likely than older participants to use the same passwords for their online accounts (Ofcom, 2016b; ICO, 2016; Gigya, 2017). For instance, 85% of Millennials use seven or fewer passwords, compared with 54% of Baby Boomers (Gigya, 2017). However, there is competing evidence to show that at least in some contexts, it is the younger age groups acting more privately. In contrast, older participants are more likely to use easy-to-remember passwords, such as names and birthdays (Ofcom, 2016b). Younger age groups are also more likely than older groups to say that they us a passcode or PIN to prevent unwanted access to their mobile phone (White, 2017).

Similarly, behaviours differ between older and younger generations in relation to providing false or limited information to protect online privacy. Those aged 55-64 are the more likely to agree that they give out minimal information online (Ofcom, 2016b), whereas younger groups are more likely to agree that they provide false information in order to protect their privacy (Ofcom, 2017b; Ofcom 2016b). The use of false names online is less common in those aged over 55 years (White, 2017).

Younger age groups reported being the least pro-active in protecting their privacy on social media platforms. For example, they are the most likely to show their full name and/or age (Equifax, 2017) and to set their profiles to public (White, 2017). They are also the least likely age group to fully consider the privacy and security implications before 'checking in' on social media (Ofcom, 2017b). The ODI (2018) found that one in four young British adults trusts social media platforms with their data, compared to just one in 20 of their parents' generation. However, these actions by younger people do not necessarily represent a lack of awareness of these issues. Blank et al (2014) found that there was a strong inverse relationship between age and whether a respondent had checked or changed their privacy settings on social network sites, with younger age groups much more likely to do so that older age groups (Figure 4.1)

Figure 4.8 Percentage of SNS users who check or change their privacy settings by age



Base: SNS users (871) *Source: OXiS (2014)*

Other differences include:

- Older participants (over 55 years of age), are least likely to turn off location services on their mobile phone (White, 2017).
- Older participants (over 65s) are least likely to make a judgement about a website before entering personal information (Ofcom, 2016b).
- Internet users aged 25-34 are the least likely to use antivirus software, firewalls and antispam software (ICO, 2016; Ofcom, 2017b).
- Older participants were more likely to read terms and conditions thoroughly (32%) than any other age group, particularly the youngest group. Only 12% of 16-24 year olds read terms and conditions thoroughly (Ofcom, 2016b).

Gender differences:

The evidence reviewed for this study suggests that variation by gender in online privacy behaviour is often minimal. Research by Ofcom (2017) highlights that men are more likely than women to say they use the following features: firewalls; downloading the latest software updates onto devices; and using ad-blocking filters or software.

Socio-economic differences:

Those from the higher socio-economic grades (AB households) take greater precautions and adopt more protective behaviours in relation to their online privacy than those from the lowest socio-economic backgrounds (DE households). Compared with those living in AB households, DE householders are:

- less likely to use a passcode on their phone (White, 2017)
- less likely to turn off location services on their mobile (White, 2017)
- less likely to use security software such as an anti-virus or anti-spyware packages (Ofcom, 2017b)
- less likely to make a judgement on the security of a website before entering personal information (Ofcom, 2017b)
- more likely to use the same passwords for multiple online accounts (Ofcom, 2016b; Ofcom, 2017b).

These findings are supported by evidence from the United States in two academic papers that were reviewed for this report. Madden et al. (2017) found that those on lower incomes were less likely to exhibit secure behaviours. For example, while 79% of those earning $20,000 or more used privacy settings to limit who could see what they posted online, only 65% of those earning below $20,000 said the same. Another example (Li et al, 2018) explored online privacy skills among disadvantaged urban communities in the US. They found no differences in digital privacy skills among those who had private access to the internet, but that those relying on public internet access, for instance in the library, cited lower digital skills.

UK versus other European countries

The Eurobarometer 2015 found that there are behavioural differences between different European countries in terms of protecting data online.

Citizens in Northern and Western European countries appear less likely to say that they read privacy policies fully. For example, only 13% of UK participants read privacy policies. Levels were lowest among participants in the Netherlands (10%). In contrast, this figure was, for the most part, significantly higher amongst citizens in Eastern European Countries[10] (European Commission, 2015).

However, findings relating to the use of privacy settings on social media accounts tell a different story. On this issue, the Eurobarometer found that people in Northern and Western Europe are more likely to say that they change their privacy settings from the default setting compared to their peers in Eastern and Southern Europe[11].

UK versus the United States

The Consumer Privacy Index was conducted in both the UK and the US (TRUSTe, 2016a; TRUSTe, 2016b), therefore allowing for direct comparison of the data and behaviours between the two countries. In terms of behaviours, there was very little difference between the two. This study assessed behaviours such as:

10 Bulgaria: 38%, Czech Republic: 33%, Slovakia: 30% and Hungary: 29%

11 I.e. UK: 71%, the Netherlands: 71% and Sweden: 70% compared with Hungary: 39%, Italy: 40%, Poland: 44% and Croatia: 49%).

not clicking on an online add; not downloading an app; withholding information; and stopping an online transaction. Across these measures the differences between the two countries were marginal.

Ipsos Global Trends also reported specific comparable data on the UK and US and found that a very similar proportion of UK and US participants do not fully read website terms and conditions; 73% of participants in GB, compared with 71% of participants in the US (Ipsos, 2017b).

What is the impact of the perception of data infringement?

Given the widespread examples of data breaches that have occurred in recent years, it is important to understand how people act and change their behaviours in response to these events to better protect their online data and privacy. The research illustrates that following a data/security breach, most participants will take action to improve their online privacy and security. These actions include: changing their passwords; adding a second level of authentication; and closing accounts. It also raises individuals' awareness and vigilance in relation to online privacy and security.

The 2017 State of Consumer Trust found that after a data breach, 62% change their passwords, 32% add a second level of authentication and 18% close accounts. However, 22% make no change (Gigya, 2017).

Qualitative research by Ofcom supports this finding, with participants stating they have taken similar action after encountering a data breach (Ofcom, 2017a).

> "We've had to change passwords. We've looked at things like firewalls, we've looked at the additional security…"

(Adult Media Lives 2016: Female, 39, Wales).

Introduction of GDPR

The General Data Protection Regulation (GDPR) is one of the most important changes made to data privacy legislation in recent years. It was introduced on May 25, 2018 and aims to increase protection for the public and to give them more control over what happens to their personal data.

However, the research shows that most people had limited awareness of the new regulation, at least until close to the implementation date. For example, Thales (2017) found that only 37% of participants in their study had heard of GDPR and that only 57% of those that had heard of it could explain it. Similarly, Big Brother Watch (2017) found that a third of their participants had heard of the GDPR and, of those, less than half (43%) knew what rights the legislation conferred upon them. This was further supported with research by Pegasystems (2017) who found that 79% did not know that the GDPR was coming.

While awareness of the regulations was low at the time of those studies, once participants were informed about the rights that GDPR would give them, the research suggested that they may take advantage of it. Pegasystems found that 82% would be likely to ask to see, limit or erase the personal data that companies hold about them. Furthermore, they said they would act if there was a breach: in one study 69% said they would consider going to a watchdog (Thales, 2017), while in another, 80% said they would complain – although 53% said they did not know who they would complain to (Big Brother, 2017).

5. A Privacy Paradox?

What is the Privacy Paradox?

It's clear from the evidence reviewed in chapter three that people generally have some concern about their online data privacy. However, chapter four highlights that their actions in relation to the privacy of their data often fall short of adequately protecting their privacy. This mismatch between attitudes and behaviour has been termed by researchers as the 'Privacy Paradox'.

There is not only a discrepancy between people's concern about online privacy and their actions, but also between perceptions of how secure their behaviour is and what they actually do. In the TRUSTe Consumer Privacy Index (2016), 74% of British internet users said that they believe they adequately protect their personal data online. However, in the same survey only 12% reported that they read privacy policies, 28% reported that they turn off location tracking on mobile devices and just under a third (31%) have changed their social media privacy settings.

It is important to note that the vast majority of behaviour recorded in the literature reviewed is self-reported. This may mean that the paradox is even more significant than it first appears. In survey research, participants can present themselves in a more positive light in order to provide the 'right' answer as prescribed by society. If such a 'social desirability effect' is at play in this instance, then it is possible that the prevalence of 'secure' online behaviour may be even lower than actually recorded.

There is some research evidence to support this hypothesis. In their 2015 US paper, Wittes and Liu took a different approach that did not rely on self-report in order to get a sense of how much personal information the public are willing to disclose online. To do this, they looked at Google 'Autocomplete algorithm', and identified that some of the most common autocomplete responses to the phrase 'I think I am' were highly personal statements such as 'pregnant', 'depressed', 'bipolar' and 'gay'. While the study did not aim to provide a robust scientific measure of privacy, it does provide an indication that, at least in certain contexts, people are willing to 'confess all sorts of things to Google', which contrasts with self-report data indicating a desire to maintain online privacy (Wittes and Liu, 2015).

What are the reasons for the Privacy Paradox?

While much of the literature describes the Privacy Paradox, the reasons for the phenomenon are not directly addressed in many of the large-scale quantitative studies. However, they are the focus of a number of the academic papers reviewed for this report.

There is no clear consensus in the literature on the drivers of the Privacy Paradox. This may partly reflect the many varied contexts within which the phenomenon has been investigated. For instance, in a study from the US, Athey, Catalini and Tucker (2017) explored the Privacy Paradox through an experimental design related to choices MIT students made to protect digital currency (Bitcoin) they had been given. In contrast, Hargittai and Marwick (2016) conducted qualitative research investigating self-disclosure behaviour on social networking sites. Such differing studies naturally produce very different results.

Of course, the lack of a consensus may also reflect the fact that there is no single explanation and people's reasons for acting less securely or less privately will be dependent on the type of interaction and the context in which it happens. The next sections outline the main explanations provided in the evidence reviewed.

As noted in chapter two, there was some evidence between 2012 and 2015 of a decrease in concern about data privacy linked to increasing apathy around data protection. As it became increasingly difficult avoid to providing personal data to navigate life online, there was a growth in the strength of feeling that there was very little people could do to control this (Ofcom, 2015). This lack of ability to change the situation meant that while they were still concerned, they did not act on their concern as they felt there was little point (Hargittai and Marwick, 2016):

> "I think like: "Oh I better add a few random numbers in this password", or do this or that, but you know besides that I'm also wondering, what can I really do?"

(Male, 20)

As noted above however, it is not yet clear whether recent high-profile data breaches and new legislation to give citizens more power have affected this feeling of a lack of control – and even if they have, has it resulted in people taking more action to protect their data?

Another potential explanation for the Privacy Paradox identified in the evidence is a lack of knowledge and awareness of the tools that can be used to make online behaviour more secure (Rainie and Madden, 2015). This includes 'do not track' search engines, email encryption or the use of proxy servers. Related to this, the evidence highlights an apparent lack of awareness among some people of the potential risks of disclosing information (Hargittai and Marwick, 2016).

> "I don't really care if somebody gets a hold of my Facebook, like I don't have anything with credit cards really linked…the most they could do would be to delete my content, which would be kind of sad for me, but, I dunno."

(Female, 20)

This lack of awareness also seems to extend to knowledge of what data is collected and what impact this may have. Findings from the 2018 Doteveryone Attitudes Report showed that only small proportions were aware that data about their internet connection (38%) is collected, data about things they do on other websites on the same device is collected (28%), or that information that other people share about them is collected (17%).

> "I didn't realise the extent to which companies were saving data personal to individuals to use or sell for their own benefit, and that it is almost accepted as a given that companies can do this."

(Doteveryone Attitudes Report, 2018)

It seems that citizens are more likely to act 'securely' in areas where protective steps are easier and where the implications for them of privacy infringement are more obvious or direct – e.g. public social media accounts; or giving out their email address details/personal details. In contrast, where protective steps

are more time-consuming or less obvious – e.g. reading website privacy policies/anonymization software/ deleting cookies – and where the implications of infringement seem more abstract, they do not. This would suggest that while people say that security is more important than convenience (KPMG, 2017), this is not the case in practice. Athey et al (2017) found that even the smallest inconvenience stopped participants in their experiment selecting the more secure option of storing digital currencies, even when they were fully informed of what the security consequences would be.

There is little information to enable international comparison between the UK and other countries to understand if the gap between attitudes and behaviours is significantly different.

What data trade-offs are the public willing to make?

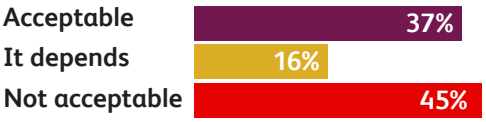
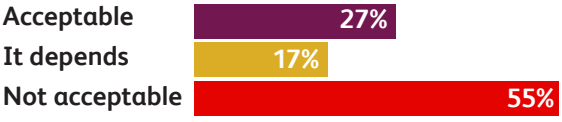
A key avenue of research on the Privacy Paradox has related to trade-offs – i.e. for what reasons the public would compromise their personal online data privacy. A number of papers (DMA, 2015; KPMG, 2017) exploring this issue have found that the public is willing to bargain their personal data for a variety of incentives:

- free/discounted products or services – access to some sort of free service (e.g. email, search engines, social media)
- a better, personalised service (although this is less popular than other trade-offs as it can lead to nuisance marketing)
- availability (people may use a service or website that they are not sure of or think has suspect security practices if they can't get that product or service elsewhere)
- for the 'public good'[12] – research by the Open Data Institute (2018) found that nearly half of respondents (47%) would share medical data about themselves, if it helped develop new medicines and treatments.

A report for the Department for Culture, Media & Sport, London Economics (2017) conducted a 'choice experiment' that tried to get participants to provide a realistic valuation of what their data rights are worth in the context of three types of transactions: loyalty cards, smart meters and health insurance rewards. The results showed that individuals would rather generally seek to protect their data rather than choose to protect savings of roughly 5% to 10%. In the US, one study revealed the circumstances under which many Americans thought it was acceptable or unacceptable to share personal information (Pew Research Centre, 2016) as shown in Figure 5.1.

12 The definition of 'public good' with regards to data use is rarely explicitly defined.

Figure 5.1 Acceptability of data trade-offs

Sharing health information. A new health information website is being used by your doctor's office to help manage patient records. Your participation would allow you to have access to your own health records and make scheduling appointments easier. If you choose to participate, you will be allowing your doctor's office to upload your health records to the website and the doctor promises it is a secure site.	
Retail loyalty cards. A grocery store has offered you a free loyalty card that will save you money on your purchases. In exchange, the store will keep track of your shopping habits and sell this data to third parties.	
Auto Insurance. Your insurance company is offering a discount to you if you agree to place a device in your car that allows monitoring of your driving speed and location. After the company collect data about your driving habits, it may offer you further discounts to reward you for safe driving.	
Free Social Media. A new social media platform is being used by your former high school to help manage communications about a class reunion. You can find out the basic information about the reunion over email, but your participation on the social media site would reconnect you with old friends and allow you to communicate more easily with those who are attending. If you choose to participate, you will be creating a profile using your real name and sharing a photo of yourself. Your access to the service is free, but your activity on the site would be used by the site to deliver advertisements it hopes will be appealing to you.	
Smart Thermostat. A new technology company has created an inexpensive thermostat sensor for your house that would learn about your temperature zone and movements around the house and potentially save you on your energy bill. It is programmable remotely in return for sharing data about some of the basic activities that take place in your house like when people are there and when they move from room to room.	

Base (461) *Source: Pew Research Centre (2016)*

However, in general, the US literature is much more focused on the trade-off between national security and civil liberties with evidence suggesting that the latter is seen as at least as, if not more, important than the former to most Americans. One study reported, for example, that only 25% of individuals would be willing to give up the privacy of their internet activities if it would help the US Government foil domestic terrorist plots (Reuters, 2017). By comparison, although there is much less evidence on UK attitudes in this area, a recent UK study indicates a slightly higher level of support for privacy infringements on the grounds of national security, with 32% of UK citizens agreeing with the statement: 'More should be done to help the Government fight crime and protect national security even if this means the privacy of ordinary people suffers' (Rogers, 2017).

How can secure online behaviour be better supported?

In addition to the lack of consistency between attitudes and behaviours, the literature covered in the evidence review does not widely explore the changes that people would like to see in the future in much depth. Among those studies that did explore this issue, there was no clear single way forward that had strong support. This was due in part to the fact that each specified an action and asked participants how much they supported the action, rather than asking an open question, and there was little convergence across the research on the actions considered. The evidence does suggest that consumers want online data privacy to be more transparent and easier to achieve.

Although there was no real consensus across the different studies, a few key improvements were highlighted by participants:

1. The ability to delete personal information collected – 66% of consumers said that they would be likely to ask companies to remove personal details held about them if it was made easier to do so (Deloitte, 2016).

2. Greater control over personal data[13] – this was a key issue for people. In the 2015 DMA report Data privacy: what the consumer really thinks, 90% of consumers said they would like more control over their data . Furthermore, 91% of participants in the Doteveryone 2018 Attitudes report said that it's important to be able to choose how much data they share with companies (although 51% can't currently find out that information).

3. Greater transparency from companies/organisations using data – the 2016 US and UK TRUSTe Consumer Privacy Indices suggested one of the top two ways organisations could lower privacy concerns among consumers was to be more transparent about how they were collecting and using data. The ODI (2018) found that a third of participants would feel more comfortable sharing data if organisations provided an explanation of how they intended to use or share it.

4. Easier to use data privacy tools – this was cited as one of the other most important ways that organisations could lower privacy concerns among consumers. However, as previously noted, there are low levels of use of existing privacy tools, so it may be that the focus needs to be on raising awareness of what is available, rather than creating new tools.

5. Clearer channels of responsibility and accountability – in several studies, there was a sense that participants wanted there to be greater oversight of data privacy online. However, there was often no consensus over what this would look like or who would be responsible. For instance, when asked who should be responsible for enforcing rules to ensure we are treated fairly, 66% said the Government should play a role, 61% said that the companies collecting the data should share responsibility, while 60% would like to see the creation of an independent body.

> "In other industries – if someone rips you off – you go to the Ombudsman. I don't know if there is an Ombudsman for the internet – but if there is who is it?"

(Doteveryone Attitudes Report, 2018)

13 However, it is important to note that 'more control' was not defined in the research.

6. Conclusions

This report sought to explore the available data on the UK public's attitudes and behaviours towards data privacy and engaged with 50 pieces of literature from the past three years. Whilst the aim of this review was not to provide specific recommendations for action, we can conclude a number of important themes from the evidence:

1. Lack of consensus on definitions, interpretations and boundaries

No clear consensus emerged across the literature on the exact definition or remit of online data privacy and interpretations are varied. Key definitions were developed pre-social media and the definition of 'privacy' in a digital age needs to be further explored within published research. What does it mean to the UK public, what is important to the public and how does that differ by different groups?

2. Concern around data privacy is significant

There is little doubt that people in the UK are concerned about the privacy of their data online. Accounts indicated that on average around 75% of the UK public are at least fairly concerned about the privacy and security of their personal data online.

3. Level of concern varies across sources

Estimates of the exact level of concern vary widely. There is little consistency across the studies explored in this review and contradictions arise within different data sets in relation to each of the key attitudinal questions. This is due in some part to a lack of continuity in the measures and definitions used in the various studies. Whereas some literature uses very broad terms (e.g. concern around online data privacy), some focuses on very specific issues (e.g. concern about using a specific social media sites, or household appliances with internet connectivity), and some still uses alternative terminology altogether.

4. Confidence in protecting data privacy is also high

Despite concern, personal confidence in managing access to personal data online is also high, with similar proportions of the public (72%) suggesting they are either fairly or very confident. Though it is also important to note that this was self-reported confidence and the genuine ability to do this was not investigated.

5. Context matters for privacy conversations

When exploring these themes around data privacy attitudes in greater detail, the evidence suggests that concern or confidence are significantly linked to the context in which personal data is shared. Users are most comfortable sharing data with public-sector organisations, and less comfortable with private companies, particularly telecommunications and social media companies.

6. Apathy was rising – is it still?

A number of studies highlighted that significant concern about online data privacy was actually decreasing over time, with the proportion of those apparently 'unconcerned' increasing. A number of explanations for this trend have been speculated, including that although the public are aware of increasing online data collection they have become more resigned to the inevitability of it. However, the evidence does not yet capture whether recent high-profile data scandals and breaches, and the implementation of new regulations to give citizens greater control over their data have slowed or reversed this trend towards a feeling of disempowerment.

7. Data privacy behaviours employed demonstrate the UK public are taking some actions to protect privacy, but more understanding is needed

Behaviours demonstrate concern to a certain extent. The findings indicate that the public do take precautions to keep their information safe in terms of employing a variety of privacy 'tactics', the most common being related to passwords and internet browsing security measures.

8. 'Privacy Paradox' is evident in the UK

Nevertheless, the evidence clearly suggests that the public's level of concern regarding online data privacy is often not reflected in the steps they take to secure their personal information. Furthermore, the behaviour that they consider to be secure is not always so. This 'privacy paradox' is evident in the UK research, but was only explicitly mentioned in a small number of studies. It was more common for this phenomenon to be explored in the US literature. There is no clear single explanation for the mismatch between attitudes to, and behaviours related to, online data privacy. Possible explanations include:

a. the feeling of powerlessness in the face of the seemingly inevitable increase in personal data collected online and lack of transparency about how it is used

b. a lack of awareness of the tools and techniques available to protect data, and what is considered secure behaviour in different contexts

c. a lack of understanding of the potential implications of a lack of online data privacy. There is a clear need for greater awareness about what the standards of 'good' privacy protection actually is – i.e. what best practice looks like when it comes to online data privacy. More consideration should be given to the public's misconceptions in relation to 'best practice' online behaviour (e.g. using different passwords for every online account) and how to address these.

9. Trade-offs are common, but diverse in their format and intention

The public report continually making trade-offs with regards to their data privacy online. However, these vary in terms of the intention, with the public reporting trade-offs both for private gain in terms of access to personal services and convenience, but also 'public good'.

10. Age is not a clear-cut indicator of overall behaviour

In terms of age, there is no clear overall pattern. There is a tendency for older participants to be more concerned and at least say that they act more securely. However, there are also particular contexts, where young people tend to behave more securely.

11. Lack of UK-based research focusing on demographic differences or implications

There is limited information available about demographics, with the exception of age and even this is predominantly constrained to views over the age of 16 or 18. The limited data does suggest that different groups exhibit different secure and unsecure behaviours online, and have differing privacy priorities. The very small amount of data on socioeconomic status suggests that those at the lower end of the socioeconomic scale are more vulnerable to behaving in unsecure ways online. There is no consensus in the literature on gender differences. This means there is unlikely to be a 'one size fits all solution' and that targeted solutions are likely to be required.

12. Culturally the UK is more aligned with the US than Europe

For both attitudes and behaviours towards data privacy, the available evidence suggests the UK is far more similar to the US than Europe. The data highlighted that people in the UK express higher levels of concern than most other European countries, but concern and behaviours are in line with, or not significantly different from, the US public.

13. Assortment of limitations in the existing literature research methods

A number of challenges with data have been noted throughout this review. Inconsistencies in terminology, reliance on self-report, lack of trend data, focus on quantitative large-scale methods and the use of a range of different indicators all contribute to the complexities of researching UK attitudes and behaviours towards data privacy.

7. References

1. Acquisti, A., Brandimarte, L. and Loewenstein, G., (2015), Privacy and human behavior in the age of information. Science, 347(6221), pp. 509-514

2. Bartlett, J. and Gaston, S., (2017). Public Views on Technology Futures. Demos: Centre for analysis of social media, Available at: https://www.demos.co.uk/project/public-views-on-technology-futures/ [Last Accessed 08/02/2018]

3. Big Brother Watch, (2017), 'Topline Figures: UK Citizens' Attitudes Towards The General Data Protection Regulation', Available at: https://bigbrotherwatch.org.uk/wp-content/uploads/2017/12/GDPR-Polling-Toplines-final.pdf [Last Accessed 28/06/2018]

4. Bode, L. and Jones M. L., (2017), Ready to forget: American attitudes toward the right to be forgotten. The information Society: An International Journal, 33(2), pp. 76-85

5. ComRes, (2015). UK Public Research – Online Privacy: Big Brother Watch. Summary Report, London, Available at: https://www.bigbrotherwatch.org.uk/wp-content/uploads/2015/03/Big-Brother-Watch-Polling-Results.pdf [Last Accessed 08/02/2018]

6. Deloitte, (2015). The Deloitte Consumer Review: Consumer data under attack: The growing threat of cybercrime. London, Available at: https://www2.deloitte.com/tr/en/pages/risk/articles/consumer-data-under-attack.html [Last Accessed 08/02/2018]

7. Doteveryone, (2018a), 'People, Power and Technology: The 2018 Digital Attitudes Report', Available at: http://attitudes.doteveryone.org.uk [Last Accessed: 28/06/18]

8. Doteveryone, (2018b), 'People, Power and Technology: The 2018 Digital Understanding Report', Available at: http://understanding.doteveryone.org.uk/ [Last Accessed: 28/06/18]

9. Equifax, (2017). Consumer Fears and Factors in The Fight Against Fraud. Available at: https://www.equifax.com/assets/unitedkingdom/article_yougov_consumer_fears_and_factors_in_the_fight_against_fraud.pdf [Last Accessed 08/02/2018]

10. European Commission, (2015). Special Eurobarometer 431: Data protection, Directorate-General for Communication, Available at: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/search/data%20protection/surveyKy/2075 [Last Accessed 08/02/2018]

11. Gfk, (2017). Europe online – an experience driven by advertising. Summary Results, Available at: https://www.iabeurope.eu/wp-content/uploads/2017/09/EuropeOnline_FINAL.pdf [Last Accessed 08/02/2018]

12. Gigya, (2017). The 2017 State of Consumer Privacy and Trust, Available at: https://2sep653x2vim4375oc23b3j9-wpengine.netdna-ssl.com/wp-content/uploads/2017/04/Gigya-Infographic-Privacy-Survey-954x3413.jpg [Last Accessed 08/02/2018]

13. Hargittai, E. and Marwick, A. (2016), "What Can I Really Do?": Explaining the Privacy Paradox with Online Apathy. International Journal of Communication 10(2016), pp. 3737–3757

14. ICO, (2015), Data protection rights: What the public want and what the public want from Data Protection Authorities. Available at: https://ico.org.uk/media/about-the-ico/documents/1431717/data-protection-rights-what-the-public-want-and-what-the-public-want-from-data-protection-authorities.pdf [Last Accessed 08/02/2018]

15. ICO, (2016). Information rights research: Annual Track 2016. Available at: https://ico.org.uk/about-the-ico/research-and-reports/information-rights-research/ [Last Accessed 08/02/2018]

16. Ipsos MORI (2017a). Cybersecurity Poll for Reuters. Available at: http://fingfx.thomsonreuters.com/gfx/rngs/USA-CYBER-POLL/010040EN0YD/2017%20Reuters%20Tracking%20-%20Cybersecurity%20Poll%203%2031%202017.pdf [Last Accessed 08/02/2018]

17. Ipsos MORI, (2017b). Ipsos Global Trends, Available at: https://www.ipsosglobaltrends.com/downloads/ [Last Accessed 08/02/2018]

18. Ipsos MORI, (2016). The One-Way Mirror: Public attitudes to commercial access to health data. Available at: https://www.ipsos.com/sites/default/files/publication/5200-03/sri-wellcome-trust-commercial-access-to-health-data.pdf [Last Accessed 08/02/2018]

19. Ipsos MORI, (2014). Public attitudes to the use and sharing of their data. Available at: https://www.ipsos.com/ipsos-mori/en-uk/new-research-finds-data-trust-deficit-lessons-policymakers [Last Accessed 08/02/2018]

20. Kang, R., Dabbish, L., Fruchter, N. and Kiesler S., (2015), My Data Just Goes Everywhere: User Mental Models of the Internet and Implications for Privacy and Security, in Eleventh Symposium on Usable Privacy and Security, Ottawa, pp. 39-52

21. KPMG, (2017). Crossing the line: staying on the right side of consumer privacy, Available at: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2016/11/crossing-the-line.pdf [Last Accessed 08/02/2018]

22. Li X., Chen W. and Straubhaar J.D., (2018), "Concerns, Skills, and Activities: Multilayered Privacy Issues in Disadvantaged Urban Communities," International Journal of Communication 12: 1269–90.

23. Li, Y., (2014), A multi-level model of individual information privacy beliefs, Electronic Commerce Research and Applications, (13)1, pp. 32-44

24. Livingstone, Sonia (2018) Children: a special case for privacy? Intermedia, 46 (2). pp. 18-23.

25. Madden, M. and Rainie L., (2015). Americans' Attitudes About Privacy Security and Surveillance. Pew Research Center, Available at: http://assets.pewresearch.org/wp-content/uploads/sites/14/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf [Last Accessed 08/02/2018]

26. Madden, M., Gilman, M.E., Levy, K. and Marwick, A. E., (2017) Privacy, Poverty and Big Data: A Matrix of Vulnerabilities for Poor Americans. Washington University Law Review (95)53

27. Marreiros, H., Gomer, R., Vlassopoulos, M., Tonin, M. and Schraefel, M.C., (2015) Scared or naïve? An exploratory study on user's perceptions of online privacy disclosures IADIS International Journal on WWW/Internet, 13(2), pp. 1-16.

28. Moritz Godel (2017) 'The business benefits of improved trust via the GDPR: UK Insurer GDPR and PCI Working Group', London Economics, Available at: https://londoneconomics.co.uk/blog/press-event/business-benefits-improved-trust-via-gdpr-uk-insurer-gdpr-pci-working-group-29-november-2017/ [Last accessed: 28/06/2018]

29. Ofcom, (2017a). Adults' Media Lives 2016: A qualitative study. Summary Report, Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0021/102756/adults-media-lives-2016.pdf [Last Accessed 08/02/2018]

30. Ofcom, (2017b). Adults' media use and attitudes: Report 2017. Summary Report, Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0020/102755/adults-media-use-attitudes-2017.pdf [Last Accessed 08/02/2018]

31. Ofcom, (2016a). Adults' Media Lives 2015: A qualitative study. Summary Report, Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0028/69256/media_lives_2015_summary.pdf [Last Accessed 08/02/2018]

32. Ofcom, (2016b). Adults' media use and attitudes: Report 2016. Summary Report, Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0026/80828/2016-adults-media-use-and-attitudes.pdf [Last Accessed 08/02/2018]

33. Ofcom, (2015). Media Lives: Wave 10 (2014) and Ten Year retrospective. Summary Report, Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0026/63629/medialives10-2014.pdf [Last Accessed 08/02/2018]

34. Open Data Institute (2018) 'ODI survey reveals British consumer attitudes to sharing personal data' Available at: https://theodi.org/article/odi-survey-reveals-british-consumer-attitudes-to-sharing-personal-data/ [Last Accessed: 28/06/2018]

35. Patil, S., Patruni, B., Lu, H., Dunkerley, F., Fox, J., Potoglou, D. and Robinson N., (2015) Public Perception of Security and Privacy: Results of the comprehensive analysis of PACT's Pan-European Survey. PACT Project Consortium, Available at: https://www.rand.org/pubs/research_reports/RR704.html.

36. Pega, (2017), 'GDPR: Show me the data: Survey reveals EU consumers poised to act on legislation', Available at: https://www.pega.com/sites/pega.com/files/docs/2017/Dec/gdpr-show-me-the-data.pdf [Last Accessed: 28/06/2018]

37. Rainie L. and Madden, M., (2015). Americans' Privacy Strategies Post-Snowdon. Pew Research Center, Available at: http://assets.pewresearch.org/wp-content/uploads/sites/14/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf [Last Accessed 08/02/2018]

38. Rainie, L. and Duggan, M., (2016). Privacy and Information Sharing. Pew Research Center, Available at: http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/ [Last Accessed 08/02/2018]

39. Rogers, J. F., (2017). Security Trumps Privacy in British Attitudes to Cyber-Surveillance. YouGov Available at: http://d25d2506sfb94s.cloudfront.net/cumulus_uploads/document/guozfocn1q/YGC,%20GB%20Surveillance%202017.pdf#_blank [Last Accessed 08/02/2018]

40. Soprasteria, (2017). The Citizen View of the Digital Transformation of Government, Available at: https://www.soprasteria.co.uk/docs/librariesprovider41/White-Papers/sopra-steria-ipsos-digital-transformation-of-govt.pdf?sfvrsn=0 [Last Accessed 08/02/2018]

41. Thales eSecurity, (2018), 'Protecting private personal data: Why there's more to the GDPR than just fines' Available at: http://go.thalesesecurity.com/GDPR-Survey-Protecting-private-personal-data-Why-there-is-more-to-the-GDPR-than-just-fines.html [Last Accessed: 28/06/18]

42. The Direct Marketing Association, (2015). Data privacy: what the consumer really thinks 2015. Future Foundation, Available at: https://dma.org.uk/uploads/ckeditor/Data-privacy-2015-what-consumers-really-thinks_final.pdf [Last Accessed 08/02/2018]

43. TRUSTe, (2016a). 2016 TRUSTe/NCSA Consumer Privacy Infographic – GB Edition, Available at: https://www.trustarc.com/resources/privacy-research/ncsa-consumer-privacy-index-gb/ [Last Accessed 08/02/2018]

44. TRUSTe, (2016b). 2016 TRUSTe/NCSA Consumer Privacy Infographic – US Edition, Available at: https://www.trustarc.com/resources/privacy-research/ncsa-consumer-privacy-index-gb/ [Last Accessed 08/02/2018]

45. White, D., (2017). Digitally Savvy Citizens: Data from across the UK and Ireland on how we manage information, security and privacy online. Available at https://www.carnegieuktrust.org.uk/carnegieuktrust/wp-content/uploads/sites/64/2017/09/Digitally-Savvy-Citizens.pdf [Last Accessed 08/02/2018]

46. Williams M., Nurse J. R. C. (2016) Optional Data Disclosure and the Online Privacy Paradox: A UK Perspective. In: Tryfonas T. (eds) Human Aspects of Information Security, Privacy, and Trust. HAS 2016. Lecture Notes in Computer Science, vol 9750. Springer, Cham

47. Williams T., Agarwal, N., and Wigand, R. T., (2015). Protecting Private Information: Current Attitudes Concerning Privacy Policies, Available at: https://www.researchgate.net/publication/279980732_Protecting_Private_Information_Current_Attitudes_Concerning_Privacy_Policies [Last Accessed 08/02/2018]

48. Wong, M., (2017). Pizza over privacy? Stanford economist examines a paradox of the digital age. Available at https://news.stanford.edu/2017/08/03/pizza-privacy-stanford-economist-examines-paradox-digital-age/ [Last Accessed 08/02/2018]

49. Yong, J. P., (2013), Digital Literacy and Privacy Behavior Online, Communication Research, (40)2, pp. 215 - 236

50. Yong, J.P., Scott W.C. and Nojin K., (2012), Affect, cognition and reward: Predictors of privacy protection online, Computers in Human Behavior, (28)3, pp. 1019-1027

The Carnegie UK Trust works to improve the lives of people throughout the UK and Ireland, by changing minds through influencing policy, and by changing lives through innovative practice and partnership work. The Carnegie UK Trust was established by Scots-American philanthropist Andrew Carnegie in 1913.

Andrew Carnegie House
Pittencrieff Street
Dunfermline
KY12 8AW

Tel: +44 (0)1383 721445
Fax: +44 (0)1383 749799
Email: info@carnegieuk.org
www.carnegieuktrust.org.uk

Ipsos MORI Scotland
4 Wemyss Place
Edinburgh
EH3 6DH

Tel: +44 (0)131 220 5699
Fax: +44 (0)131 220 6449
www.ipsos-mori.com
http://twitter.com/IpsosMORIScot

August 2018

CarnegieUK TRUST

CHANGING MINDS • CHANGING LIVES

Carnegie United Kingdom Trust
Incorporated by Royal Charter 1917
Registered Charity No: SC 012799 operating in the UK
Registered Charity No: 20142957 operating in Ireland

ISBN 9781909447899