Ipsos MORI
Social Research Institute

COMMUNICATIONS
CONSUMER
PANEL

November 2016

Digital Footprints: Consumer concerns about privacy and security

Contents

List of Figures

List of Tables

Key Findings

- Whilst there are high levels of **confidence** when using the internet, a significant minority of people are not confident;
- There is a digital divide in high/low confidence - one in five people lack confidence online; and one in three people are not confident to protect themselves by adjusting privacy settings;
- Young people are generally more confident internet users - approximately half of people aged 65-74 are not confident online and this rises to seven in ten in the 75+ age group;
- Younger people are also generally less concerned about privacy than older people;
- The digital confidence divide is not just age-related - there are lower levels of confidence among disabled people, compared to non-disabled people;
- Privacy and security of personal information are major concerns for high confidence and low confidence internet users alike - financial transactions are a particularly sensitive area;
- **Trust** is a key consumer issue - three tenets are essential in building trust: transparency, personal control and security;
- Many people are confining their purchasing to the brands they already trust in the offline world;
- Consumers do not feel completely in **control** of their personal information - people want more control and to decide for themselves what is shared or not;
- Lack of control leads to a sense of disempowerment;
- 14% of people are not using **security** software, or are unaware of it;
- Security measures and the choice to opt out of receiving marketing information are not generally well known;
- People have higher levels of concern about using public Wi-Fi – they have less confidence and are more concerned about hacking and identity theft;
- People have a greater sense of security when using home broadband;
- There are lower levels of confidence when it comes to using security settings on mobiles/tablets;
- There is a perceived lack of transparency about **data use** - people may understand that data is collected but not how it is used, how long it is kept for and why;
- Terms and Conditions and privacy policies are not widely read or fully understood and need to be clearer;
- People want more information about how their personal information will be used; third party sharing was an area of particular concern;
- There is confusion and inconsistency - and conflicting emotions around sharing data online; on balance, consumers feel that collection of personal data is most beneficial to the companies collecting it;
- Consumers do not fully recognise the link between providing personal information and the benefits of doing so;
- There are concerns regarding privacy and control of personal data in regard to Smart products.

Executive Summary

Executive Summary

In 2016 there are more people connecting to the internet than ever before. Consumers use the internet for essentials and entertainment, to keep in touch with family and friends, stay connected with work, consume news and carry out daily tasks such as shopping and banking. Almost nine in ten UK adults say they use the internet somewhere.[1] Most people understand that personal information is collected, stored, and used by public and private sector organisations, however a smaller proportion are aware of how such technologies work or how their personal data is used.

The Communications Consumer Panel commissioned Ipsos MORI to conduct a new study to update their understanding in this area. This research was conducted in February and March 2016 using both quantitative and qualitative methods and began with desk research to inform the design of project. The quantitative element of the research utilises a face-to-face survey conducted with 1,423 adults across the United Kingdom. These findings are enhanced through 21 in-depth interviews with consumers of varying demographics and internet experience. The key findings of the research are summarised below:

Confidence and concern

Eight in ten consumers feel confident using the internet, including nearly all who use the internet on a frequent basis. Most are also confident setting privacy features, but about one in three say they are not confident doing this.

There are signs of a 'digital divide', with one in five people saying they lack confidence in using the internet. The difference between the views of high and low confidence users is a common theme throughout this research and is a primary indicator of consumer attitudes towards online privacy and security. Low confidence users in particular tend to be older, and much more restricted in their internet use.

Overall, privacy and safety of personal details are the top two spontaneous concerns that people have about using the internet. Low confidence internet users are concerned about privacy yet also have specific concerns regarding scamming, being tricked or taken advantage of. Confident users were also concerned about privacy, and were more likely to discuss issues about how their personal information is being used by companies.

When asked directly about online privacy about two-thirds (67%) of respondents expressed some degree of concern while non-internet users and low confidence users expressed even greater concern.

[1] Ofcom (April 2016), *Adults' media use and attitudes*, p. 8

Financial transactions such as banking, paying bills, and buying and selling online (especially when giving out their credit and debit card details) cause the most unease to consumers over the use of their personal information.

Issues of Trust

The research strongly indicates that pre-existing trust in an organisation seems to be used as a short-hand for determining whether or not to share personal information with organisations online – especially given that people feel they have little control over what happens to their information once they have handed it over.

Three factors are key to building trust:

Being open and transparent about what data is being collected: Most people felt that they can only find out what happens to their personal information if they are prepared to do some digging on a company's website. This reinforced a general belief that consumers are not being put first. Even the most confident internet users had issues with reading Terms and Conditions and cookie policies.

Providing the consumer with the opportunity to opt-out of any use of their data: Internet users felt that "opt outs" could be as confusing as Terms and Conditions; for example, it was not always clear whether a box should be ticked or unticked to opt out of receiving marketing information, and the full extent of what an opt out really means was unclear to some.

Organisations should keep consumers' information secure: Consumers are not just concerned about protecting their own devices from hackers, but also worry about their data being protected once it is in the possession of companies. For some consumers, concerns have been heightened by newspaper coverage about sensitive data being lost or stolen.

Despite financial transactions causing people the most worry on the internet, banks are the organisations most trusted to deal with consumers' personal information. The in-depth interviews show this may be because they are seen as experienced in dealing with sensitive information as well as having an established reputation to protect. Government and public services are the next most trusted, while social media networks and online marketplaces are the least trusted. Charities are viewed with some suspicion - with concerns about personal information being shared between different charities.

Trust in an organisation is particularly important given that consumers say they are more willing to share personal information with organisations they know and trust. On balance, people would also like more information about how their personal information is used. There is little sign that Government and public services are viewed any more positively than private companies.

Consumer control over personal information

High levels of concern over privacy are matched by a feeling of a lack of control – seven in ten people say they do not have much control over what happens to their personal information online. The in-depth interviews suggest that the only real control some feel they have is to choose whether or not to enter information or visit a website in the first place; once data is in the hands of a company or online organisation, users feel they have lost control.

Online security software is the most popular coping mechanism for consumers to protect themselves online, used by around three-quarters (74%) of internet users. Those more confident using the internet are more likely to have security software than those who are less confident, lack of knowledge being the main barrier for those who do not have this protection.

Most people also say they often opt out of receiving marketing materials. Just over half say they often check the website they are visiting is secure, or change privacy settings on social media accounts; however only a minority say they regularly read Terms and Conditions, change browser settings to delete cookies or use a private browsing mode. The in-depth interviews showed some people recognised that security software is only part of the solution, as their concerns about privacy extended to what happens to their personal data after they have handed it over to a company.

Overall consumers are split on whether or not they feel they are doing enough to protect themselves online (29% say they are, compared with 27% who say a lot more needs to be done), but there is clearly a feeling that companies, Internet Service Providers (ISPs) and the Government have a responsibility to do more. About half of users (and more among older and less confident internet users) feel these bodies should do more to protect people's personal information.

The benefit exchange and behaviours

Consumer attitudes towards personal information, and trust in how it is used, may be related to perceptions of companies' motives for collecting it in the first place. While there is a broad awareness that a great deal of personal information is collected online (87% believe that companies store a great deal or a fair amount of personal information about them), knowledge of the details is mixed, especially between confident and less confident internet users. Confident users tend to be more aware of the various methods that companies use to collect information, while less confident users are more unclear of what is done with their data - with some completely unaware that their data had a digital footprint.

People tend to assume companies collect personal information for the company's benefit instead of the consumer's, for example, thinking it is done to send more marketing materials or to sell on to other companies rather than improve customer service or develop new products. The qualitative interviews suggest that while some accept companies can use personal information for some internal purposes, there was still an underlying suspicion – especially of companies selling personal information on to third parties.

There is also evidence of contradictions between consumer attitudes towards online privacy and their actual behaviours. For example, many people say they are not willing to provide their personal information in exchange for free access to a website (some saying under any circumstances), but this does not seem compatible with the reality of the way in which the internet works. This may reflect a lack of knowledge of the ways personal information is actually collected online, or it may be an expression of concern over a risk that some feel they cannot avoid if they want to use the internet in the way to which they have become accustomed. Similarly, although most say they are unwilling to provide personal information in exchange for free access to websites, when pressed in the in-depth interviews most say they would actually rather not have to pay.

This report is intended to inform policymakers and the wider public about consumer perceptions of online security. Consumers show that they are aware that much of that responsibility lies with the consumer but feel that companies and other organisations must do more to earn public trust. This includes companies being transparent and educating consumers about what they do with people's personal information.

1 Background context

1.1 Objectives

This research was carried out by Ipsos MORI on behalf of the Communications Consumer Panel. The Communications Consumer Panel works to protect and promote people's interests in the communications sector. As an independent body, it carries out research, provides advice and encourages industry stakeholders to keep consumers, citizens and micro businesses at the centre of their thinking.

In 2011 the Panel carried out research into consumer attitudes towards online privacy and given the importance of this issue has decided to carry out further research into this topic in 2016 to provide a snapshot of things for consumers as they currently stand. The objectives of the 2016 research are to better understand the following:

- the extent to which people are aware of the various methods of collecting data in the online environment;
- the extent to which people are prepared to share their own data and what benefits they expect in return;
- consumer awareness of ways they can protect their online data, and their use of these methods;
- people's understanding of online terms and conditions and the nature of the consent they are giving online;
- expectations of how companies hold and treat their data;
- attitudes towards what is currently being done to protect personal online data;
- awareness, understanding and use of 'smart' products and 'the internet of things'.

1.2 Methodology

A representative survey of 1,423 adults aged 15 and over across the United Kingdom was conducted face-to-face on Ipsos MORI's Capibus survey. Interviewing was conducted between 19 February 2016 and 23 March 2016.

Capibus uses a controlled form of random location sampling (known as 'random locale') to ensure that the sample drawn each week is closely matched to the UK population it covers. This approach involves the weekly random stratified selection of between 170 and 190 primary sampling units (PSUs -

aggregated from UK Census Output Areas), with quota interviewing based on age, gender and working status within the randomly selected PSUs to match the geodemographic make-up of each one selected.

The sample size was 'boosted' to at least 100 respondents in nations which otherwise would have contained fewer than 100 respondents (in a purely random representative sample), to allow reliable analysis by nation. This includes 176 interviews in Scotland and 150 interviews in Wales and Northern Ireland. A boost was also included to achieve 200 interviews of those aged 75+. Down-weighting was then used to ensure that the final sample remained representative of the overall population.

Weighting was also used to correct for minor differences between the final sample profile and the population profile. Weighting is applied to surveys as standard and adjusts the data to account for potential differences between the demographic profile of all members of the public and those who are surveyed.

We report differences between subgroups (e.g. age, gender, nation, internet confidence) only when they are significantly different to the total sample. We have reported differences at the 95% confidence level; meaning if we repeated the survey 100 times we would expect the results to fall in to the confidence range 95 times.

In addition to the quantitative survey, qualitative in-depth interviews were also conducted. This allowed the research team to explore some of the issues in greater depth and to add context and understanding to the quantitative data. Quotas of respondents were based on internet use frequency, age, nation and whether or not they had a disability. Interviewees were recruited from the quantitative survey with the exception of two interviews who were recruited in public places using qualitative recruitment specialists. In total 21 interviews were conducted (10 by telephone and 11 face-to-face).[2]

While qualitative research was an integral part of this study, it is important to bear in mind that qualitative research is based on very small samples, and is designed to be illustrative rather than to produce statistics. This should be taken into account when interpreting the research findings. It is also important to remember that the research deals with perceptions rather than facts (though perceptions are facts to those that hold them).

Throughout this report, the findings from the qualitative research are woven into the text and we have made use of verbatim comments to expand upon and provide further insight into the quantitative findings.

[2] In some instances, quotes within this report may slightly differ when comparing word-for-word with those shown in the series of video clips produced for this project. This is because respondents were occasionally asked to repeat their statements while filming to achieve more than one workable clip for editing purposes.

1.3 Literature Review

Desk research was carried out with the purpose of informing the design of research materials and to ensure researchers were well versed in relevant literature. In this review we discuss some of the existing research surrounding online data protection and privacy. Key themes from the relevant literature include the disparity between technological literacy and awareness of how personal data is used, contradictory behaviour around how people safeguard their personal data, and a brief contextual overview of the changing market environment surrounding internet use.

Awareness and use of personal data

Most people understand that personal information is collected, stored, and used by public and private sector organisations, however a lower proportion are aware of how such technologies work or how their personal data is used. This also holds true for the public sector where 45% think it is using people's personal data in a beneficial way for the organisation. Furthermore, regardless of the extent to which regulations around personal data and privacy are clear cut from a legal perspective, this same clarity does not exist within the minds of consumers (WIK-Consult 2015). On the whole, consumers are largely unaware of how organisations are using personal data and for the most part do not understand privacy policies (Catapult Digital 2015) (Office of Fair Trading 2013).

The literature indicates that, as internet use and the adoption of new platforms continues to grow, the overall levels of concern about the commercial use of personal data remains consistently high. In a study by the European Commission (2011) 80% of European respondents said they are concerned that companies holding personal information may sometimes use it for a purpose other than that for which it was collected, without informing the individuals concerned. A study for the Office of Fair Trading (2013) showed that 79% of UK consumers were concerned about their personal data being sold to third parties, and Catapult Digital (2015) found that 80% were of the assumption that companies use the personal data that they gather for economic gain.

Some are in favour of government implementing sanctions against companies which misuse or lose citizens' personal data. The Eurobarometer Flash Survey 359 found that half of all Europeans say that a fine should be imposed on any such company, followed by four in ten saying the company should be banned from using personal data or compensate the victim. Ipsos MORI research (2014) into consumers' willingness to share information with preferred brands and organisations found 71% still remain concerned about how companies are using that personal data.

Nonetheless, consumers do not necessarily oppose companies using their data for internal business development or improving services. The majority of consumers (68%) are happy to provide personal information online to companies in order to obtain something they want (Ofcom 2015). An Annenberg School for Communication report (2015) found that the more one knows about the commercial usage of personal data the more likely one is to give up personal data in exchange for benefits. However, research by Ipsos MORI (2014) found that three in five consumers would rather keep online activity private, even at the cost of missing out on personalised services and more relevant recommendations. This paradox highlights a need for further exploration into public understanding and attitudes towards data commerce and their role in the trade and where their tolerances lie.

When it comes to data being monitored, rather than used by companies, people tend to make a distinction between crime and terrorism in relation to surveillance technologies. Ipsos MORI/KCL found that roughly four in ten said it would be completely unacceptable for the government to monitor personal data without consent in order to combat crime. However, the same report finds that while they are just as likely to rule out monitoring their own communications to fight terrorism, only 18% see it as completely unacceptable to monitor other people.

Having access to different technologies and platforms also plays a role in influencing how people get online. There is a sense amongst consumers that data tracking is an inevitable part of life. In the 2013 Global Trends Survey by Ipsos MORI, 77% of respondents thought that it is inevitable that new technology will lead to the loss of some levels of privacy in the future. Furthermore, a study from the Annenberg School for Communication shows that as consumers acclimatise to the new online environment the more likely it is they will share personal data online. Interestingly, there are different levels of trust depending on the technology in question. People are more likely to trust smartphone apps when compared to online browsing and pay little attention to user policies when downloading apps. The app environment is generally regarded as safer than that of browser based internet access, with users paying little, if any, attention to permission requests when downloading or using apps (Kantar Media 2014).

Contradictory behaviour

The literature suggests that some common contradictions exist between people's attitudes towards data security and their behaviours in safeguarding their own data. A Communications Consumer Panel report (2011) indicates that when asked unprompted, more than half (52%) of UK internet users had no top of mind concerns when using the internet. However, more recent research by Ipsos MORI for the Royal Statistical Society (2014) shows only 8% of people with no top of mind concerns (reasons for this may partly be due to the change in the market context since 2011, discussed in the next section). Furthermore, when prompted, this study showed that the top concerns for people related to data were companies providing a poor service (72%), failing to keep personal data safe (72%), and selling anonymous data (63%).

According to Ofcom (May 2015) research, four in ten internet users felt that they are very confident they can stay safe online, with the majority using padlock icons and system messages to measure website safety. Most attempt to protect their data from serious issues such as cyberattacks or identity theft, for example Ofcom's *Adults' media use and attitudes* report found three quarters of users use antivirus software, and over half use firewalls. Yet the number of those who still use the same passwords for most or all websites has increased, as has the number of consumers experiencing a financial loss through cyberattacks. This raises questions as how best to ensure consumers are able to give informed consent on how their personal data is used, and if consumers are accepting cookie sharing because they are now more comfortable with them or if people are simply ignoring the message. Ipsos MORI's research for the National Statistical Society (2014) shows that while "easy" privacy precautions are fairly common; few people take measures that would involve a loss of service. The disparity between people's concerns and their behaviour online may highlight some misconceptions of what constitutes safe behaviour (Ipsos MORI 2013).

Consumers within the UK admit concerns for their personal data, yet often do not understand exactly what the term covers and how such data may be used. Users often misunderstand the term 'privacy policy' assuming that it is a policy that is in place to protect their privacy and as a result disclose even more personal information (WIK-Consult 2015). There exists a need to understand whether the presence of privacy policies gives rise to users sharing more personal data than they would otherwise. Most consumers do not read policy terms and conditions or actively change their web browser settings for a more secure mode, and the signing/clicking-without-reading problem is a well-documented phenomenon (WIK-consult 2015). Indeed, Ofcom research (2015) confirms that internet users increasingly say that they do not read website terms and conditions or privacy statements at all.

While the literature evidences a growing caution towards giving out information online amongst internet users of all ages, consumers are not necessarily fully against data sharing. They do want more control over their data, and to decide for themselves what is shared and not shared. Deloitte (2015) found 57% of consumers said they are more likely to use or recommend a company that lets the user decide how his/her personal data is used.

Market context

Higher numbers of people with internet connections, along with advances in internet speeds and ways to connect, mean that consumers are now gaining a great understanding of computer technology more than ever. Ofcom's *Adults' media use and attitudes* report (2016) shows that while 21% of people did not use the internet in 2011, the number dropped to just 13% in 2015. Likewise, volume of internet use per week has risen from 14.2 hours in 2010 to 21.6 hours in 2015. These changes have helped affect consumers' perceptions of how their internet use has changed, as described in Ofcom's Media Lives study (2014). In 2005, when the Panel's study began, using the internet was described as an activity in its own right. In 2014, however, people described the internet more as a facilitator to conduct tasks that were previously done in another way. This Ofcom study illustrates how users now use the internet to connect with family and friends, stay connected with work and school, and both create and consume more user generated content as an alternative to mainstream media.

However, Ofcom's study also discusses the reality that the proliferation of sources and platforms raises questions of trust. As users have more and more exposure to content online, they tend to find it more difficult to know what sources to trust, and they find confusion, inconsistencies and conflicting emotions surround the sharing of personal data online. Furthermore, high profile data breaches have become a point of contention amongst consumers, partly due to prevalent reports in the press. Instances of corporate security failures with the hacking of iCloud, TalkTalk, and Sony gained much publicity and may contribute to growing concerns over data protection.

Shifts in circumstances in how people go online and how they perceive online activities may help explain changes in how people perceive issues surrounding personal data online. This dynamic will be considered throughout this report, in particular when referencing trends from the Panel's 2011 report.

2 Consumer pen portraits

In this section we provide example pen portraits of individuals interviewed within the qualitative element of the research. They present a depiction of typical UK consumers and their perceptions of online security. These examples have been selected based on the various characteristics found within the project including those with high and low internet confidence as well as different ages.

John has low confidence when online and limits his online usage to feel safe

John is 79 years old and married. He has grown up children and ten grandchildren. He has difficulty walking long distances. He is a carer to his elderly wife, who suffers from Alzheimer's disease. His daughter helps with the caring duties. He is currently in the process of moving home to live closer to his daughter.

Internet usage / reliance

John relies on his children to install security software and give online advice. He only accesses the internet on his PC for the following reasons (out of necessity) only ever using trusted brand sites:

- Online grocery and household shopping on trusted sites, such as Sainsbury's, Wiltshire Foods and Amazon.
- Emails from family and friends (this is his main link to the outside world).
- Online banking, so he doesn't have to visit a branch.
- House-hunting online so he doesn't have to visit many houses.
- Facebook. He is a passive user, mainly using it to see photos his grandchildren post whilst on their travels.

He limits his online usage because of security concerns. He is worried that someone can hack into his PC and steal his bank details.

Security & privacy: knowledge

John has some awareness that companies somehow obtain his information when junk mail / marketing messages are received. He feels quite safe due to the software he has but mainly because his method of control is just to visit trusted brand sites only.

John has no knowledge of cookies and how they work. He is concerned, but not overly surprised to learn about this. He is more concerned about companies sharing information. John believes cookies deliberately lack transparency, so that fewer people disallow them.

He strongly believes that more transparency is needed so consumers can have more control. He trusts banks and believes they never share info of any kind. He often opts-out of marketing simply to avoid being overloaded with 'junk mail'.

Benefit & value exchange

He is likely to exchange superficial information, such as age, location, and search history, for free usage of websites, but is less willing to allow companies to share information with others. He finds this more concerning.

"I don't know what Cookies do...I just get rid of them."

"I only go to trusted places (brand sites)."

Protecting personal info

John believes that firewalls and anti-virus software is essential for security. He believes the responsibility lies with the consumer.

However, more transparency is needed to make an active choice rather than be 'tricked' into disclosing personal information in this way (cookies). He argues that a government regulatory body should be pushing for greater transparency.

"I can tell it is happening.... when it all (junk mail) comes through the door."

SMART technology

He has a SMART meter, and no awareness of any info being disclosed or shared other than his provider reading his meter and billing him. Anything above and beyond this has not been made clear to him.

"It's the job of the government...to do something about it (the perceived lack of transparency)."

"(My bank) wouldn't do that (share information) ... they aren't allowed to do that..."

KEY TAKEOUTS: Heavy reliance on others to install security software and to direct him to trusted sites. No awareness of cookies exchanging information. Would be likely to exchange superficial information for free website usage. Is unlikely to agree to companies sharing info with others and is concerned about this.

Internet savvy Rick has concerns about privacy and the storage of his data

Rick is in his 40s, married with young children and lives in Wales. He works in IT, and as such is very internet savvy and confident online. He spends most of each day online using several devices.

Internet usage / reliance

Rick uses the internet every day for work, information searches, banking, shopping, and recreation. He spends a large proportion of his time online when at work, home and whilst travelling. He has lots of online devices including a smart phone, laptop, PC and iPad.

"I don't trust Facebook…. I have more trust for sites such as the BBC."

Security & privacy knowledge

Rick knows he has to have sophisticated software and he installs this himself for security and privacy.

He's fairly comfortable with sharing his information with companies he chooses. He sometimes allows cookies if he sees a clear benefit to himself, for example, the BBC website so they can tailor information to be more relevant to him.

He is aware of cookies and that companies might share his information. He is less comfortable with this. He often clears his cookie track history to feel in control of what is shared and when.

He will also opt-out of marketing info to control the amount that he receives (when the company or product has less relevance).

Ultimately he believes the responsibility for security and privacy is with the user / consumer.

"Initially it has to be yourself (who has responsibility) …. have to be mindful of what you're giving away and who to."

Benefit & value exchange

He is less comfortable with companies sharing information. This is where he feels his control is handed over. He thinks this is not transparent enough. He doesn't always read the "small print" or Terms & Conditions.

With free services he believes the companies benefit more from the information they take.

He claims he sometimes will opt-out of subscribing if too intrusive and too much info is asked for. He has also given false information in the past. Rick's main concern is how companies store his data, and how secure this is.

"Amazon probably have more data on you than anyone else."

Protecting personal info

He claims he has very sophisticated software to help with security.

He allows certain companies such as his broadband provider and bank to take his information and market relevant info to him, He believes social media and other sites, just sell info to anyone. He disallows his cookies for social media. He believes there are lots of companies trading off these platforms. He doesn't think cookies are transparent in how they work and use personal data. He considers himself to be aware of this only because he works in IT. He worries about the amount of people who don't know about cookies.

"Cookies don't make it clear what they are obtaining from you or how they store the data."

SMART technology

He has a SMART meter, and has a lot of trust in its use. He has not considered how the information might be used beyond billing and has no concerns about this, when this was raised with him.

KEY TAKEOUTS: Internet savvy user who seems more concerned about privacy, and the storage of his data, particularly when information is shared with other companies. He believes that more regulation of companies sharing and storing information is needed. In addition, he argues that the public need to be educated about this.

Trust in his bank and other brands is how Alan feels secure online

Alan is 59, married with grown up children and grandchildren. He works fulltime as an outdoor market supervisor. His wife has a similar post on a part-time basis. They have a dog and a cat. He collects coins and builds model helicopters.

Internet usage / reliance

Alan has a PC and a tablet in his living room. His wife prefers using a laptop. They both access the internet daily for the following reasons:

- Social media to keep in touch with friends.
- Research, e.g. about his model building.
- Shop and browse online retailer sites for items that are difficult to find on the high street such as coins that he collects.
- He occasionally looks at the BBC news website.
- Browse holidays online too, but prefers to book through an agent, in person.
- Banks online

He is reluctant to download anything such as games or movies, as he has a fear of getting a virus.

"Bit of a minefield to me (downloading games and movies)."

Security & privacy knowledge

He tends to opt-out of receiving marketing where that option is provided and trusts the brands he deals with to honour that.

He has noticed that companies seem to share information, but is a bit unsure as to when and how they do this. He notices targeted material after visiting certain sites, he has often wondered how this happens.

He doesn't read T&Cs, but trusts that they are all similar between companies. He believes the companies have these to primarily protect themselves.

Once he learns about cookies he seems annoyed that he did not know about them. Although he has seen cookies warnings pop up on his screen he has dismissed them and not given them much thought.

"Pages and pages of terms and conditions and it (a problem you have) can be disguised within it. They are there to protect the company."

Benefit & value exchange

More personalised marketing messages is a clear benefit, you can see more of what you like and less of what is not relevant. On the other hand, he is afraid of receiving large quantities of junk mail online and via the post.

If websites were to charge him to visit their site, he would be less likely to visit them. He would be prepared to exchange certain information, such as age, location, how many times visited the site, for free use, but believes permission should be granted in a transparent way first.

If he pays to visit a site, he would feel a little safer. But he would be put off visiting a site if he had to pay.

"I won't go to a site I don't know...only go to Thomson's... big names."

"I never download stuff except for bills."

SMART technology

He also has a SMART meter and no awareness of any info being disclosed or shared other than his provider reading his meter and billing him.

KEY TAKEOUTS: No knowledge of cookies. Some uncertainty as to whether he has adequate software to protect his security and privacy. Likely to exchange superficial information for free website usage, but is concerned at the lack of transparency. Is concerned at the idea of companies sharing info with others.

Agnes does not use the internet, but would like to learn how to Skype

Agnes is 71 years old and is married with grown up children and grandchildren. She owns a laptop and has tried to learn how to use it in the past, but it has been a struggle. She does not feel that the internet is a necessity for her, but she would like to learn how to Skype with family in Australia.

Internet usage / reliance

Agnes is not confident at all at using a computer, and thus is her main barrier to using the internet.

She has tried to learn how to use a computer in the past, ranging from family members helping to adult learning courses. However, she has struggled, and now does not think she will ever become competent at using the internet.

She feels that she is missing out on being able to communicate with family in Australia over Skype, and she feels that if she managed to learn how to do that it might encourage her to learn more computer skills.

"You don't have person to person contact."

"I need something that's easy. That I can remember."

Security & privacy knowledge

As well as her low capability, she is worried about getting scammed into things. She does not trust the internet generally.

"A lot of the internet is rubbish - people can be convinced to buy a lot of rubbish. It makes it too easy to buy on impulse."

"If you make a mistake on the internet, you can't get it back… I think I'm too slow."

Benefit & value exchange

Although she could not comment on the internet specifically, she knows that companies do sell information on. It annoys her because she ends up getting the end result in the letter box and she becomes inundated.

"My husband and I are dinosaurs. I'm not confident at all. I don't use it (the internet). The internet is in a box and it stays there."

Protecting personal info

She does not believe that her personal information would be of any value to anyone. Because of this, she does not see safeguarding her personal information as a priority. Someone taking or mishandling her information is not a high risk.

Rather, she sees her low capability as the biggest risk to her on the internet. She believes this could lead to her buying something she does not want to buy.

"I'm afraid to use the internet. Someone more cleverer than me could take advantage...."

"My son and daughter-in-law are in Australia, the other children talk to them over the internet. That would be nice."

SMART technology

She does not have SMART products and does not understand how they might work.

KEY TAKEOUTS: She is frustrated with computers and the internet from past struggles with learning IT skills. Although she says that she has given up with computers, learning how to Skype with family might encourage her to do more. She is not concerned about the use of her personal information, and instead sees her lack of competency as the main risk to her on the internet.

Richard is a frequent internet user and is not very concerned about his privacy

Richard is 25 years old and a part-time factory worker from Glasgow. He goes online multiple times every day and is very comfortable using a wide range of devices to connect to the internet. While he is confident in using the internet, his technical knowledge around privacy and security is limited.

Internet usage / reliance

Richard uses the internet every day for social media, to search for information, use mapping applications, internet banking and instant messaging. The internet plays a part in his every day routines.

He uses a lot of different online devices to connect to the internet, namely his tablet, phone, laptop and games console. If he was at home he would usually connect using his home Wi-Fi, and if he was on the move he would use his mobile network.

"As a company I would probably want people's personal information so I can go back to them and see what they're looking at. It's all about sales."

Security & privacy knowledge

He has received marketing information from websites in the past, and would not know how to opt-out of receiving such emails.

He has not noticed the use of cookies notifications before and he does not recall reading them. He does not understand what a cookie is, describing them as a bookmark, and sees them as a utility for users rather than for websites.

He does not read Terms and Conditions as they are too long and technical. However, it does concern him when he signs up to something and he has to agree to them, particularly when it has something to do with money.

He feels that companies are generally not open about how they use your personal information.

"I would hope that the government is monitoring how these companies use your data."

"Depending on the website, if I really was concerned about it I would look into it. But it's hard, websites don't give away much."

Benefit & value exchange

He struggles to see how there would be any benefit for him. He just sees it as benefiting companies by increasing revenue. He doesn't mind this as long as they do not harass him.

He is aware of companies sharing information with other companies, but he says that he does not really understand it.

He likes the idea of companies using personal information to improve customer service. If it helps the consumer, then it is a good thing.

"(Having a lack of information) doesn't stop me. I'm a chancer. I'll risk it."

"Websites don't tell you what they're doing, they just do it. They don't have a notice telling you they're sharing your information."

Protecting personal info

He feels like he does not have control over his personal information on the internet, 90% of the time he does not think about it and it does not affect what he does.

He thinks that the government should be responsible for monitoring how companies are using your personal information.

He trusts that ISPs play a role in protecting people's personal data, basing this on the fact that they are established brands.

He struggles to see what he might do to better protect his personal information, and does not see it as his responsibility, rather it is the responsibility of organisations that he provides his information to.

SMART technology

He does not have strong opinions on SMART products. He thinks they are a good idea, and while he doesn't own any, he would like to. He can't think of any risks that may be associated with them.

KEY TAKEOUTS: Although he is a frequent internet user his level of technical knowledge is quite low such as no awareness of cookies exchanging information. He would be likely to exchange information without putting much thought into it. However, when risks surrounding information sharing are presented to him he does become concerned. Although he admits that this concern would not be enough to limit his internet use.

Sarah likes websites that give her a more personalised service

Sarah is a 38-year-old HR manager and is married with children. She is a frequent internet user. She accesses the internet for a number of reasons and gets online using her phone and tablet. She believes that the ultimate responsibility for protecting data falls on the individual.

Internet usage / reliance

Sarah mostly logs onto the internet on her phone, and uses it for accessing social media, online banking, online shopping and generally looking things up. She also sometimes uses a tablet for streaming video as it has a larger screen size. She worries about cyber bullying and the safety of her information online, but these do not affect her overall internet usage.

> *"In the past, if I wanted to find something out I would have had to go the library, now I just think 'oh I'll Wikipedia that'. It's information that is accessible within seconds."*

Security & privacy knowledge

She relies on brand reputation and the advice of security software when deciding what websites to trust. Sarah sees larger companies that she has built a relationship with as having more to lose by mishandling her information or selling on to third parties.

She is pleased that internet companies are now asking her to opt-in, whereas previously she remembers having to find ways to opt-out. She would give companies consent to use her data in return for receiving deals and vouchers for products, for example baby club vouchers.

> *"History of the companies and how long they've been around (referring to trusting websites). If they were abusing that information, then they would have been slammed for it."*

Benefit & value exchange

To Sarah the main benefit in giving her data to companies is that it allows them to tailor communications and advertising to the individual consumer. In her view, this benefits consumers as they receive offers that are relevant to them, and it benefits companies in that they can target their products to those who want them.

Protecting personal info

Sarah believes that the government should play a limited role in protecting people's personal info, and worries about the implications of too much government monitoring. Instead, she sees the onus as being on the individual to make decisions on keeping their data safe. However, she thinks that there is limited awareness about how people can keep their data safe, and there should be an effort to raise this awareness.

> *"Because I've never had my personal information abused then I'm probably not as cautious as I might be. Unless it's happened to you, you probably don't really."*

> *"If you're going to be a responsible retailer, when people are buying things like tablets etc. a leaflet could be provided... that goes through the main risks of internet security and tips to stay safe online."*

SMART technology

She was sent a SMART product but does not use it and has never connected it to the internet. She sees a danger with SMART products in that people could hack in to them and know when you're not at home – putting you more at risk of burglary.

KEY TAKEOUTS: Frequent user who is aware of the risks of using the internet, and relies on brand relationships and security software to manage those risks. While she thinks the government should help to raise awareness amongst internet users, she does not see the government as having a direct role in protecting people's data.

Janice has only been using the internet for the last two years

Janice is 75, married and retired, and lives in North Yorkshire. She doesn't use the internet for many activities, but communicating with friends going around the world is one of them.

Internet usage / reliance

Janice has only been using the internet for the last two years after one of her friends 'hassled' her. She generally uses the internet to do email, crossword puzzles and goes onto to shopping sites to compare prices. However, she sees social networking sites as dangerous, due to the possibility of hacking and bullying. She finds not being able to use the internet quickly frustrating, and says she still prefers to do some things face-to-face.

"I had a friend who was travelling around the world and I learned email so that I could keep in touch with her."

Security & privacy knowledge

She thinks that companies aren't open with what they do or how they get people's data, and she bases this on what she reads or sees in the news. However, in regards to her personal data, she doesn't use the internet enough to get into a situation where she would be asked to opt-in or out of something.

She does not understand what cookies are, but once explained to her she said that something like that would bother her. She understands companies want information for marketing and perhaps stock control, but as she shops in person she does not see how this applies to her.

"There's no benefit for me as I like to go to the shop in person, but there might be some benefits to some others who want to learn about new products."

Benefit & value exchange

Janice is uncomfortable with all forms of data usage except improving customer services. She sees it as an invasion of privacy and would not like companies holding her data for any other reason.

However, she does think that if companies are holding personal data in order to improve customer service, then this may be an acceptable reason for holding personal data.

"If the Pentagon could get hacked anybody can be hacked."

Protecting personal info

Janice believes that she has control as long as she does not provide personal information, but if she was to provide information, she would immediately be giving up control. She sees the choice as binary, and believes that even the government cannot protect your personal information once it has been released on the internet to companies.

Although she conceded that she could learn more, as her internet usage is low, she believes that she knows enough for what she wants to do online, and has no interest in learning more.

"No I don't have control; nobody has total control. If you put your data into a website, you have no more control over it. I don't ever enter my information to try and have some control."

Smart technology

Although she and her husband have a SMART meter Janice is reluctant to believe the product was designed to save the customer money but rather it makes the energy company run more efficiently thus saving them money.

KEY TAKEOUTS: She has a low level of technical knowledge and no awareness of cookies exchanging information. She feels however that she doesn't use the internet enough to get into compromising situations regarding sharing data. Despite this she feels that companies holding any data about consumers is a breach of privacy and is adamantly against it.

3 General Attitudes to Online Privacy

This report investigates perceptions of online security and the usage of personal data online through both a large-scale quantitative survey and 21 qualitative in-depth interviews. The findings from this report provide a glimpse into consumer perceptions as they stand in 2016. This section highlights people's general attitudes to going online, matters of privacy and who they trust most with their personal information. It finds that although privacy is a top of mind concern when going online, younger people are less likely to be concerned about privacy than older people. Banks are considered to be the most trusted organisations when it comes to holding peoples' personal data even though financial data transactions themselves are of most concern to people. When consumers are asked what constitutes "trust" the three priorities mentioned were: being fully open about what data a company collects and uses, providing the consumer the opportunity to opt-out of any use of their data, and keeping consumers' information secure. These are all important factors around trust, and are reoccurring themes throughout the report.

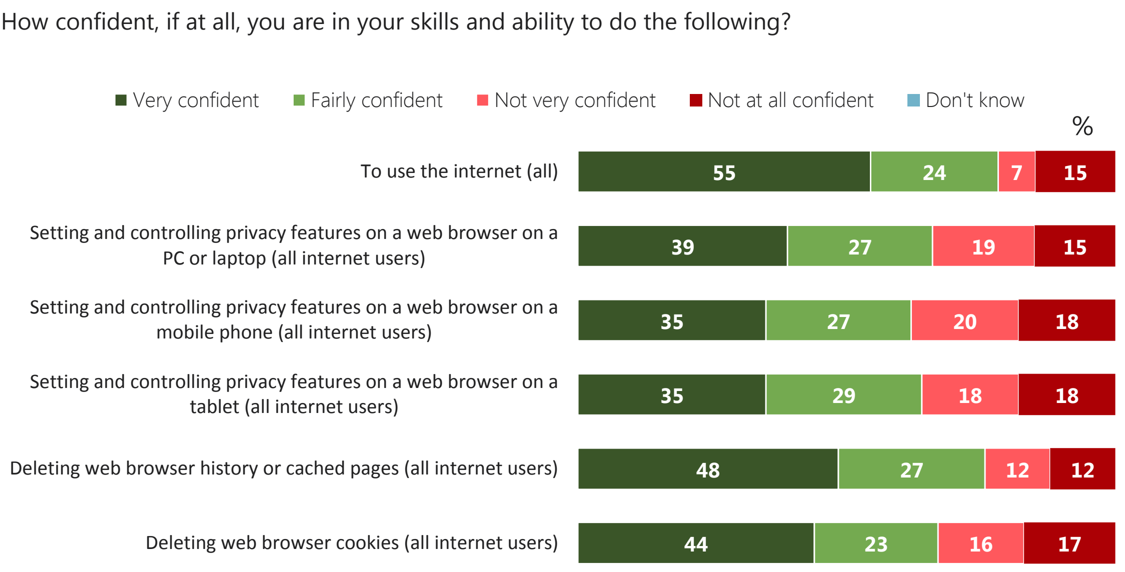
3.1 Levels of confidence using the internet

Eight in ten consumers feel confident using the internet, including nearly all frequent internet users. Most are also confident setting privacy features, but to a lesser extent – around one in three say they are not confident doing this. There are though signs of a 'digital divide', with one in five overall saying they lack confidence in using the internet. The difference between the views of high and low confident users is a common theme throughout this research, so it is important to understand the two groups – low confidence users in particular tend to be older, and much more restricted in their internet use (both in terms of the devices they use and the activities they use it for).

Overall a majority of consumers said that they were confident when it comes to using the internet. More than half (55%) said they were 'very confident' while a further one in four (24%) said that they were fairly confident. However, around one in five (22%) said that they were 'not very' or 'not at all confident'.

Regarding the ability to protect themselves online three in four (75%) internet users say they have confidence in their ability to delete their browser history (24% are not confident), a smaller number say they have confidence in using the privacy features on their laptop or PC (66% are confident and 34% are not), and even fewer have confidence in using the security settings on other devices such as mobile phones and tablets. When it comes to deleting web browser cookies, two in three (67%) said that they are very or fairly confident while one in three (33%) say they are not very or not at all confident.

Figure 3.1: Confidence in internet usage?



Base: All 1,423 adults; Internet users 1,155adults

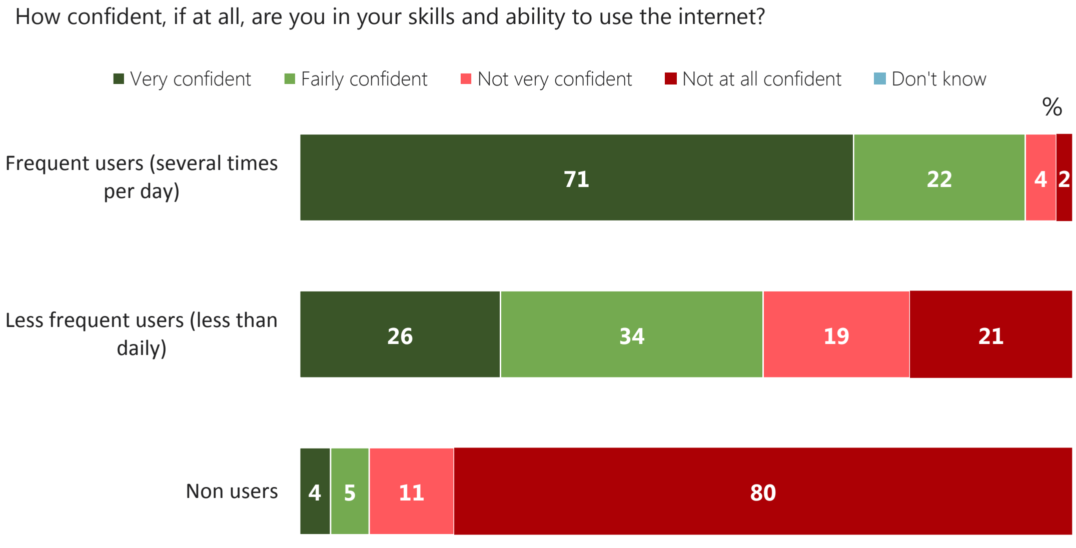
Sub group analysis reveals there is a high degree of correlation between age and confidence in using the internet. For example, 96% of those aged 15-24 and 94% aged 25-34 said they are confident in using the internet, compared with 56% who were between 65-74 years of age and just three in ten (30%) of those aged 75+. Four in five (80%) of 15-24 year olds were confident in their ability to use the security features on their web browser, compared with 47% of 65-74 year olds and 26% of those aged 75+.

Men are also more likely than women to say they are confident in using the internet. 82% of men say they are confident using the internet (18% are not confident) compared with three quarters of women (24% are not confident).

Fewer people with a disability claimed to have confidence in using the internet than those who have no disability (63% compared to 83%) and there is some evidence that this may not be solely age related. When comparing those with a disability and aged 55+ with those without a disability within the same age group, three in five (61%) without a disability had confidence using the internet compared with 48% of those with a disability.

Internet confidence is also found to be highly correlated with frequency of internet use. 93% of those who access the internet several times a day said they are either very or fairly confident in using the internet. This compares to three in five (60%) of those who access the internet less than daily and just 9% of those who never access the internet at all.

Figure 3.2: Confidence in using the internet versus online frequency



Base: Several times per day 883; Less than daily 124; non-users 268

The qualitative findings shed some light into the relationship between internet confidence and usage. Those who used the internet more frequently were more likely to do multiple tasks online ranging from recreational use to online banking and shopping – often these people struggled to name everything as their activity list was so long.

> *"I like to do as much of my shopping as I can online, although I do like to go to the shop for fresh produce" (Female, 35-44, London, high confidence internet user)*

Less frequent users however tended to conduct a smaller range of activities and their confidence in ability to use the internet seemed to be the biggest barrier to doing more activities.

> *"I use the internet to do just the things I want, and I'm very comfortable only doing things within these limits" (Female, 75+, Yorkshire and Humberside, low confidence internet user)*

> *"I saw my daughter using the internet to listen to music and I thought I'll give that a go, but I don't want to do anything else" (Female, 45-54, Northern Ireland, low confidence internet user)*

Overall the level of confidence in using the internet is a useful variable for analysis due to the differences between these groups in terms of demographics and attitudes towards internet privacy and security. Table 3.1 provides a number of the key differences between high and low internet confidence users found throughout this report.

Table 3.1: Profile of high confidence and low confidence internet users

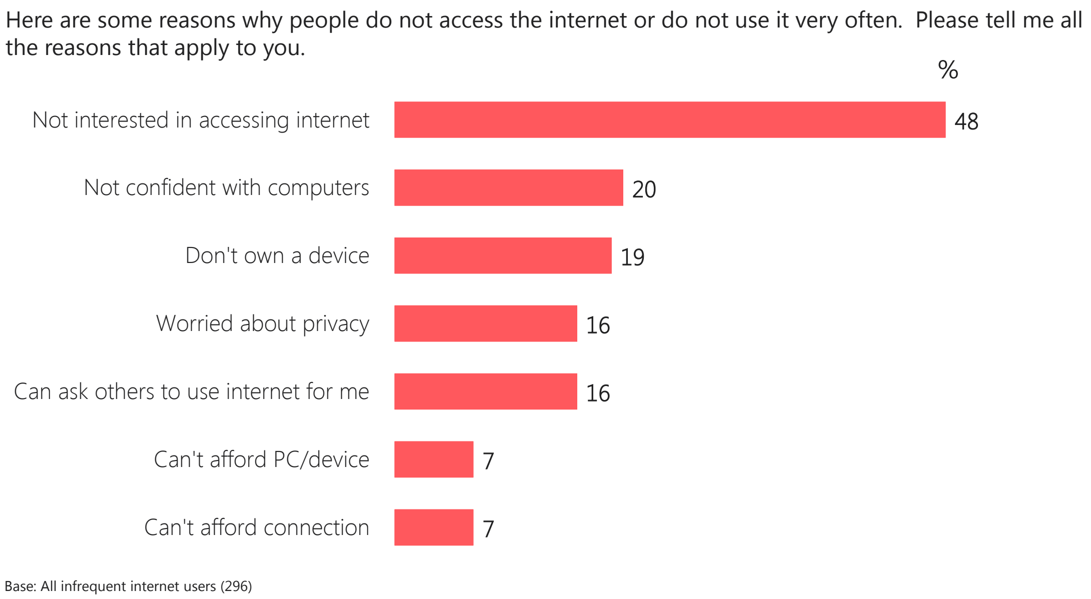
High confidence internet users	Low confidence internet users
• Tend to be younger (95% of 15-34 year olds vs. 33% of 65+)	• Tend to be older (45% of 65+ vs. 4% of 15-34 year olds)
• More likely to be male (82% of males vs. 75% of females)	• More likely to be female (24% of females vs. 18% of males)
• Tend to be more frequent internet users (93% of those who use the internet several times per day vs. 60% who use less than daily)	• Tend to use the internet less frequently (40% who use the internet less than daily vs. 7% who use it several times per day)
• Connect via multiple devices, including smartphones	• Connect via a single device, usually a laptop or tablet
• Activities are woven into daily life - e.g. shopping, banking, social media, communicating, and other recreational purposes	• Are focused on a small range of few activities, mainly recreational purposes and communicating.
• Are more familiar with security features and behaviours (83% use some sort of security software compared with 71% of those with low confidence)	• Main barrier is lack of confidence to do more as opposed to privacy concerns – although privacy is a barrier when sensitive information involved, such as banking
• Are more aware of concerns around personal information/how it is used for commercial purposes, even if they don't act on them	• Have particular concerns about scamming/being taken advantage of

3.2 Why some individuals do not access the internet

Confidence using computers is one of the largest barriers for individuals when it comes to accessing the internet. Despite having lower levels of confidence many also say they have no interest in learning more about it.

While online privacy is a concern among non-internet users this does not appear to be the largest barrier preventing them from using the internet. Reasons for non-usage are more often related to a lack of interest. When asked why they did not access the internet, half of non-users (48%) said they were simply not interested, one in five (20%) said it was because they were not confident with computers. One-in-six (16%) mentioned privacy as a reason they did not access the internet.

Figure 3.3: Reasons non-internet users do not access the internet



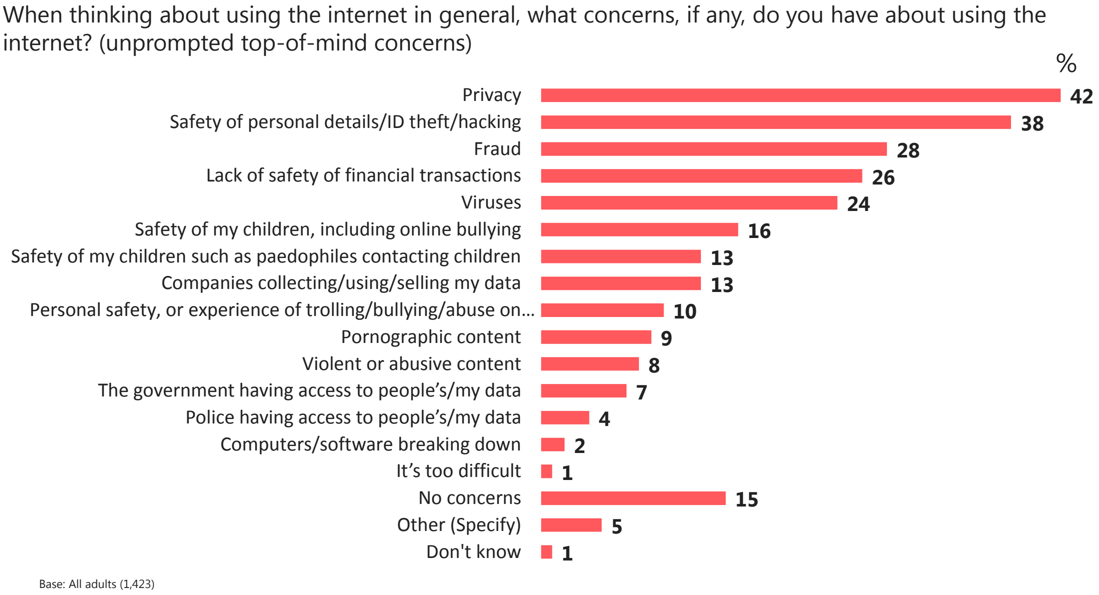
3.3 Concerns when using the internet

Privacy and safety of personal details are the top two spontaneous concerns that people have about using the internet, for both high and low confident users. As noted in the literature review, the market context has changed significantly in recent years, in the extent and ways in which people use the internet. This is reflected in the in-depth interviews with frequent users in particular demonstrating they are aware that there are risks to their personal information online (even if precise knowledge of the details could be better, as shown in later findings).

In the survey, respondents were asked what top-of-mind concerns they had when using the internet.[3] More than two in five (42%) said privacy was a concern followed by 38% mentioning safety of personal details (including identity theft and hacking), 28% saying fraud, 26% saying lack of safety around financial transactions and one in four (24%) saying viruses. 15% said they had no concerns at all.

[3] Responses were not read out to respondents.

Figure 3.4: Top-of-mind concerns when using the internet



When exploring sub groups, older individuals appear more concerned about the safety of personal details than those who are younger. Almost half (45%) of those aged 55-74 mentioned safety of personal details as a concern compared with 38% of those aged 15-24 and three in ten (30%) of those aged 25-34.

While privacy was of equal high concern in England (43%), Northern Ireland (43%) and Wales (40%), it was of lower concern in Scotland where one in three (33%) mentioned it. People in Scotland showed more concern when it came to the safety of their personal details with 41% saying this was of concern. People from Wales however were the least likely nation to mention safety of their personal details with one in four (25%) stating this (compared with 45% in Northern Ireland and 38% in England).

When looking at confident internet users, privacy and safety of personal details shared a similar level of concern amongst this group (42% and 39% respectively). Non confident users, on the other hand, consider privacy as a greater concern than safety of personal details. Two in five (41%) of those not confident in using the internet said privacy was a concern, while only 28% said safety of personal details. Concerns were also higher among more frequent users than less frequent. For example, three in ten (30%) who use the internet less than once a day were concerned about personal safety/ID theft, compared to four in ten (39%) who use the internet several times a day. Concern over viruses also changed with internet use, with 15% of infrequent users mentioning viruses, compared to 25% of frequent users. These differences may be explained by better familiarisation that is associated with higher levels of internet confidence and more frequent internet usage.

The 2011 Panel report found lower levels of concern relating to privacy (mentioned by 14% of respondents), and safety of personal details/ID theft (mentioned by 26%). Just over half (52%) of respondents in 2011 had no top of mind concerns at all. It is important though to bear in mind methodological differences between the two surveys may have some influence on these differences

(2011 was conducted by telephone and 2016 was carried out face-to-face). However, there may also be contextual and market changes that help explain some of these differences. For example, internet penetration has increased significantly since 2011 and there are now many more ways to connect to the internet – particularly when on the go using connected mobile devices. This means greater numbers of people now experience the internet and as such may have more related concerns. More news stories within the media detailing data breaches and computer hacking may also contribute to this higher level of concern.

The in-depth interviews found less confident internet users citing concerns such as hacking, identity theft and stolen financial information, which are things they often hear about through the media. Being tricked or scammed also seemed to be a bigger concern for less confident internet users, for example email phishing scams.

> *"The Internet opens up the world… but I have this phobia…. About (getting a) virus, hacking…. Trying to steal information (from me)." (Male, 75+, London, low confidence internet user)*

> *"I have money invested and I'm concerned that people can suddenly hack in and take this… there's a lot of money in there," (Male, 65-74, Northern Ireland, low confidence internet user)*

More confident users were more likely to discuss more informed concerns about their personal information being used by companies largely regarding how the data is collected, often without them knowing about it.

> *"I get a bit worried about giving out my personal information and my own privacy. It's really easy to make a mistake and get your information out there" (Female, 55-64, Wales, high confidence internet user)*

3.4 Levels of concerns when going online

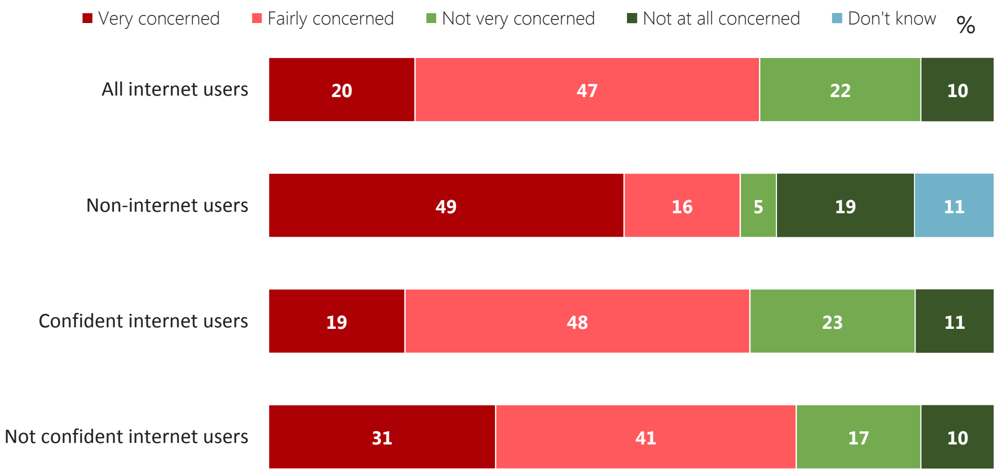
Following on from this spontaneous concern, and in line with other research, most internet users are worried about their privacy online. Non-internet users, and low confidence users, have an even greater intensity of concern (compared with younger people, for example, who are slightly less worried). This may be because more frequent users have become more used to the risks, even if they are just as aware of them (if not more so). Concern about privacy using the internet through a mobile signal is on par with concern about the internet generally, although there is a slightly higher degree of concern when accessing the internet through public Wi-Fi.

When respondents were asked directly how concerned they were about online privacy most showed some degree of concern. Two in three (67%) internet users say they were concerned about privacy online with one in five (20%) saying they are very concerned. Just one on three (32%) say they are either not very concerned or not at all concerned. A similar level of concern is seen amongst non-internet users (65%) while the number of those saying they are very concerned is much greater (49%).

A similar pattern of response is seen when looking at confident internet users compared with non-confident users. Two in three (67%) confident users say they are concerned compared with 72% of the non-confident group. However, the number of those very concerned is again much higher amongst those without internet confidence. Three in ten (31%) within this group say they are very concerned about their privacy when they go online compared with one in five (19%) of those with more confidence.

Figure 3.5: Levels of privacy concern about when going online

Generally speaking, when you use the internet, how concerned, if at all, are you about your privacy on line?



Base: Internet users 1,155 adults; non-internet users 268 adults

Younger users are less concerned than older users about their privacy online. 57% of 15-24 year olds and 60% of 25-34 year olds indicated a privacy concern, compared with 72% of 35-44 and 55-64 year olds, 75% of 45-54 year olds, and 73% of 65-74 year olds.

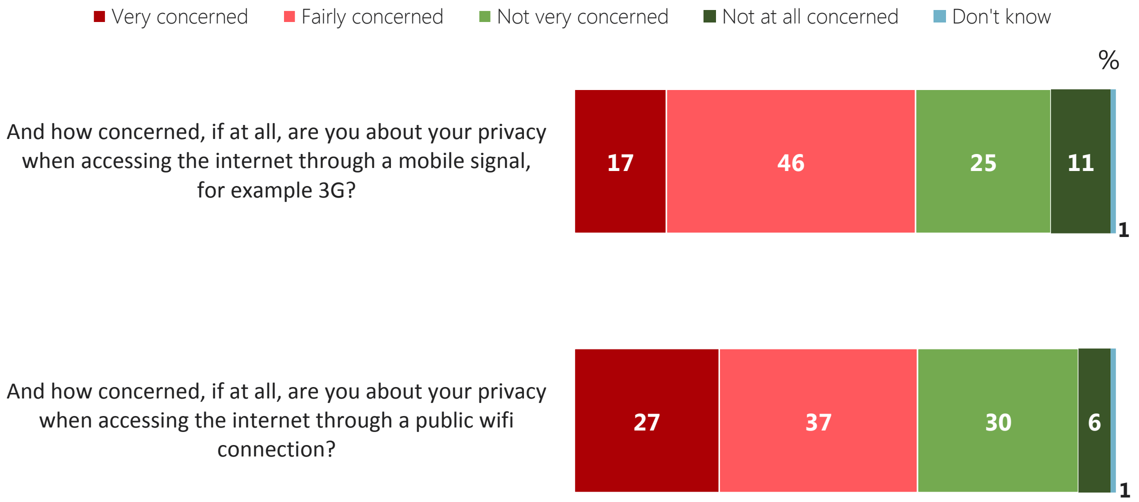
> ***"I'm paranoid about security and protection and data about myself. I do not feel safe at all. Maybe I'm being irrational... I do not feel safe using the Internet at all, except for the odd email." (Male, 65-74, Northern Ireland, low confidence internet user)***

Levels of concern have risen since the 2011 research where 58% overall said they were concerned about online privacy (18% were very concerned).[4] As noted previously, these changes may partly be explained by the increase in internet usage within the past five years as well as increases in media coverage regarding privacy issues.

[4] Although there are some comparisons to findings in the 2011 report it is important to note these comparisons are only indicative as there were changes in methodology.

The number of those concerned about online privacy in general (67%) is similar to those concerned about privacy when using the internet through a mobile signal (63%) and public Wi-Fi (64%). More people however are very concerned about privacy when accessing the internet through public Wi-Fi (27%).

Figure 3.6: Levels of privacy concern accessing the internet via a mobile phone and public Wi-Fi



Base: All who access the internet via a mobile phone 476 adults; All who access the internet via public wifi 159 adults

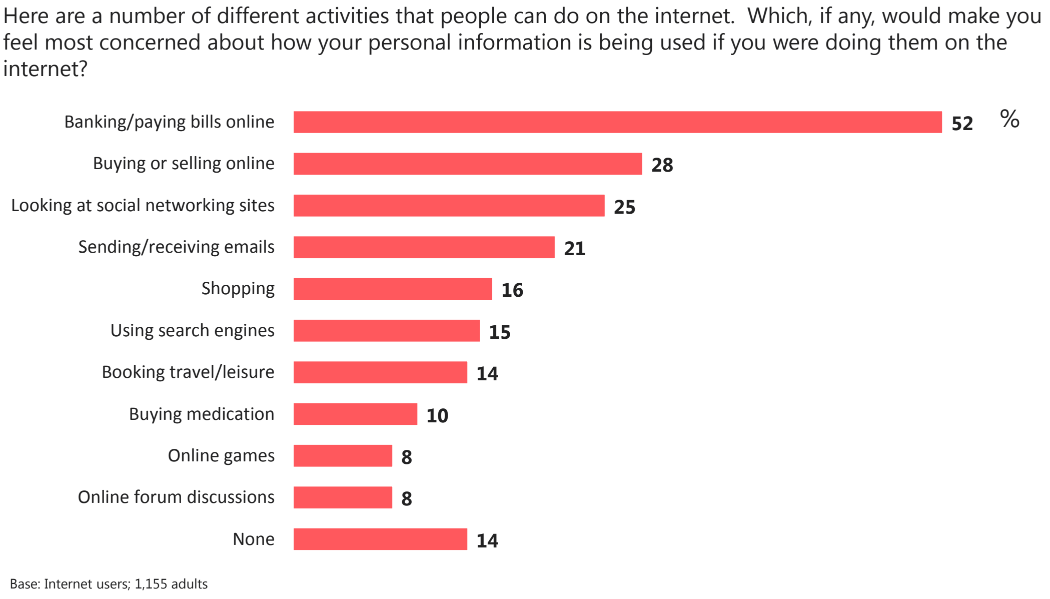
There are similar age differences when it comes to concern when accessing the internet through means other than home broadband. For example, 51% of 15-24 year olds are concerned about accessing the internet through a mobile signal, compared with 74% of 65-74 year olds, and 60% of 15-24 year olds concerned about public Wi-Fi connections compared with 76% of 65-74 year olds.

3.5 Activities people are most concerned about

Financial transactions such as banking, paying bills and buying and selling online cause most unease to consumers over use of their personal information, and people are also more worried about giving out their credit and debit card details online than other information such as their email or postal address. The in-depth interviews suggest different users respond to these concerns in different ways – high confidence users continue to buy things online regardless, but for some low confidence users concern about the privacy of their financial details is enough to make them limit their use of the internet.

Overall online financial transactions make people feel most concerned about how their personal information is being used. More than half (52%) say they are concerned about their personal information when banking or paying online bills, while 28% say that they are concerned about how their information is used when buying or selling products online on sites such as eBay. Other activities which people were concerned about how their personal information was being used include looking at social network sites (25%), shopping (16%), using search engines (15%) and booking travel (14%).

Figure 3.7: Most concerning internet activities



Base: Internet users; 1,155 adults

Interestingly the results showed no statistical significance when it came to differences between those with and without internet confidence. There was also little age difference when it came to concerns about banking and paying bills online. Half (51%) of those aged between 15 and 34 said they are concerned about how their personal information is being used when banking or paying bills, compared to 55% of 65-74 year olds and 45% of those aged 75+.

The qualitative interviews supported these findings and found that people were concerned about doing any financial transactions online in fear of exposing themselves to fraud or their details being stolen. However, this concern would not necessarily stop confident users from doing financial transactions online but would make them more cautious while doing so. Low confident internet users were more likely to cut out doing any financial transactions online altogether and as one interviewee demonstrated below can be persistent in doing so.

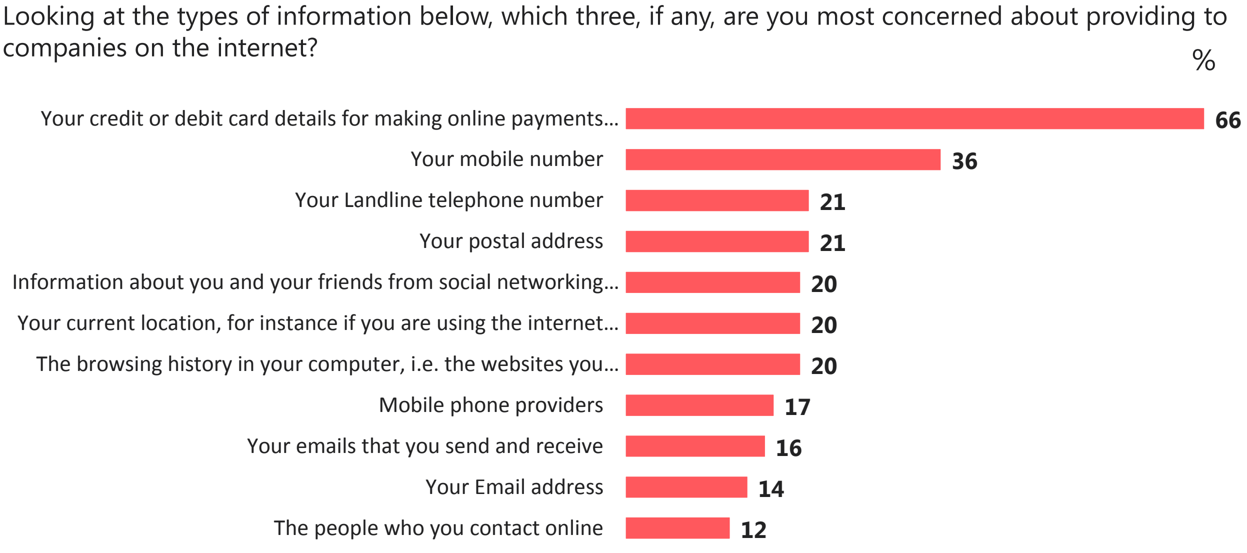
> ***"Unless I'd absolutely have to, I wouldn't do internet banking on a network outside of this house. Some networks are fairly easy for someone with a bit of savvy to get access to what you're doing." (Male, 55-64, Northern Ireland, high confidence internet user)***
>
> ***"The bank told me that if I don't join this (internet banking) I will not be allowed to use the bank. I fought this and have now been given until 2020 without internet banking." (Male, 75+, East of England, low confidence internet user)***

Younger people however were more likely to be concerned about buying and selling things online as well as using social media sites. Two in five (39%) 15-24 year olds said they were concerned about how their personal information was used on buying/selling sites such as eBay. This compares with roughly a quarter of those aged 45-74 and 19% of those aged 75 and above. A third (33%) of 15-24 year olds also said they were concerned about their personal information when using social media sites compared with 23% of those aged 45-54 and 19% aged 55-64. This may however be a generational issue as younger people may be more likely to access both websites used for buying and selling goods as well as social media websites. The survey found that a third of those (33%) with a social media account are concerned about their personal information when on these websites compared to 19% without an account.

> *"I have no confidence in how my data is shared on things like that (social media). I think Facebook turned into a limited company and they needed to make a profit, making a profit means they need my data to sell to companies to advertise to me. Now it's being run as a business it means all my data is out there, including my photographs, and what I'm looking at and what I'm interested in." (Male, 35-44, London, high confidence internet user)*

There were considerable reservations about providing credit or debit card details to companies online where two in three (66%) said they were concerned about providing these details on prompting. This concern was much higher than concern surrounding providing a mobile phone number (36%) which was the second highest concern from the list.

Figure 3.8: Types of information consumers are most concerned about providing online



Base: Internet users; 1,155 adults

Non-confident users were more likely to be concerned about providing their landline number compared to confident users (33% compared to 20%) while confident users were more concerned providing credit/debit card details than non-confident users (68% compared with 54%) as well as their location (21% compared with 13%). Those who have a social media account were also more concerned about sharing their mobile number than those without (38% of social media account holders saying they were worried about this compared with 30% of those without an account).

> *"I don't like the idea of websites like Facebook having my contact details, so I never put my mobile phone number or address on there" (Male, 25-34, Scotland, high confidence internet user)*

Older people were more concerned about sharing credit or debit card information than younger people. Two in three (66%) aged between 15 and 24 said they were concerned as did 57% of those aged 25-34. This compares to eight in ten (79%) of those aged 55-64 and 70% of those aged 75+.

Those in England exhibited the least amount of concern when it came to sharing credit and debit card information when compared to other nations. Two in three (65%) of those in England mentioned their concern about providing this information compared with four in five (80%) in Northern Ireland, 77% in Wales and 70% on Scotland.

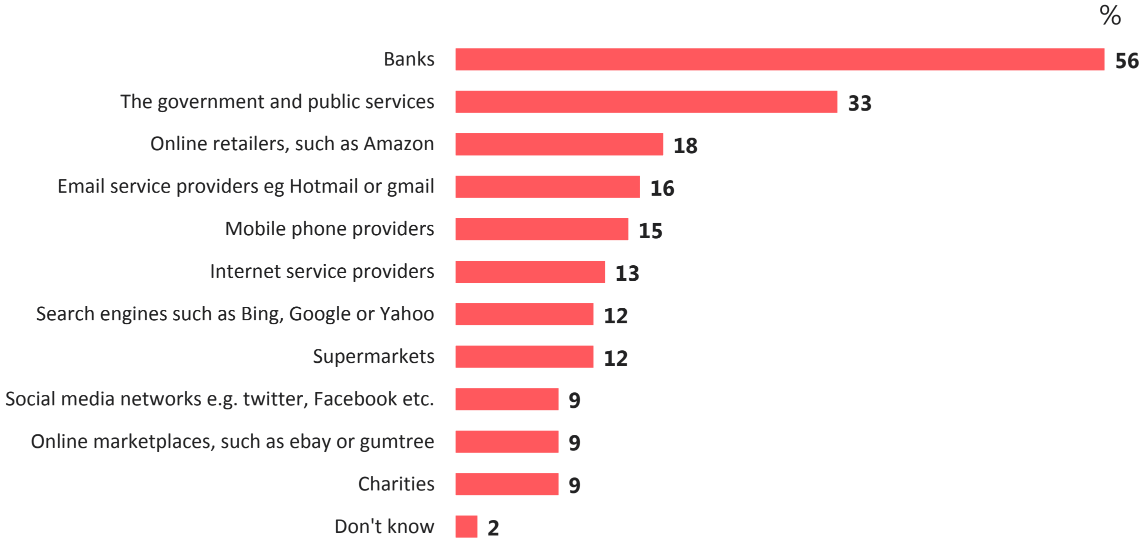
3.6 The most trusted organisations with personal data

Despite financial transactions causing people the most worry on the internet, banks themselves are the most trusted organisation to deal with consumers' personal information – perhaps because they are seen as experienced in dealing with sensitive information as well as having an established reputation to protect. Government and public services are the next most trusted, but social media networks and online marketplaces are the least trusted. Even charities are viewed with some suspicion with concerns about personal information being shared between different charities.

In the quantitative survey internet users were read out a list of different types of organisations and asked to identify which they trust most with their personal information. Banks were seen to be the most trusted organisation type mentioned by 56% of those surveyed. This was followed by the government and public service organisations (33%), online retailers (18%) and email service providers (16%).

Figure 3.9: The organisations consumers trust most with their personal information

Which of the following types of organisations, if any, do you trust with your personal information?



Base: 1,423 UK adults

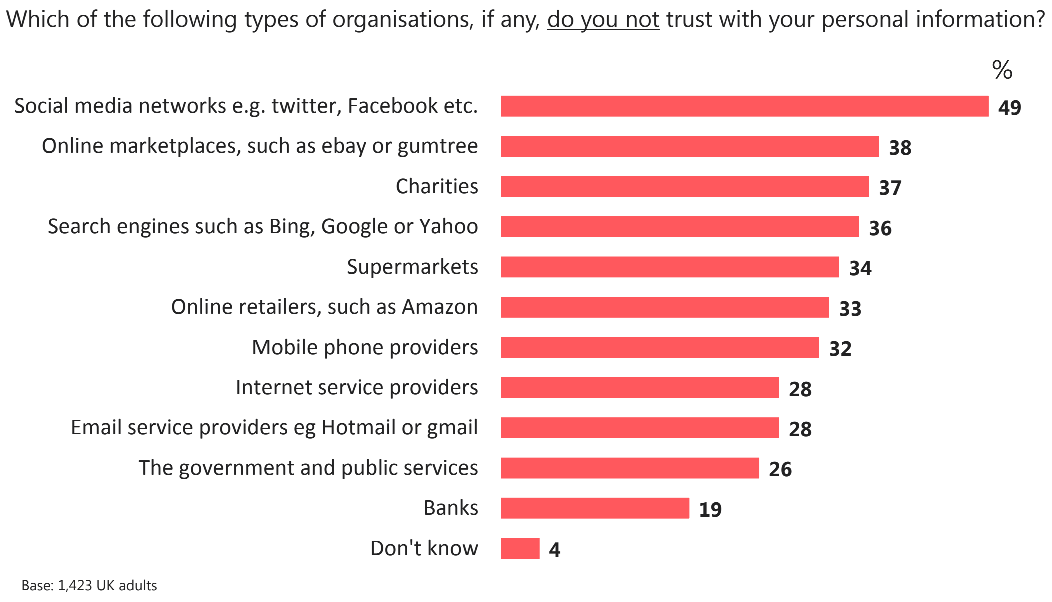
When asked why they trusted banks, several participants in the qualitative research cited that it is because banks are more accustomed to dealing with sensitive financial information and are thus more likely to have better security practices in place. Some also mentioned their recognisable branding and having a high reputation to preserve while one other respondent stated that trust comes from the personal relationship already established with his bank.

> *"(My bank) wouldn't do that (share information with other companies) … they aren't allowed to do that." (Male, 75+, East of England, low confidence internet user)*
>
> *"I've got a relationship with my bank and the online service is an aspect of that which makes it easier for me to interact with them…. I choose to use that…it's not a website that is trying to sell me something I wouldn't normally buy…. In my mind." (Male, 35-44, London, high confidence internet user)*

Trust in banks holding personal data was highest amongst all age groups however younger internet users expressed higher levels of trust for banks than did older users. Two-thirds (65%) of 15-24 year olds and 56% of 25-34 year olds said that they trust banks compared to 44% of 55-64 year olds and 38% of those aged 75+. Despite comparatively lower levels in trust of banks amongst older people, trust for all organisations tended to be lower than those seen in younger age groups.

Consumers were also asked which organisations they trusted least. Social media networks were the most cited type (49%). Online marketplaces were also seen as less trusted (38%), as were charities (37%).

Figure 3.10: The organisations consumers trust least with their personal information



Which of the following types of organisations, if any, do you not trust with your personal information?

Base: 1,423 UK adults

By nation, people in Scotland were least trustful of charities with two in five (40%) saying they do not trust them. This compares with a similar level in England (37%) while one in three (32%) in Northern Ireland and a quarter in Wales (25%) said they do not trust charities.

While charities were low on the list of trusted groups in the survey findings, several people explained why this might be within the in-depth interviews. People mentioned they tend to trust the larger more recognisable charities such as Greenpeace. Some claimed that charities often share information with other charities, and that once they sign up to help one charitable organisation, they start to see 'junk mail' appear from other types of charities.

> *"I'm willing to share information only with the bigger known charities, like Greenpeace or Friends of the Earth. I'm a bit weary of the fundraising tactics of the smaller ones and they can share your information with each other." (Female, 55-64, Wales, high confidence internet user)*

3.7 How consumers identify trust

Throughout this research, pre-existing trust in an organisation was regularly used as a short-hand for deciding whether or not to share their personal information with them online – especially given (as later findings show) many feel they have little control over what happens to their information when they do hand it over. In particular, three factors were key to building this trust: 1) being open and transparent about what data they collect and use, 2) providing consumers the opportunity to opt-out of any use of their data, and 3) keeping consumers' data secure.

We asked respondents in the qualitative interviews what "trust" in a company means in regards to online privacy. Three issues were identified as recurring themes across the interviews:

1. **Organisations should be fully open about what data they collect/use and what they will do with it**. Most felt that they can find out what a company does with their data only if they are willing to do some digging on their website – there is still a belief that consumers are not being put first. Even those with advanced technical abilities had issues with reading terms and conditions and cookie policies.

> *"Terms and conditions often make no sense and sound too legal. They should be written from the common man's point of view" (Male, 35-44, North-west England, high confidence internet user)*

2. **Organisations should provide the consumer the opportunity to opt-out of any use of their data**. Although many respondents recognised they often have the opportunity to opt-out, the wording of "opt-outs" could be just as confusing as terms and conditions, for example it was not always clear if they should tick or untick a box to not receive marketing information. Some participants were also unclear over the full extent of what an opt out really means. There might be occasions when a consumer wants to hear from their company about relevant products, but this does not mean they are willing to receive marketing messages about new products and services or have their data shared or sold.

> ***"I always opt-out of marketing emails whenever I'm given the chance to but I always trust the websites and companies I deal with most to honour that." (Male, 65-74, North-West England, high confidence internet user)***

3. Organisations should keep consumers' information secure. Consumers are not just concerned about protecting their own devices from hackers, but they also worry about their data being protected once in possession of companies. Concerns have been heightened by newspaper coverage about sensitive data being lost or stolen.

> ***"Trust means not to be hacked or misused… not to sell information for their benefit. I got car insurance now I receive messages everyday about car insurance." (Male, 75+, London, low confidence internet user)***

The qualitative research also showed it was common practice, particularly amongst the less confident (often older) internet users to restrict their internet usage to only visiting "safe places", for example, recognised brands or websites they trust. There was sometimes a sense of 'overlooking' the fact that these websites use their personal data, but deliberately deciding not to think about it and instead placing their trust that these brands will use their data responsibly.

> ***"I'm not all that worried because I only use sites I trust like Sainsbury's or my bank. I feel safe with them but wouldn't visit a website I don't know or ever heard of." (Male, East of England, 75+, low confidence internet user)***

> ***"I go to websites like John Lewis which I trust, partly because I trusted them even before there was the internet." (Female, 55-64, Wales, high confidence internet user)***

4 Consumer understanding and awareness of the uses of personal data

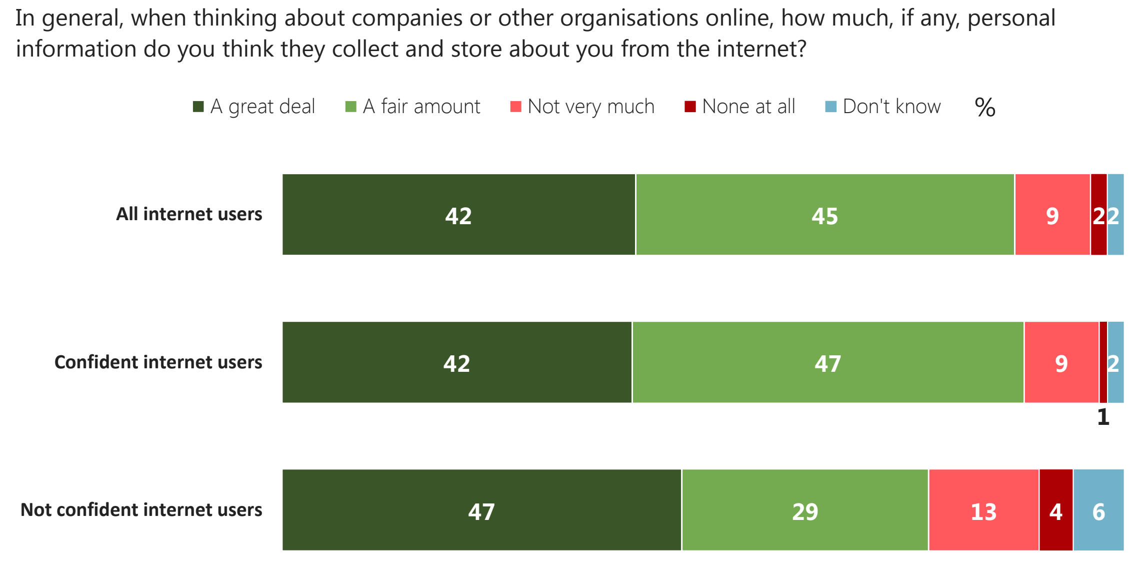
This section reviews consumer awareness of personal information being used by companies online, their willingness to share personal information, and to what degree the value of this exchange benefits both companies and consumers. While many are aware of various methods of personal data collection, this is lower among older and less confident internet users. Few consumers feel they benefit personally from the use of their personal data, and nor do they feel companies are very transparent about it, even though they are resigned to it, despite their concerns.

4.1 Awareness of what methods companies use to collect personal data

As previous research has also shown, nearly all internet users believe that companies store a great deal or fair amount of personal information about them. Confident internet users tend to be more aware of the various methods that companies use to collect information (despite expressing slightly less intensity of concern over privacy overall), while less confident users had a vaguer idea of what is done with their data.

In the quantitative survey internet users were asked how much personal information they thought companies and other organisations online collect and store about them. A vast majority (87%) believed that companies collect and store either a great deal or fair amount of personal information about them with perceptions regarding the volume of data collected being higher among more confident internet users.

Figure 4.1: Consumer perceptions of how much personal data companies collect


In general, when thinking about companies or other organisations online, how much, if any, personal information do you think they collect and store about you from the internet?

Base: Internet users 1,155 adults

There was some difference between age groups with older people being more likely to say a great deal of information is collected about them than younger people. 47% of 55-64 year olds and 41% of those aged 75+ said a great deal of information was collected compared with three in ten (31%) 15-24 year olds and 37% of 25-34 year olds.

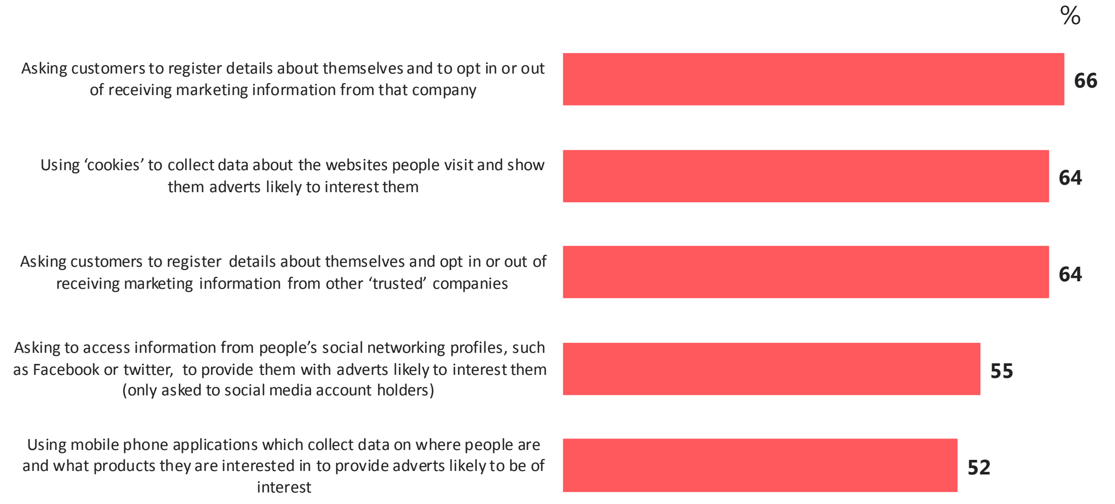
The qualitative interviews indicated people's knowledge regarding how this information gathering process works or what control you have over it is low.

> ***"There are ways of getting it (personal information) …how they get it I don't know." (Male, 75+, East of England, low confident internet user).***
>
> ***They will store information (about you) …. I live with it… I don't know how to avoid it…. When people know what you've been looking at… I accept it…. I don't know how to stop it… "(Male, 65-74, North-west England, low confident internet user).***

People in Wales and Northern Ireland were more likely to say companies collect and store a great deal of personal information about them. Nearly three in five (58%) Welsh respondents and 54% of Northern Irish respondents thought a great deal was collected about them, compared with two in five (41%) in both England and Scotland.

All respondents in the quantitative survey were provided with a list of ways in which companies and organisations collect data online and asked which of them they had heard of. Two-thirds (66%) said they were aware of companies asking consumers to register details about themselves in order to send them marketing information from that company. Similarly, most were also familiar with companies asking consumers to register details to receive marketing information from other 'trusted' companies as well as the use of cookies to collect personal information (both mentioned by 64%). Accessing people's personal information from social networking sites (mentioned by 55% although rises to 69% amongst those who have a social media account) and collecting data from mobile phone applications (52%) were slightly less familiar than the other methods listed.

Figure 4.2: Consumer recognised methods personal data is collected by companies



Base: 1,423 UK adults

In terms of age, there were only differences observed among the 75+ age group where, for example, fewer people (34%) said they had heard of registering details to opt-in or out of marketing information from that company. Those with disabilities were also less likely to have heard about each of these personal information methods (for example 57% of those with a disability have heard about registering details to opt in or out of marketing information from that company compared to 68% without a disability).

Those with lower internet confidence also had lower awareness levels. For example, just a third (34%) of those not confident using the internet had heard about registering personal details to receive marketing information (the most popular data collection methods) compared with three-quarters (75%) of internet users. This was true even amongst older people where four in five (80%) confident internet users aged 65+ had heard of this data collection method compared with 27% less confident users the same age.

The order of awareness of these methods is broadly in line with figures from the 2011 Panel report. However, 85% of people claimed to have heard of companies asking to register details to receive more marketing information from that company in 2011 (compared with 66% in 2016) and 80% said they have heard of companies asking to use personal information to receive marketing information from other 'trusted' companies (compared to 64% in 2016).

The qualitative interviews provided the opportunity to discuss methods of personal data collection in more depth. Less confident (and often older) internet users had a vaguer awareness of the different ways companies can collect personal data online than did confident users. Many of these respondents were completely unaware that their data footprint included information on their location and that they were routinely sharing their web surfing history (although, some might have guessed that this happened when they receive junk mail).

"I don't know what the situation is [meaning companies collecting and using personal information]. It's grown out of control… It seems to be just accepted now…. spam keeps coming through the door, I despair." (Male, 65-74, Northern Ireland, low confidence internet user)

"I didn't really know they could do that (meaning cookies collecting personal information after being explained by the interviewer), but I can say I'm uncomfortable with the idea." (Female, 55-64, Northern Ireland, low confidence internet user).

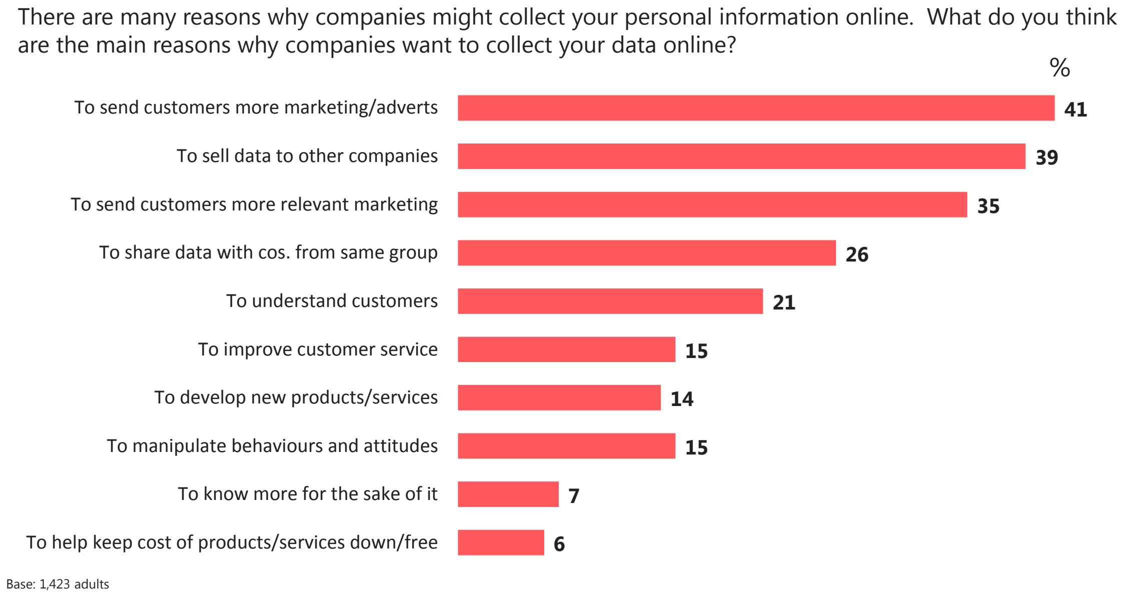
"Yeah I can tell it's happening, like on Facebook when an ad pops up and it says something like 'Amazon recommends this for you'. But I only like this when it's a connection to me, like my local area or local club, not larger companies." (Male, 55-64, Scotland, high confidence internet user)

4.2 Awareness of why companies want consumer personal information

Consumer attitudes towards personal information, and trust in how it is used, may be related to their perceptions of companies' motives for collecting it in the first place. In the main, people assume companies collect personal information for the company's benefit rather than their own (for example, to send more marketing materials or to sell on to other companies rather than improve customer service or develop new products or services). The qualitative interviews suggest that while some accept companies can use personal information for some internal purposes, there was still an underlying suspicion – especially of companies selling personal information on to third parties.

The quantitative survey asked all people what they thought were the main reasons for companies to want to collect their personal data. Marketing related reasons were the most common cited, with 41% saying to send customers more marketing information, 39% saying to sell personal data to other companies and 35% saying to sell them more 'relevant' marketing material.

Figure 4.3: Reasons companies want personal data according to consumers



Confident users were more aware of the reasons why companies collect consumers' personal data then low confident users. For example, two in five (41%) confident users said companies use it to send marketing/advertisements compared with a quarter (25%) of low confident users, and 42% of confident users said companies sell the information to other companies compared with another quarter (25%) of low confident users. Nearly a quarter (23%) of all low confident internet users could not state any reason, compared with just 3% of confident users, showing the low level awareness of what companies do with personal data amongst this group.

Those with higher concerns around privacy when going online were also more likely to say that companies want personal data for marketing purposes. 44% of those who were concerned about privacy stated companies want their data to send customers marketing material or advertisements compared with 38% who were not concerned about privacy, and 42% who were concerned about privacy said companies want their data to sell on to other companies compared with 34% who were not concerned about privacy.

Within the qualitative findings, consumers felt that on balance if there was more transparency it would be more acceptable for companies to use their personal data under certain conditions. For example, it was considered acceptable to use customer data to improve products and services, or to tailor marketing messages.

> *"It benefits them to know what other websites you've been to… so they can build a profile of you based on those sites and target marketing to you based on that history." (Male, 35-44, Wales, high confidence internet user).*

> *"To know your tastes… to sell your information on… putting that information together is worth money for them." (Male, 35-44, London, high confidence internet user).*

However, it would be less acceptable to sell personal data onto third parties. Their reasons for this were unease around consumer control over their own data which it was felt would be permanently lost once it is handed over, or shared with other companies. To many this was simply a form of being taken advantage of.

> *"They're looking for how to somehow or other exploit us, and our spending habits… I don't like it at all." (Male, 65-74, Northern Ireland, low confidence internet user)*

The qualitative interviews also revealed that there was some recognition that companies want to make money from consumers' personal information and views in this area tended to be negative and related to the profit interests of the organisations as opposed to benefitting customers.

> *"Why do companies want your information? They make big money from it! Then they can sell to you, if you like certain things they can push that on you." (Male, 75+, East of England, low confidence internet user)"*

> *"They (companies) take the information about you, they sell these details to other people (meaning other companies)." (Male, 75+, London, low confidence internet user).*

4.3 Views on cookies

The in-depth interviews revealed that consumers have diverse attitudes on what cookies are and what they do. Less confident internet users have a vaguer awareness of cookies, while awareness was higher among confident users. General attitudes towards them were suspicious, although more regular users had got used to them, and a small number even identify some positive results from using cookies. Cookies generally do not cause enough concern to stop consumers using the internet. They are however considered somewhat "devious" as they operate in the background.

The qualitative element of this research allowed the chance to speak more in depth with consumers about the use of cookies by companies to collect data. Several less confident (often older) internet users had only a vague awareness of cookies, often being unable to explain what a cookie is, or what implications cookies have for their privacy. They were also less aware of the cookies policies pop ups when visiting websites.

> *"I understand that it's something subliminal by directing me to adverts but it's rather uncomfortable. I have no idea you can do anything about them but I think my husband might be doing something about it" (Female, 75+, Yorkshire and Humberside, low confidence internet user)*

> *"I can tell it is happening when it … the junk mail comes in more and more often." (Male, 75+, East of England, low confidence internet user)*

> *"I don't know what Cookies do...I just try to get rid of them." (Male, 75+, low confidence, North-west England)*

Generally, the idea of cookies did not cause enough concern to stop people using the internet even if seen as a bit “sneaky” operating in the background. Some more confident internet users however were more concerned about cookies knowing where they were in terms of location on top of what they browse on the internet.

> *“Cookies don't make it clear what they are obtaining from you and how they store the data” (Male, 35-44, Wales, high confidence internet user)*

> *“It’s not the cookies tracking your web browsing that bothers me, it’s the location finder I don’t like. They can tell where I am!” (Male, 35-44, North-west England, high confidence internet user)*

Positive views towards cookies were less common. Two interviewees mentioned that cookies can actually make web browsing easier as they do not have to repeat entering certain details when revisiting a website or making certain aspects within a website more accessible.

> *“Cookies have information about what I've done before, so that if I use website again it's easier. Your information is filled in automatically. I never delete cookies. I probably would do it if I had a virus and needed to clean it up” (Female, 35-44, Wales, high confidence internet user)*

> *“I let the cookies work when I visit the BBC website… I’m not 100% sure but … the way the website is arranged then those articles I’m interested in are more accessible because of my history.” (Male, 35-44, Wales, high confidence internet user).*

4.4 Consumer attitudes towards the openness and transparency of companies using personal data

As the previous results have shown, while there is a broad awareness that a great deal of personal information is collected online, knowledge of the details is mixed, especially between confident and less confident users. Similarly, in the qualitative interviews consumers believed that information on what organisations do with personal data is out there, however they share a sense that it is not readily available and requires significant time and effort to uncover. Generally, users feel that there is a lack of transparency, in some cases deliberately, in order to confuse or mislead consumers (this feeds into general perceptions of mistrust in organisations’ behaviour online, discussed earlier). As found in other studies, only a minority (35%) say they often read Terms and Conditions (and even this may be an overstatement), and to make it easier some desired a summary of important information in order for users to broadly understand what they are agreeing to.

Most qualitative participants felt that if they wanted to find out how companies collect personal information, and what they do with this data, it was possible to do so by researching their websites. There was a sense however that there is a lack of transparency, and that any information provided would be difficult to find. Furthermore, some stated that this was deliberately confusing and possibly even misleading.

> ***"You can find out how most companies use your information with a little research but they certainly don't promote it." (Male, 15-24, Yorkshire and Humberside, high confidence internet user)***

> ***"Depending on the website, if I really was concerned about it I would look into it. But it's hard, websites don't give away much." (Male, 35-44, Scotland, high confidence internet user)***

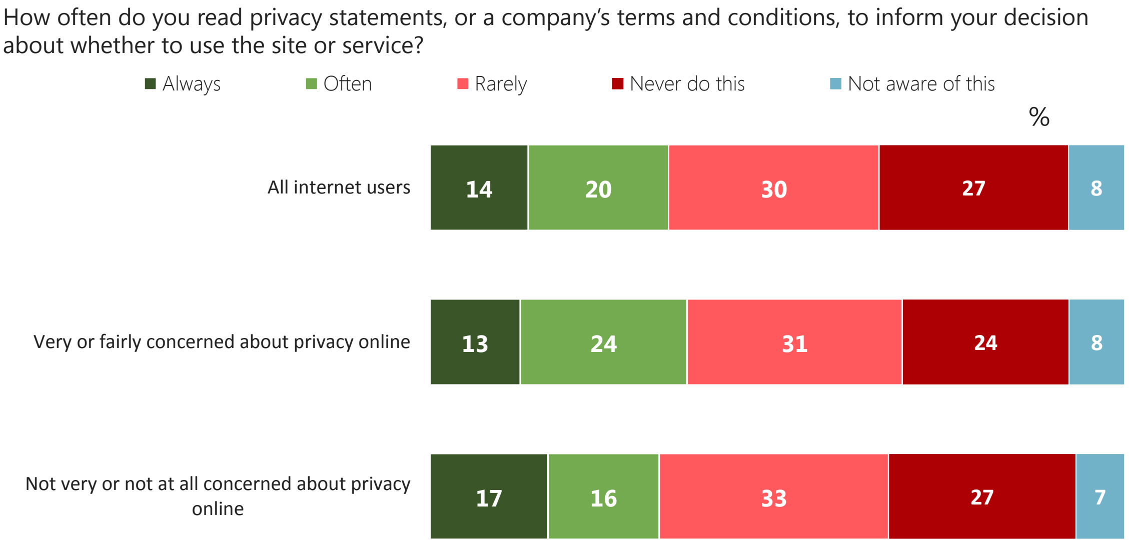
The research found that respondents consider Terms and Conditions to be like legal documents: lengthy and difficult to understand. This contributed to the sense of companies being misleading with the use and collection of personal data. There was a strong desire for 'executive summaries' to be included in these statements which would encourage their chances of reading them. Respondents argued that currently companies simply provide disclosures in an agreement or present Terms and Conditions at sign up to meet basic regulatory requirements, but these do little or nothing to help increase transparency.

> ***"People, (and) myself included, can't be bothered reading all of that. People don't care about terms and conditions" (Female, 45-54, Northern Ireland, low confidence internet user)***

> ***"Terms and conditions are so long! They must know that people aren't going to read all these things. They should use the Plain English Society to help them write these better." (Female, 55-64, Wales, high confidence internet user)***

The quantitative survey data also finds that one in three (35%) consumers say they often read privacy statements on websites while 57% say they rarely or never read them (there may also be some social desirability bias here and actual levels could even be lower). There was little difference between those with high concerns in regards to privacy on the internet and those with low concerns (which perhaps suggests little confidence in Terms and Conditions as a way of alleviating concerns). 37% of those who said they are either very or fairly concerned about privacy online said they often read Terms and Conditions, which compares to a third (33%) of those who are not concerned about privacy. The habit of rarely reading these policies seems to be a shared across all segments of society as there was also little difference in those who read privacy statements between most characteristics, including internet confidence level and educational attainment level.

Figure 4.4: Frequency of internet users reading website Terms and Conditions



Base: Internet users; 1,155 adults

Most respondents within the qualitative interviews, regardless of internet confidence level, expressed a need for greater understanding and awareness in how their personal data is being used. This would in part be helped by having greater transparency; to see exactly when, and which, information is taken from them when a website uses cookies, for example, a banner warning when cookies are used. This was noted in the previous chapter as one of the three elements of what constitutes "trust" in a company. There was a general feeling however that companies are not very open in how and why they collect data, or how they store it and whether they share it with other companies.

> *"Websites don't tell you what they're doing, they just do it. They don't have a notice telling you they're sharing your information." (Male, 25-34, Scotland, high confidence internet level)*

> *"When they contact you they don't tell me where they got my information. Who passed it on to them? They should disclose this" (Female, 75+, Yorkshire and Humberside, low confidence internet user)*

4.5 Consumer willingness to hand over personal data

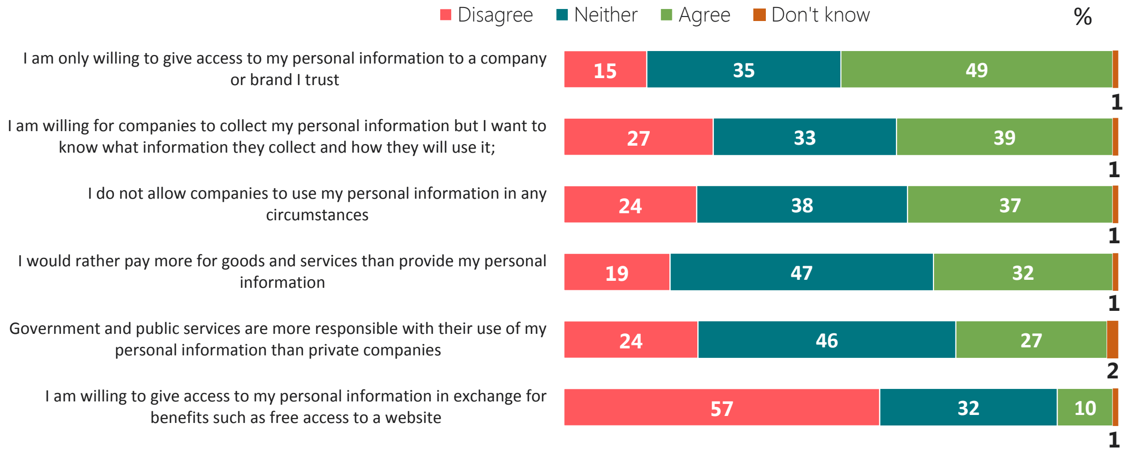
The importance of trust in an organisation is reiterated with the finding that consumers are more willing to share personal information with organisations they know and trust. People would also on balance like more information about how their personal information is used, and there is little sign that government and public services are viewed any more positively than private companies. There is also further evidence of the contradictions between consumer attitudes towards privacy online and their actual behaviours. While many say they are not willing to provide their personal information in exchange for free access to a website (and even some saying under any circumstances), this does not seem compatible with the reality of the way the internet works. This may reflect a lack of knowledge of the ways in which personal information really is collected online, or be an expression of concern over a risk that some feel they cannot avoid if they want to use the internet in the way they have become accustomed to.

In the quantitative survey internet users were asked how willing they were to share personal information in various circumstances. Overall, internet users were most comfortable with sharing personal information with companies or brands they trust most. This reflects the earlier qualitative findings that overall trust in a brand is a big factor in how consumers decide to share their personal data online. They were also likely to say that they would not allow companies to use their personal information in any circumstance although it is not clear if this means only when given the option to disallow the use of their data. In fact, as other research has shown in the first chapter, there is a mismatch between consumer attitudes towards privacy and their behaviours (i.e., despite being concerned about privacy, people still use the internet). This may be another example of people expressing concern, even if in reality their personal information is often used.

Lack of awareness may also be a contributor to the contradictions between consumers' behaviours and attitudes. For example, in our data we find that 37% say that they do not allow companies to access their personal information in any circumstance; however, we know that providing personal information is generally a prerequisite to website access. It may be that many of those within our 37% are not aware that they are indeed giving access to their personal information, for example through cookies when visiting these websites. There is a general lack of understanding within this area necessitating further research.

Figure 4.5: Internet user willingness to provide their personal information to companies and organisations

Each of the following statements describe how some people generally feel about companies using their personal information. For each statement can you please say if you agree or disagree, on a scale of 1 to 10 where 1 means you totally disagree and 10 means you totally agree.



Base: Internet users; 1,155 adults

Confident internet users are more likely to agree to give access to their personal information than those with little confidence. Half (50%) of confident internet users agreed (with a score of 8-10) they would be willing to give their personal information to a brand they trusted compared with 38% of those with low confidence. Higher social grades were also more likely to provide information to a company or brand they trust. More than half (57%) of ABs would do this compared with 41% of DEs.

Less confident internet users were more willing to agree to paying more for goods and services than provide personal information. Two in five (41%) of those who are not confident using the internet agreed to this compared with one in three (32%) confident internet users. Even 42% of those in the lowest income bracket (earning less than £9,500) said they would be willing to pay more compared with 27% of those in the highest income bracket (earning more than £40,000).

More than half (52%) of non-confident internet users said that they do not allow companies to access their personal information in any circumstance, compared with 36% of confident users. This was also demonstrated amongst older age groups. 62% of 55-74 year olds and 64% of those aged 75+ agreed to this compared with a quarter (26%) of 15-24 year olds and a third (33%) of 25-34 year olds. Those who felt like they have no control over their personal information (explained in the next chapter) were also more likely to agree that they never give their personal information away. Half (49%) who say they have no control claimed they never give their information away compared with 31% of those who feel they have control. These differences may provide some evidence to the argument made above that there may be a discrepancy between awareness and behaviour. Some consumers simply may not be aware that they are providing personal information to companies even when they think they are not.

In the quantitative survey, there was some more favourability in allowing personal data to be used if consumers were told how it was collected and how it was being used, with 39% agreeing (although this means there was slightly less in agreement than was in the 2011 Panel report). Most were in disagreement however that they would be willing to give away their personal information in exchange for benefits, including using the website free of charge. Again, this may reflect an expression of concern more than an actual behaviour. In fact, many do use free websites that collect their data. Indeed, the qualitative findings suggest that there is more of a sense of resignation towards this as well as a possible lack of awareness of when websites collect data. When pressed people say they can accept that companies will use their data, even if they do not recognise they get a great deal of benefit from it, and that it feels an unavoidable part of using the internet. The findings also suggest that there is a lack of understanding amongst consumers surrounding website business models used by companies and more specifically how they operate. Although many say they would not allow companies to use their personal information it may be that some are not fully aware when it is in fact being collected and used.

4.6 Who benefits most – the consumer or company?

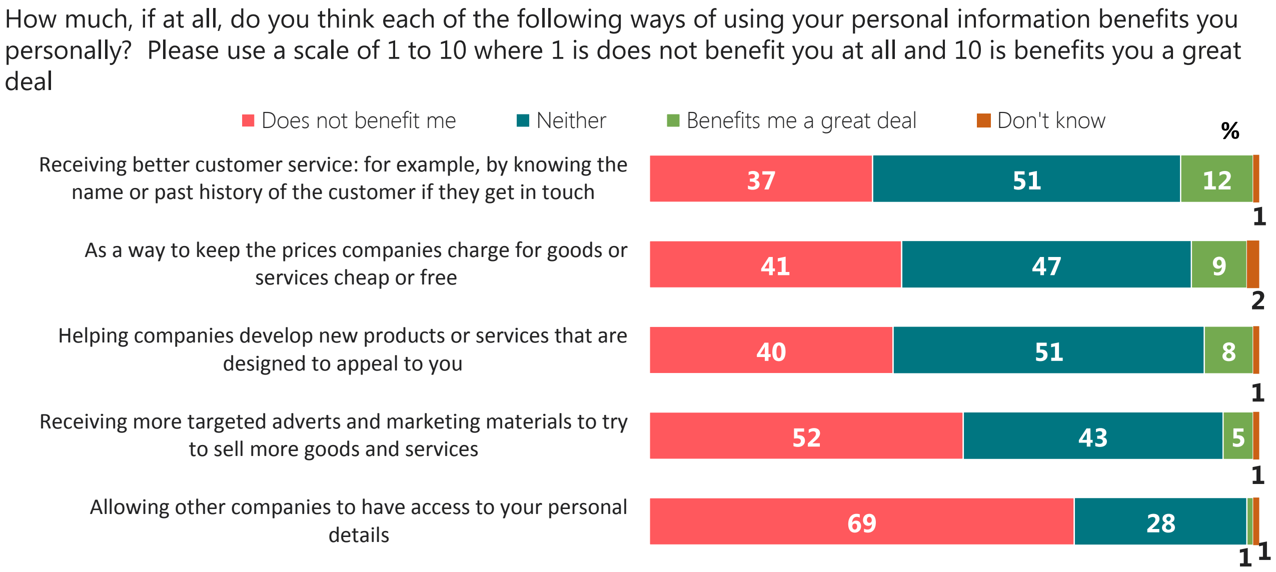
As noted above, people are more likely to feel that companies collect personal information for marketing and selling on rather than for improving customer service or developing new products, and in general very few feel that this exchange benefits them personally. Consumers are particularly concerned about the prospect of their personal information being shared with third parties.

Respondents in both the survey and in-depth interviews expressed opinions demonstrating they believed companies want consumers' personal information to make money and sell products. They struggled however with recognising the benefits which the consumer receives within this value exchange.

In the survey internet users were given a list of various uses of personal data and asked on a scale of 1-10 how much each use benefits them personally, where 1 does not benefit them and 10 benefits them a great deal. Each of the listed uses however were felt to offer little benefit to consumers.

Overall, improving customer services was the use of personal data that was felt to provide the most benefit for the internet consumers (with 12% agreeing) while allowing other companies to have access to personal details was seen as having the least benefit for consumers (with just 1% agreeing).

Figure 4.6: Perceived benefits by internet users for providing personal information to companies



Base: Internet users; 1,155 adults

The qualitative interviews confirmed there was a struggle to recognise the benefits sharing personal data can bring consumers. However, in line with the quantitative findings, some did mention that improving customer services were also seen as positive, yet not as a top of mind benefit, as respondents only reacted positively to the idea when it was asked by the interviewer.

> *"If there is a positive use to the data like that, to improve how they interact with customers, then yeah, I'm generally happier about them using it (personal data)." (Male, 35-44, London, high confidence internet user)*

All qualitative participants were uncomfortable with companies selling their data to other organisations, citing that it is an unfair exchange after they make a conscious decision to visit one specific website or brand and not the one their information is being passed on to. Most however felt they would accept the use of their personal data if it was kept only within the company (that is not passing it on to other companies) and even if for marketing purposes. Although if given the choice they would also opt-out of this type of data usage.

> ***"It's not really fair [meaning the exchanging of personal data between companies], I made a conscious decision to visit a certain website and not the one they sold my information to" (Female, 45-54, Wales, high confidence internet user).***

Nevertheless, many still struggled to articulate the benefits of exchanging personal information with companies. This may again be related to consumer predispositions and understanding that companies exist to be profitable.

> ***"It's not going to benefit me… it benefits them not me… it's all about sales." (Male, 65-74, North-west England, low confidence internet user).***

> ***"The consumer only really wants to hear about these things at the point of purchase… we were looking at fitted wardrobes at Xmas… I'm still going onto YouTube and half way through my video a post relating to wardrobes pops up on my screen. I'm not benefiting from that anymore…. It can last too long after the initial enquiry." (Male, 35-44, London, high confidence internet user).***

Despite consumers saying they had reservations about companies collecting and using their personal information while they browse the internet there was also some sense of resignation. Several saw it as a way of life.

> ***"I guess it doesn't matter to me, it's just part of life using the internet these days. You have to accept they'll use your information if you want to use the internet" (Male, 55-64, Scotland, high confidence internet user)***

> ***"I sometimes feel I have no choice but to provide that information… if I want a certain product sometimes I have to supply it." (Male, 35-44, London, high confidence internet user)***

Others, when thinking about the use of personal information in more depth believed that although using information for things such as advertising can be seen as underhand it did not cause the consumer any damage.

> ***"Some things [meaning the use of personal information by companies] are so minor, people don't notice their information is being used so it doesn't bother them. Things like personal advertising aren't so severe or malicious I suppose" (Male 15-24, Yorkshire and Humberside, high confidence internet user)***

Overall consumers perceive that they receive few benefits when it comes to the exchange of personal information and assume that companies are the primary beneficiary. In some instances, this may be related to a lack of understanding of how the website business model used by companies works. Despite this however there is a perception that consumers need to protect their personal data while online – discussed in the following chapter.

5 How consumers protect themselves online

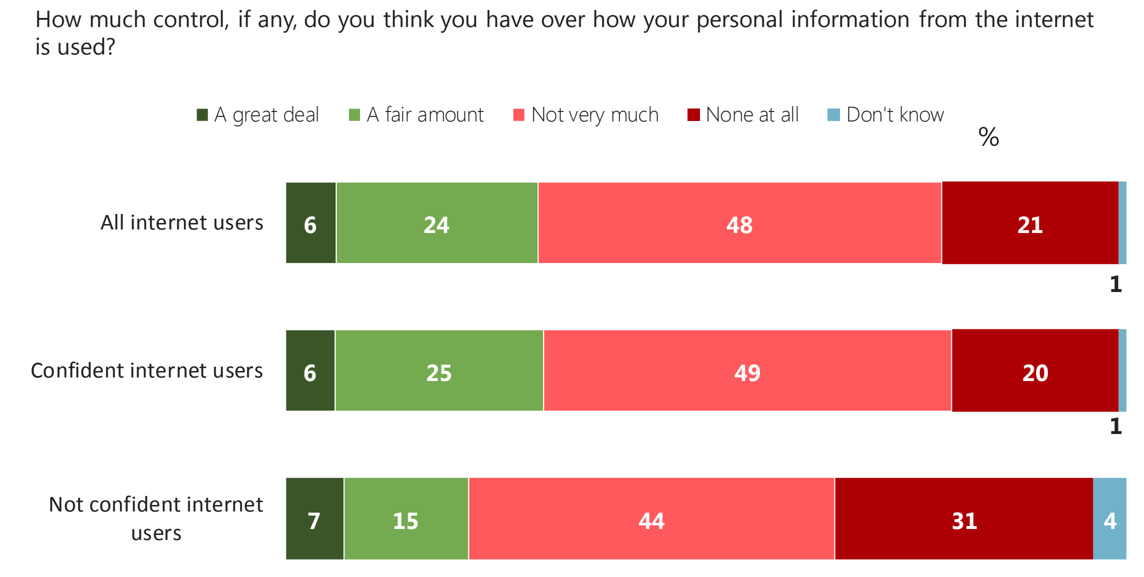
This chapter explores how consumers deal with the risk to their personal data online, and what methods they use to counteract these risks on the internet. The research finds people generally show a sense of disempowerment when it comes to protecting their personal information online, particularly amongst the less confident internet users. Many feel it is difficult to have total control over all the data they provide and consequently there are 'trust' issues when going online. As a result, some users have developed coping mechanisms, ranging from using security software to limiting their online activities.

5.1 Perceptions of control over personal information

The high level of concern over privacy is matched by a feeling of a lack of control – seven in ten say they do not have much control over what happens to their personal information online. The in-depth interviews suggest that the only real control some feel they have is to choose whether or not to enter information or visit a website in the first place, but that once data is in the hands of the company or online organisation control is lost.

The survey asked internet users how much control they think they have over how their personal information from the internet is used. Three in ten (30%) internet users said they did have control over their personal information on the internet, whereas nearly seven in ten (69%) feel they have little or no control. While a majority felt they had little control there was some variation between internet confidence levels. Three in ten (31%) of those who feel they have confidence in using the internet said they either had a great deal or a fair amount of control over their personal information compared with 22% of those with little or no confidence.

Figure 5.1: Internet user perceptions of control over personal information



Base: Internet users; 1,155 adults

The proportion of those who said they have no control is also strongly correlated with age. 16% of 15-24 year olds said they have no control at all over their personal information, compared with a third (32%) of those aged between 65 and 74, and 38% of those aged 75+.

The qualitative research adds some depth to this with some participants discussing how they feel they have complete control of their personal information up to a certain point, and after that point having no control at all. Specifically, they described having complete control of the first transfer of their personal information, for example inputting their information in to a website. In other words, they can control whether and which website to give their personal information to. They asserted that, until they submit personal information they are in control. However, once they have provided their personal information they have then relinquished all control, as they cannot influence what is done with the information once it is out of their hands.

> ***"Once you've entered that contract to let them use your data, you've lost control… you can do what you want with it… you can't call that company 6 months down the line and say give me my data back… your data has gone." (Male, 35-44, London, high confidence internet user)***

> ***"I'm actually really against that (companies sharing / selling his info) … that's where you get the most harassment, you have no control over the quality of company they are selling it to." (Male, 35-44, London, high confidence internet user).***

Some confident users however conceded that control is not a top of mind thought when using the internet.

> ***"90% of the time I'm on the internet I don't think about it [meaning control over personal information]" (Male, 25-34, Scotland, high confidence internet user)***

Less frequent and less confident users also felt that their control is limited to deciding when and when not to provide personal information. They felt less clear however in knowing when their information was actually being collected. They generally feel that they have fewer mechanisms to overcome this lack of control (described further on) than more frequent users, other than by reducing their internet use.

> ***"You have a lot of control, if you simply don't give it out. I think I have a lot of control over my personal data because I don't really do much on the internet. I don't have an email address and I never input any of my details anywhere" (Female, 45-54, Northern Ireland, low confidence internet user)***

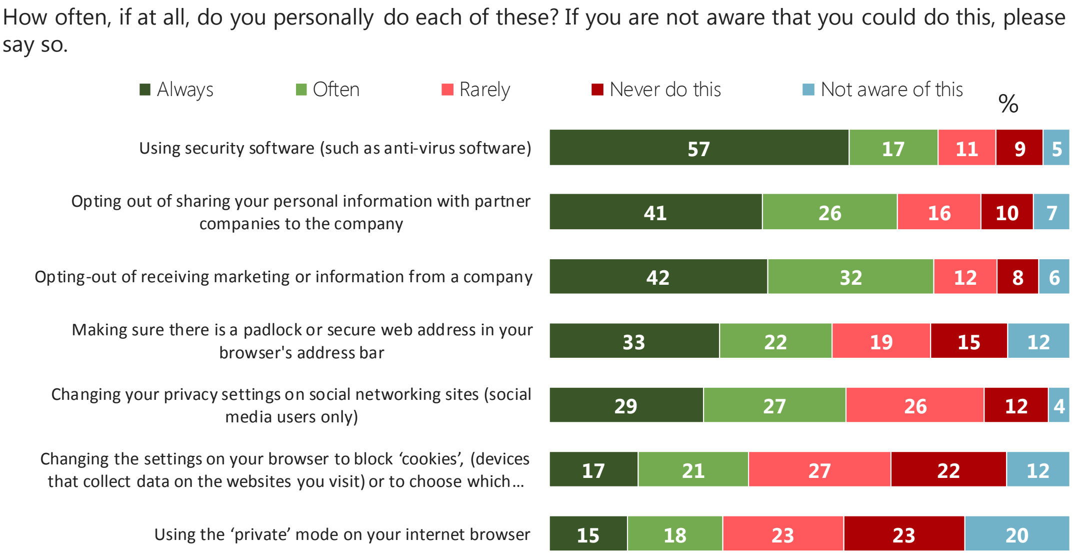
5.2 Consumer coping mechanisms for control

Online security software is the most popular coping mechanism for consumers to protect themselves online, by around three-quarters of internet users. This is followed by simply opting-out of marketing

information or data sharing (or even limiting internet use in the first place, especially among less confident users). Consumers are also aware that they have the ability to change their browser settings to delete cookies yet most do not often do so, despite the sense of unease that they can cause (perhaps because more regular users have got used to them). While confident internet users are more likely to delete their cookies nothing prompts or triggers them to do it.

In the survey internet users were presented with a list of various ways consumers can protect themselves while online and asked to identify how often, if at all, they do each of these. By far the most commonly cited method of internet protection was using security software, such as anti-virus software. Three quarters (74%) of internet users claimed they used some form of security software with 57% saying they always use security software, and a further 17% saying they often use security software.

Figure 5.2: Internet user frequency of different online protection methods



Base: Internet users; 1,155 adults

Other commonly cited security mechanisms included opting out of marketing information (74% claim to do this), opting out of sharing personal information with partner companies (66%), making sure there is a padlock or secure web address in the browser's address bar (54%), and changing privacy settings on social networking sites (56% - this was asked only to those with a social media account).

> *"Yeah I opt out when I can. It can often be a bit confusing though if you're doing it quickly. It should be a simple explanation with a simple tick box to opt-out" (Male, 15-24, Yorkshire and Humberside, high confidence internet user)*

Although awareness of these coping mechanisms was generally high, those aged 75+ showed the lowest awareness of these options. For example, 17% were not aware of the ability to opt-out of receiving marketing information, one in five (21%) were not aware of opting out of sharing personal information with other companies, and 35% were not aware of the secure web address padlock on web browsers.

The qualitative interviews indicated that some confident internet users to more likely look for the padlock although do not always remember to do so.

> ***"I forget to look for the padlock and did get caught once. I went on what I thought was the Adidas website and it turned out to be bogus. I bought two pairs of trainers that got impounded by customs…. So I did get caught out there, and fortunately I used my credit card there and the credit card company refunded me. Using credit cards helps with protection and PayPal." (Female, 55-64, Wales, high confidence internet user)***

Additional coping mechanisms came to light in the qualitative in-depth interviews. Some participants discussed choosing not to provide information about themselves when they had the option not to, or when it did not seem relevant towards a transaction. Respondents generally tended to avoid giving any information as much as they could, and when it became a necessity some would only proceed with trusted sources.

> ***"I trust the websites I go to honour that they'll use my data respectively [Discussing when he enters personal data on a website or opting out of marketing information]" (Male, 55-64, North-west England, high confidence internet user)***

Low confident users often discussed limiting what websites they visited or how they connect online. Often staying within the confines of trusted brands or only using connections that they perceived as being safe and secure (such as their home broadband connection) was an important coping mechanism for them.

> ***"I won't go on a site I don't know… I never buy off eBay…. Only visit Thomson's and Argos the big names (I know)." (Male, 65-74, North-west England, low confidence internet user).***

> ***"I bank online… but only ever when I'm at home… I know it's safe here (at home) … and only on my PC… not on my iPad." (Male, 65-74, North-west England, low confidence internet user).***

One highly confident respondent managed to get around the problem of being asked for information from untrusted sources by simply providing old or false email addresses, or giving inaccurate or misleading information about him. However, when directly asked no other respondents admitted to using false information.

As discussed in the previous chapter cookies tend to be seen by consumers as more "sneaky" than actively malicious. Nonetheless some internet users have different ways of limiting the accessibility of their personal information through cookies. As shown in figure 5.2, 38% of respondents said that they often would change the settings in their browser to block cookies, 27% said they rarely change their cookies settings, and 22% said that they never do it. A further 12% said that they were not aware of setting browser settings.

Older respondents were less likely to block cookies and more likely to be unaware of this capability than younger age groups. Two in five (41%) respondents aged 75+ said that they never set their cookie settings and a further 36% had no awareness that they could change their cookie settings (compared to just 9% of 15-24 year olds).

Levels of confidence had some bearing on how often users said that they changed their browser settings to block cookies. Three in ten (30%) internet users with high confidence said that they changed their browser settings always or often, in contrast to 25% of users with low confidence. While these figures are not far apart the largest difference was in relation to users' awareness of cookie settings. While one in ten (10%) confident users is not aware of cookie settings, the number jumps to 28% amongst internet users who were not confident.

While cookies were not a top of mind concern for low confidence users, when they were explained cookies were met with a degree of suspicion (as noted in the previous chapter). Some low confidence users saw cookies as an inevitability when going online, and while they thought that ways existed to avoid using cookies, they did not know how to do this themselves.

> ***"You have to accept cookies when going on websites…. They will store information (about you) …. I live with it… I don't know how to avoid it…. When people know what you've been looking at… I accept it…. I don't know how to stop it… "(Male, 65-74, North-west England, low confidence internet user)***

Older users with low confidence often get around their lack of confidence and knowledge on cookies by relying on family and friends to give them advice or actively manage their cookie settings.

> ***"If you clear your cookies all your information is gone… it helps clear your computer, the computer slows down… my son goes through the history (for me) … and clears it (every now and then)." (Male, 65-74, North-west England, low confidence internet user)***

High confidence internet users had a better ability in knowing how to control cookies via the use of their browser settings than low confident users. However, despite knowing how to do this there was nothing that appeared to trigger them to delete their cookies or change their settings. This was done on a more habitual basis by simply deleting them when they have realised they had not done so in some time.

> ***"Nothing really triggers me to delete them [cookies]. I usually just figure I haven't done it in a while so that's the point when I go into my web browser and delete them" (Male, 15-24, Yorkshire and Humberside, high confidence internet user)***

5.3 Where consumers feel safe while online

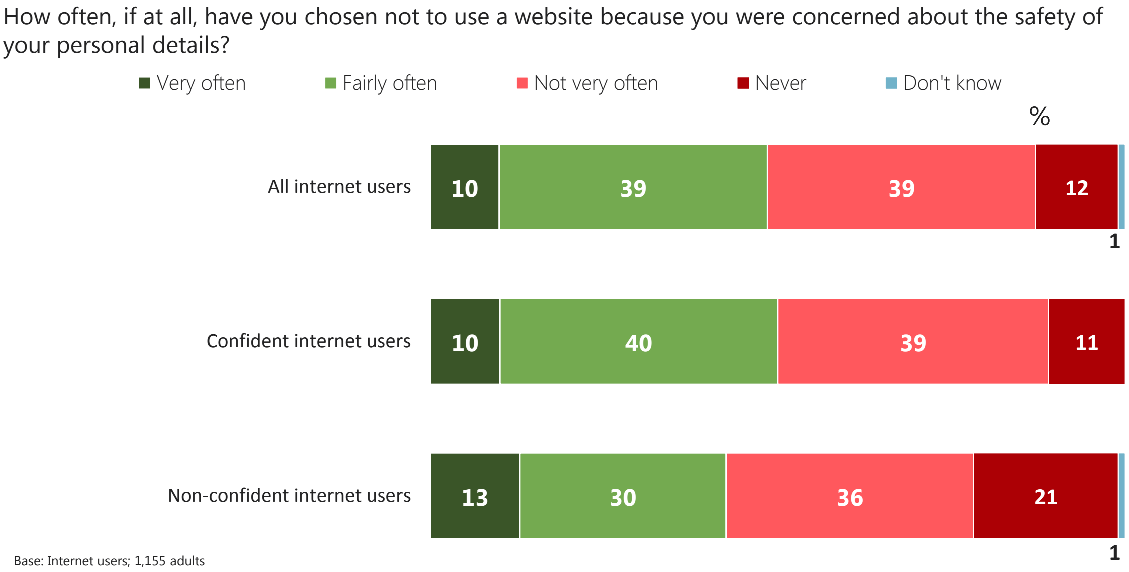
Trust is an important driver in online behaviour, especially as many internet users feel they do not have much direct control over what happens to their personal information. Related to this, half of internet users

say at some point they have chosen not to visit a website because of concerns about the security of their personal information (especially high amongst those more concerned about privacy).

As discussed earlier in this report, in order to navigate the digital data landscape, it was common practice, particularly amongst the less confident (often older) internet users to restrict their internet usage to only visiting "safe places", i.e. recognised brands or websites they trust. There was sometimes a sense of 'overlooking' the fact that these brands/websites must use their data, deliberately deciding not to think about it and instead placing their faith that these trusted brands will use their data responsibly.

Within the survey internet users were asked how often, if at all, they choose not to visit a website because they were concerned about the safety of their personal details. Just under half (48%) of those surveyed said that they either very or fairly often choose not to use a website because they were concerned. Furthermore, over half (54%) of those who had indicated a general concern about privacy online had avoided websites in this way, compared to 37% of people who were less concerned.

Figure 5.3: Frequency internet users choose not to visit a website because they were concerned about their personal information



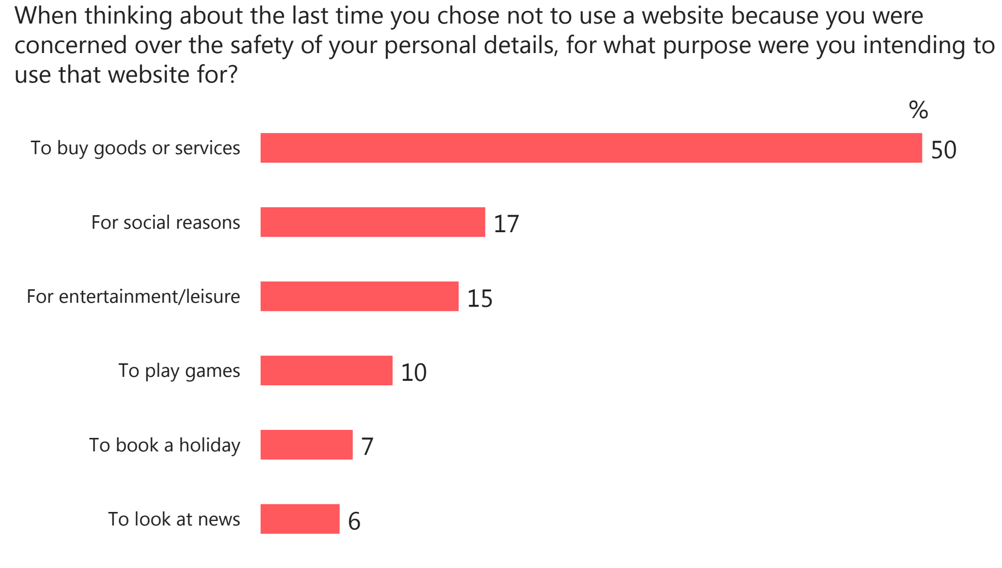
Base: Internet users; 1,155 adults

There was only a small difference between internet confidence levels when it came to deciding not to visit a website out of concern. Half (50%) of confident internet users said that they often do not visit a website out of concern compared to 43% of less confident users.

There were some differences between educational attainment level when it came to deciding not to visit a website. Those with a degree were less likely to say that they have not visited a website due to concerns about the safety of their personal information than those with no qualifications. Two in five (41%) of those with a degree said that they often do not visit a website out of concern. This compares to half (51%) of those without a qualification who said they often do not visit a website out of concern.

When asked about the last time they decided not to visit a specific website, regarding what purpose they were intending to use it, half (50%) said they had intended to use it for buying goods or services reflecting concerns about conducting transactions online. Other kinds of websites that people mentioned avoiding included social reasons (17%), entertainment/leisure (15%), to play games (10%), to book a holiday (7%), and to look at news (6%).

Figure 5.4: Type of website chosen not to visit because of concern about safety of personal information



Base: All those who have chosen not to use a website; 985 adults

When discussed in the qualitative interviews, high confidence users put their trust in companies that have a vested interest in keeping their information secure. Banking and well-known brands were trusted with personal data as there was a belief that these kinds of organisations would be more careful with personal data, as a breach in data would be harmful to their business.

> *"(I trust) The organisations I've already chosen to interact with…such as banks and credit card companies, because I've gone to them for business, we have a relationship and they have an inherent benefit from keeping my info secure and encouraging me to keep using their services… also government type sites in general… my perceptions are that … they will be more stringent and … adhere more closely to (security) regulations." (Male, 35-44, London, high confidence internet user).*

Conversely, free websites and lesser known brands were less trusted because they were seen as having less to lose if they mishandled people's data.

> *"Websites that I use most of the time for shopping, I check that they are reputable, I would never shop from a site I don't recognize, or put my card details into a site I don't recognize. If I'm booking travel, there are certain sites I will always use… if I use Booking.com I know booking.com is going to be fine…than go to random hotel sites…. It's different where I have a relationship with them already." (Female, 35-44, London, high confidence internet user)*

Some low confidence users similarly tend to stick to brands that they have an established relationship with. However, other low confidence users were resigned to the belief that there are no safe places online.

> ***"The firewall doesn't reassure me at all. You hear of people getting around firewalls… nothing is safe on the internet." (Male, 75+, Northern Ireland, low confidence internet user).***

5.4 Using security software

Those more confident using the internet are more likely to have security software than those who are less confident, with lack of knowledge the main barrier for those who do not have this protection. Usage seems to be split between free and paid-for software, with those who pay tending to be more satisfied than those who use free versions. Nevertheless, in the in-depth interviews some recognised that security software is only part of the solution, as their concerns about privacy extended further to what happens to their personal data after they have handed it over.

As noted earlier in Figure 5.2, 57% of consumers said they always use security software, with a further 17% saying they use it often, making it the main way for people to protect themselves online.

Concern about privacy appears to have a minimal effect on the use of security software, with 76% of those who are concerned about privacy using security software, and 73% of those who are not concerned also having security software. However, those with more confidence on the internet are more likely to have security software than those with less confidence (77% compared to 56% respectively).

Younger age groups also tend to use security software more than their older counterparts. 77% of 15-24 year olds and 83% of 25-34 year olds use security software, compared with 72% of 55-64 and 66% of 65-74 year olds.

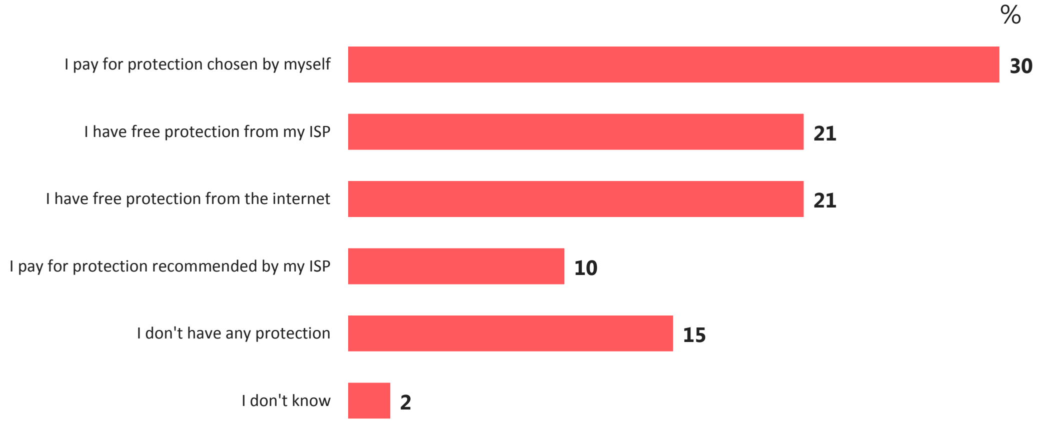
Overall there are differences between social grade and use of security software. Two in three (65%) of those within the AB social grade said that they always use security software compared with 44% of those within the DE social grade. Education attainment also showed some influence where 62% of those with a degree said they always use security software compared to two in five (41%) of those without a qualification.

There was some national variation within security software usage. The highest rate of use was seen in Wales and Scotland where two-thirds (67% and 65% respectively) of internet users said they always use security software. A similar level was also seen in Northern Ireland with 62% always using security software, while usage was lowest in England with 56% saying they always use it.

For those who stated that they did not use security software the main reason given was lack of knowledge on how to use it, mentioned by almost a quarter (23%) of those who do not have security software. A further 16% said that they did not know whether they have any security software at all, reinforcing that lack of knowledge is a key driver. Other reasons for not having security software included not being able to afford it (16%) and not thinking it would work (14%).

Figure 5.5: Types of security software protection used by internet users

When considering online security features, such as anti-virus software, spyware software, or firewalls, which of the following most applies to you?



Base: Internet users; 1,155 adults

Those who pay for security software are more likely to be satisfied with the level of protection that it provides. Eight in ten (82%) of those who pay for protection they chose themselves and 74% of those who pay for protection recommended by an Internet Service Provider (ISP) agree that the protection offered by their security software is sufficient. In comparison, only 55% of people who received free protection from their ISP and 59% of people who have a free service other than from their ISP say that they are satisfied with their level of protection.

In the qualitative interviews, across the sample, most claimed to have anti-virus software installed to help with security. Paid versions are seen as the most reliable, particularly amongst those with experience of having a virus.

> ***"I pay £50 a year to Norton, and I've stuck with them for 10 years. Though there is a possibility that if I looked in to it there might be free versions that do as good a job" (Male, 65-74, Northern Ireland, low confidence internet user)***
>
> ***"I use a paid subscription anti-virus software. I prefer the paid version because it has additional features, which I like. It's more in your face for example with warnings that the website you're accessing will use your personal data" (Male, 15-24, Yorkshire and Humberside, high confidence internet user)***

Less confident internet users tend to rely on others including their ISP provider, or family to install or update this type of software.

> ***"My son in law changed it all (updated his security software)." (Male, 75+, East of England, low confidence internet user).***

> *"My wife has just recently put some firewall or something on. She uses the computer she doesn't do online banking… we don't do anything other than use it for emails…." (Male, 65-74, Northern Ireland, low confidence internet user).*

However, it was mentioned by some participants that, while security software is important, it is not security software that is most important for protecting their personal information. These respondents did not see hacking and viruses as the main threat to personal data, and instead saw the problem as people legitimately giving their personal data, and then companies not using this data in a responsible way, or themselves being targeted by hackers.

> *"It's good and protects you [security software] from hacking but it doesn't really give you control when you give your data away [to companies]. Once it's out there it's out there. Better to be vigilant with what you sign up for" (Male, 35-44, North-west England, high confidence internet user)*

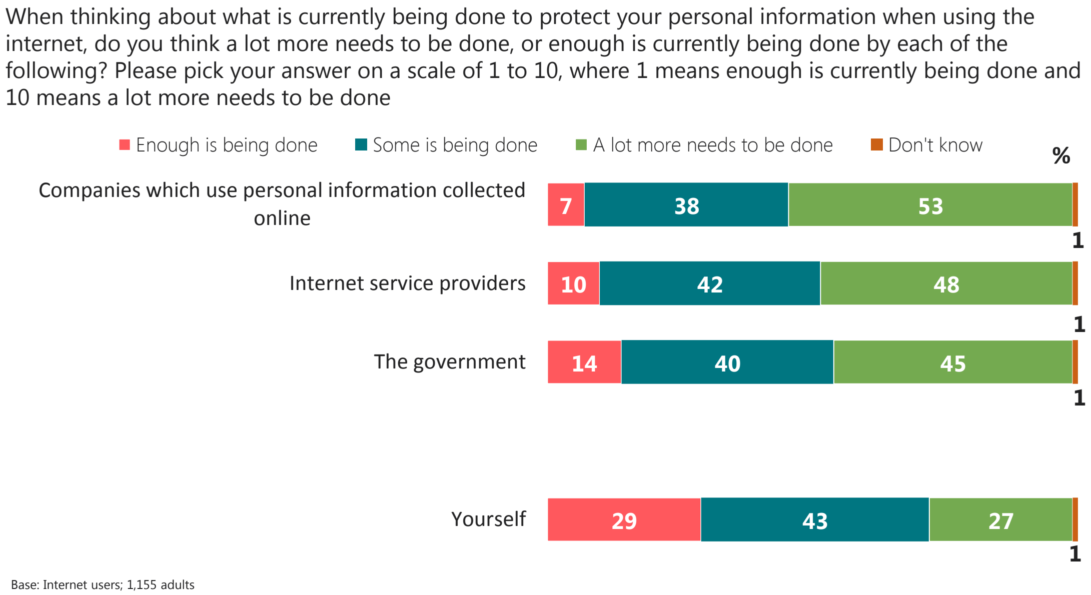
> *"It's not the lack of having security software that's the problem, the problem is after people legitimately give their personal information away and then companies not using it in a responsible way! (Male, 35-44, London, high confidence internet user)*

5.5 Who is responsible for protecting personal information?

Consumers are split on whether or not they feel they are doing enough to protect themselves online, but there is clearly a feeling that companies, Internet Service Providers (ISPs) and the government have a responsibility to be doing more. Around half of users (and more among older and less confident users) feel these bodies should do more to protect people's personal information.

Respondents were asked to rate various groups including themselves on whether more needs to be done to protect their privacy online or if there is enough being done already. Overall consumer opinion is split about what they are doing themselves. Only 29% believe that they are close to doing enough to protect themselves online (rating a score of 1-3), while 27% believe that they could do more (rating a score of 8-10). Belief that one is doing enough tends to increase with age. While only 22% of 15-24 year olds believe that they are doing enough to protect themselves, the number rises to 39% of 75+ year olds despite older users being more concerned about privacy in general. Those with a disability are also more likely to believe that they are doing enough when compared to those who are not disabled (37% vs 28%). Those who use the internet less than daily are more likely to say they are doing enough as well as not doing enough (i.e. at both extremes). More regular internet users tend to place themselves in the middle.

Figure 5.6: Internet user perceptions on how much is being done to protect consumers



Two in three (64%) internet users say that companies should do more to protect customers' personal information online. When looking at social grade the proportion of people believing this decreases between ABs and DEs. While 70% of people in grade AB shared this sentiment, only 54% of people in DE believe companies should do more. Additionally, the less internet confident users are more likely to believe that companies should do more. More than half (54%) of those with high internet confidence say companies should do more, but the proportion grows to 76% of people who have low internet confidence. Older people are also more likely to believe that companies are not doing enough. Two in three (66%) of those aged between 55 and 64 say companies should do more while two in five (40%) of 15-24 year olds say the same.

Three in five (59%) of those surveyed believe that ISPs need to do more to protect their users' data online. While this was said by half (51%) of 15-24 year olds, the proportion who believe that ISPs need to do more again increases with age, with 67% of 65-74s mentioning this. There is also a difference of opinion among more and less frequent internet users. Whereas 57% of users who use the internet more than once a day believe ISPs can do more, the proportion rises to 75% of users who go online less than once a day.

> ***"The government and Sky [her broadband provider] should be doing more to tell you about this [meaning companies collecting and using personal data]. They should just make it clearer for consumers that this is happening" (Female, 55-64, Scotland, low confidence internet user)***

Over half (55%) of people surveyed believe that the government needs to do more to help protect peoples' online data. Those in Scotland are more likely to believe that the government should do more with two in three (64%) stating this compared with 53% in Wales, 52% in Northern Ireland and 42% in England. Furthermore, the less that someone uses the internet, the more likely they are to believe that the government needs to do more. While 52% of users who access the internet more than once a day believe the government needs to do more, the number climbs to 63% of users who only use the internet once a day, and 73% who use it less than once a day. Users who have a disability are also more likely to believe that the government needs to do more than those who do not (67% vs 52%). Older consumers are more likely to believe that the government is not doing enough. Three in five (58%) of those aged 65-74 say the government is not doing enough compared with 38% of those aged 15-24. The findings show that there is a general pattern of less confident regular internet users saying that companies, ISPs and government should do more. They slightly stop short on this sentiment however when it comes to how much they can do themselves.

> ***"You have to be responsible for your own data don't you… I have no idea of who is responsible for doing something about companies who overstep the mark… there should be someone governing what they do and how they do it." (Male, 35-44, London, high confidence internet user).***
>
> ***"Penalise them (companies who take data without people knowing)!" (Male, 75+, London, low confidence internet user).***

Although most consumers are taking the steps to protect themselves while online most believe there is more to be done to better protect their personal information. There is a clear difference however between those who are confident using the internet and those who are not with confident users more likely to take the extra step in assuring they have security software while less confident users are more likely to limit their activities online.

The following chapter will conclude the report findings while also looking into two future aspects of internet use that are becoming more prominent by the day – paid websites and SMART products.

6 Looking towards the future of online security

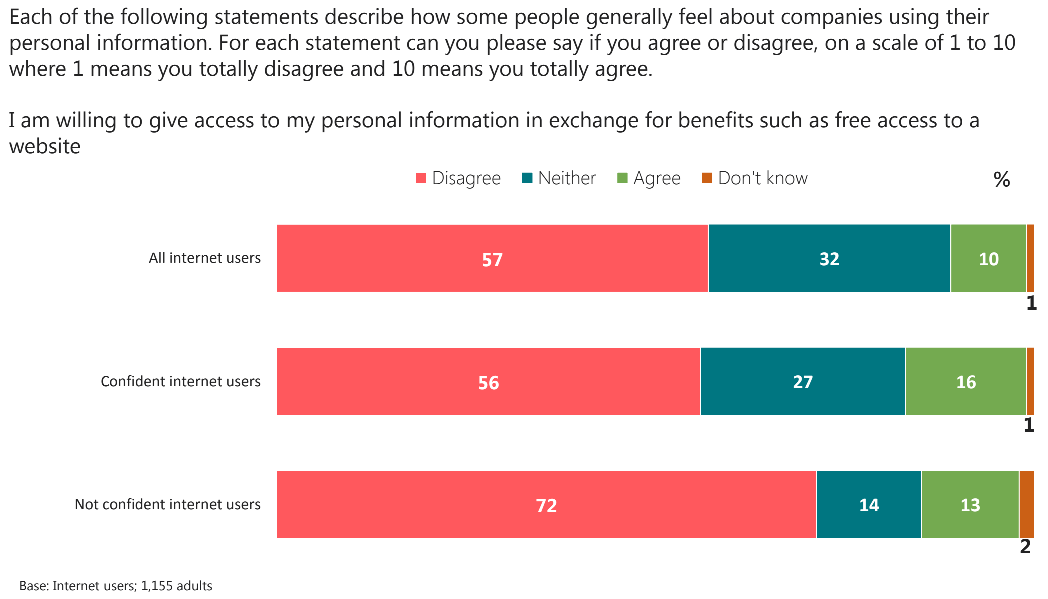
This chapter looks at consumer attitudes towards what the future may hold for the internet including consumer perceptions of the paid versus free website models as well as consumer thoughts on SMART products.

6.1 Paying for access to websites – a preferred model for the future?

Consumers say they are not willing to give access to their personal information in exchange for benefits such as free access to websites, although confident internet users are more likely to take part in this exchange than less confident users. This may be another example of consumers expressing a concern over privacy and what is done with their personal information that is not matched by their behaviour. Indeed, when pressed in the qualitative interviews, the stronger feeling was that people would rather continue with the free access model.

In the quantitative survey we found little support from internet users to give access to their personal information in exchange for benefits such as free access to a website. Just 16% agreed that they would be willing to give their personal information for such benefits while 57% disagreed.

Figure 6.1: Internet user willingness to give access to personal information in exchange for benefits



Each of the following statements describe how some people generally feel about companies using their personal information. For each statement can you please say if you agree or disagree, on a scale of 1 to 10 where 1 means you totally disagree and 10 means you totally agree.

I am willing to give access to my personal information in exchange for benefits such as free access to a website

Base: Internet users; 1,155 adults

Non-confident internet users were more likely to disagree with the concept of giving access to their personal data in exchange for benefits with 72% disagreeing compared with 56% of confident users. There was also some difference between those who protect themselves with paid security software and those that use free security software downloaded off the internet. One in five (21%) who use a free downloaded security software agree that they would be willing to give their personal information in exchange for free benefits compared with 13% who use a paid version.

Younger people were also more likely to be willing to exchange their personal information for free benefits. 23% of 15-24 year olds, 18% of 25-34 year olds and a quarter (25%) of 35-44 year olds agreed to the exchange compared with one in nine (11%) 45-54 year olds, 8% of 55-64 year olds and 3% of 65-74 year olds.

Social media account holders were also more likely to agree to allowing access to their personal information in exchange for free benefits than those without an account (18% vs. 10% respectively) while those with a disability were more likely to disagree to the exchange than those without a disability. Two in three (65%) with a disability disagreed compared with 55% of those without a disability. There is little evidence that this is also an age effect as the data show 63% of those with a disability and aged between 35 and 54 would not give their information in exchange for free benefits compared with 53% without a disability in the same age group.

The qualitative findings were somewhat contrary to what was found in the quantitative analysis. When directly asked if they would rather pay for website access without providing personal data or not pay but allow access to their personal data, most said that they would rather not pay and would be willing to provide access to their personal data.

> *"I'd prefer not paying for that website … but if it comes down to it, if some websites started charging and I could get the same service for free by selling my data I'd probably use that (free one) to be honest." (Male, 25-34, London, high confidence internet user)*

> *"I don't think companies should charge fees for us to visit their sites. I think in general there's an option for getting things for free, and people will put up with the adverts (for a free service)." (Female, 55-64, Wales, high confidence internet user)*

> *"I much prefer the paid website model as I'd prefer them not to use my personal info but I think the free 'use your info' model will be the way of the future. I prefer the paid version but think the free model is better for the masses. Some people don't have money for accessing websites and charging them would limit them to what they can do on the internet" (Male, 15-24, Yorkshire and Humberside, high confidence internet user"*

Despite consumers within the quantitative survey overwhelmingly saying that they would not give companies personal information in exchange for benefits the qualitative interviews show that when push comes to shove, consumers will still take the free website model over the paid website model. As one of the above respondents demonstrates, paying a fee could limit what many can do online.

6.2 Consumer perceptions on SMART products

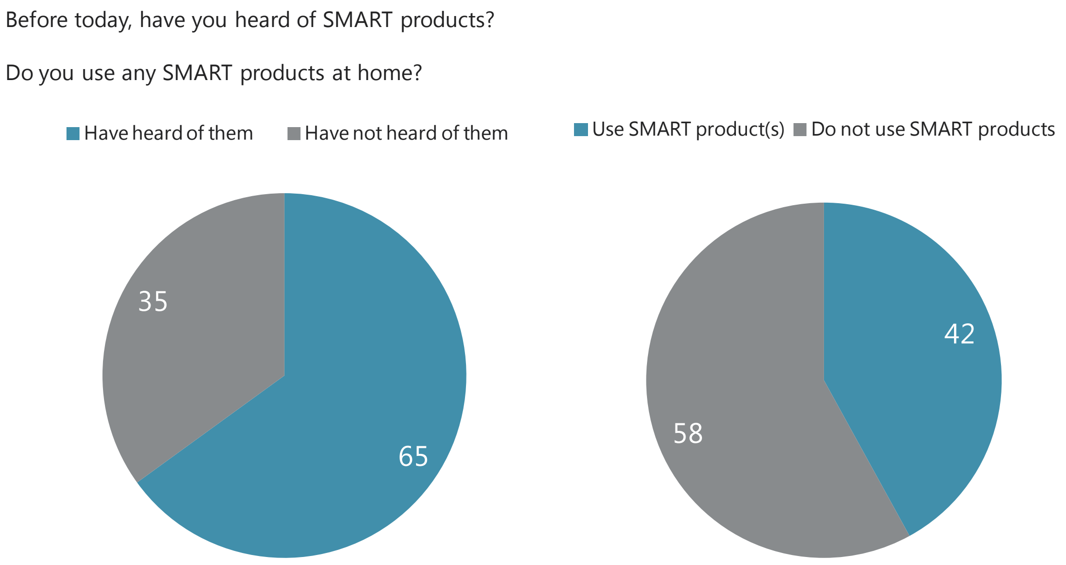
One of the changes to the marketplace since 2011 is the growth in 'SMART' products. Most consumers claim they have heard of SMART products although only a minority actually use them. Younger and more confident internet users are more likely to own a SMART product when compared with older and less

confident internet users. Given the lack of direct experience there are fewer spontaneous concerns expressed about them compared with the internet overall, but the ones there are tend to mainly be about privacy such as the product being hacked.

Many aspects of the internet have changed since the 2011 study including broadband penetration and overall internet use. Device technology has also changed including the more frequent use of SMART products – devices such as household appliances which have the capability to use the internet to communicate with other devices, the product manufacturer or managing company, as well as giving the consumer control over the product while away from home.

Both the quantitative survey and qualitative interviews explored consumer perceptions around this new technology and its relationship to privacy concerns over the use of personal data. The survey found that two-thirds (65%) of the public have heard about SMART products, with just a third (35%) not having heard of them. Those more confident using the internet were more likely to have heard of SMART products with seven in ten (71%) having heard of the technology compared with less than half (45%) of those less confident using the internet. There was also some age variation when considering which groups were familiar with SMART products. On average, 67% between 15 and 74 had heard of SMART products but just 46% of those over 75 had heard of them. Internet confidence explained much of this difference within this age group however with 84% of those aged 75+ and confident internet users having heard of SMART products compared with 30% of non-confident users aged 75+.

Figure 6.2: Consumer knowledge of and use of SMART products



Base: All; 1,1423 Adults; All who have heard of a SMART product; 846 adults

There were also differences between nations. Two-thirds (66%) of those within England had heard of SMART products as did 65% of those in Scotland and 63% of those in Northern Ireland. Less than half (46%) however in Wales had heard of SMART products.

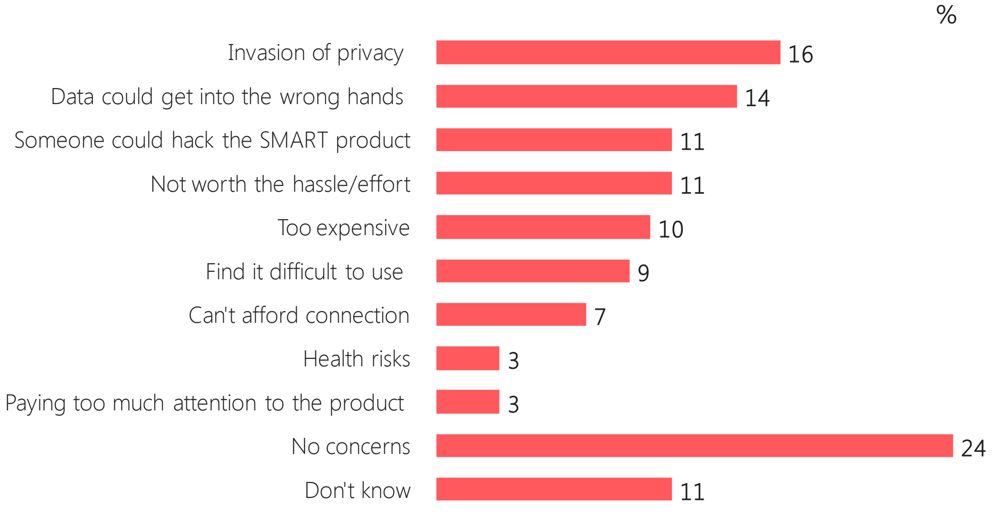
Although a majority of the public have heard about SMART products just 42% of these consumers actually use them. This equates to 28% of the general public. One in three (34%) confident internet users said that they have a SMART product compared with one in nine (11%) non-confident users.

Amongst those who have heard about SMART products, younger age groups were also more likely to use SMART products with 49% of 15-24 year olds, 55% of 25-34 year olds, 51% of 35-44 year olds, and 42% of 55-64 year olds saying they have a SMART product, compared with 26% of 65-74 and 14% of those aged 75+. One in five (21%) of those earning below £9,500 said they use SMART products compared with two in five (40%) earning between £9,500 and £17,500 and half (48%) of those earning above £40,000. Those with more education were also more likely to use SMART products where 42% of those with a GSCE, 44% with an A-level and 46% with a degree said they have a SMART product compared with three in ten (30%) without any educational qualification.

Both the quantitative survey and qualitative interviews asked consumers about the possible top of mind concerns around using SMART products. The survey found 16% saying invasion of privacy as a concern. Other concerns mentioned were someone hacking into the SMART product (11%), it being not worth the hassle or effort to use (11%), being too expensive (10%), and being difficult to use (9%). Nearly a quarter (24%) however said there were no concerns using SMART products while one in nine (11%) said they did not know of any.

Figure 6.3: Consumer concerns using SMART products

When thinking about using SMART products in general, what concerns, if any, do you have?



Base: All who have heard of a SMART product; 846 adults

Those within the AB social grade were more worried that someone could hack into a SMART product (mentioned by 14%) when compared with those within the DE social grade (mentioned by 6%). 16% of those without a qualification said that they found SMART products difficult to understand compared to 11% with a GCSE and 5% with a degree. 14% of those with a disability said that they found them difficult to understand compared with 8% without a disability.

Although there was little difference between those with and without confidence using the internet, one in five (20%) of those who said they were concerned about privacy online overall also said they were concerned about privacy using a SMART product. This compares with 8% of those who were not concerned about their privacy overall online. Interestingly there was no difference between these two groups when actually using SMART products. 44% of those concerned about their privacy online said they used a SMART product compared with two in five (40%) who were not concerned.

The qualitative interviews established similar findings to the survey. Less confident internet users found it more difficult to understand the risks and benefits of SMART products while more confident users were positive towards their value. Confident internet users tended not to mind that companies could collect information about them through SMART products, as they assume this was happening anyway (for example they must eventually tell energy companies the amount of gas and electricity they use). Most respondents thought the primary risk of SMART products related to hackers (or a rogue employee of the energy company) gaining access to their home by knowing when they may or may not be present. This concern was mentioned when probed however and did not outweigh the perceived benefits of SMART products

> ***"I think they sound like a nice thing to have but I don't have the confidence to use one. I wouldn't care if a company knew I was using their product I suppose" (Female, 55-64, Northern Ireland, low confidence internet user)***
>
> ***"I have a SMART meter and there isn't much a company can know about me other than when I have the gas on or off. I guess a risk of having them (SMART products) could be that they're open up for abuse if not monitored, for example being hacked and someone can turn your lights on or off" (Male, 35-54, North-west England, high confidence internet user)***
>
> ***"It's nothing they (companies) can't find out already so I don't think this represents any risk." (Female, 35-44, London, high confidence internet user)***
>
> ***"We've had a SMART meter for two to three years. They're smart because they make it out that it saves you money when really it just makes them or saves them money. But one risk I can think of is if you're away from home and if that information got out it could cause problems, for example dishonest employees can get a hold of it" (Female, 75+, Yorkshire and Humberside, low confidence internet user)***

Overall there was a general positive sense from respondents that SMART products can make life easier while things like energy use can become more efficient as a result. Others felt suspicious about companies who use SMART products as they were surely a new way for companies to make a profit. There was an overall sense however that SMART products were the way of the future and will likely become more integrated into consumer lives.

6.3 Conclusions

What these final analyses show is that consumers are indeed thinking about the future for internet users and what this might mean for online privacy. Despite consumers saying that they would rather not give away personal information for free access to websites they would still prefer doing this over paying for access. This might be a more economically calculated decision after deeper thought on how paying for website access might limit their use of the internet.

In this report we find that consumers are concerned about the safety of their personal information when using the internet. There are large disparities within the public however towards awareness of how personal data is collected and used as well as how they go about protecting themselves online. Confidence using the internet is one of the biggest indicators explaining these differences. Those with a higher degree of internet confidence tend to be more aware of when their personal data is being used and why companies may want this information. They also have a clearer sense of what steps they need to take to protect themselves. This group tends to be younger and use the internet more frequently to perform multiple tasks. Less confident users still recognise that companies use their personal information, however they are less aware as to when it is collected. They also have fewer skills to protect themselves while online and often either rely on friends or family to help them or limit their internet use altogether. This group tends to be older, less frequent internet users and while they share concern about online privacy with confident internet users they tend to have a slightly higher degree of anxiety. Many however are satisfied within the limits of their internet use and do not feel the effort of learning more about is worth the time.

All internet users are concerned over how their personal information is used online. Although most prefer companies to not use their personal information if given the choice many do feel that they can live with companies using their data if done responsibly while being transparent with how the data is being used – even if this is for marketing purposes. Nearly all consumers however feel a sense of suspicion if companies sell their personal information to other companies. The research finds that 'trust' is a cornerstone in regards to how we use the internet with consumers also using pre-existing levels of trust as a proxy to decide whether to trust the website or not. For companies to gain consumer trust in a brand they need to adhere to three things:

- Be fully open about what data they collect/use and what they will do with it
- Provide consumers the opportunity to opt-out of any use of their data
- And, keep consumers' information safe and secure

This report is intended to inform policymakers and the wider public about consumer perceptions of online security. Consumers show that they are aware that much of that responsibility lies with the consumer but feel that companies must do more to earn public trust. This includes companies being transparent and educating consumers about what they do with their personal information.

Appendix 1: Reviewed Reports

Title	Organisation	Date	Link
Adults' media use and attitudes	Ofcom	May 2015	http://stakeholders.ofcom.org.uk/market-data-research/other/research-publications/adults/media-lit-10years/
Personal Data and Privacy	WIK-Consult, Ofcom	May 2015	http://stakeholders.ofcom.org.uk/internet/personal-data-and-privacy/
The Commercial Use of Consumer Data	Analysys Mason, DotEcon, Competition Markets Authority	June 2015	https://www.gov.uk/government/news/cma-publishes-findings-on-the-commercial-use-of-consumer-data
The trade-off fallacy: How markets are misrepresenting American consumers and opening them up to exploitation	Annenberg School for Communication, University of Pennsylvania	June 2015	https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf
Trust in Personal Data: A UK review	Catapult Digital	July 2015	http://www.digitalcatapultcentre.org.uk/wp-content/uploads/2015/07/Trust-in-Personal-Data-A-UK-Review.pdf
The Deloitte Consumer Review Consumer data under attack: The growing threat of cyber crime	Deloitte	2015	https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/consumer-business/deloitte-uk-consumer-review-nov-2015.pdf
Personalisation versus privacy	Ipsos MORI, KCL	February 2014	http://www.ipsosglobaltrends.com/personalisation-vs-privacy.html
Apps Environment	Kantar Media, Ofcom	March 2014	http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/Apps_Environment.pdf?utm_source=updates&utm_medium=email&utm_campaign=apps-report
Public attitudes to the use and sharing of peoples' data	Ipsos MORI, Royal Statistical Society	July 2014	https://www.ipsos-mori.com/researchpublications/researcharchive/3422/New-research-finds-data-trust-deficit-with-lessons-for-policymakers.aspx
Dialogue on Data	Ipsos MORI, Economic & Social Research Council, Office for National Statistics	2014	https://www.ipsos-mori.com/DownloadPublication/1652_sri-dialogue-on-data-2014.pdf

Recent research about consumer attitudes	Office of Fair Trading	May 2013	
Being online: an investigation of people's habits and attitudes	Ipsos MORI, Ofcom	June 2013	http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/being-online.pdf
The Data Dialogue	Populus, Demos	2012	http://www.demos.co.uk/files/The_Data_Dialogue.pdf
Online personal data: The consumer perspective	Communications Consumer Panel	May 2011	http://www.communicationsconsumerpanel.org.uk/online-personal-data/online-personal-data-1
Eurobarometer Flash Survey 359	European Commission	June 2011	http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf
Information technology and data privacy	Eurobarometer 46.1	January 1997	http://ec.europa.eu/public_opinion/archives/ebs/ebs_109_en.pdf

Gideon Skinner
Research Director
Gideon.Skinner@ipsos.com

Glenn Gottfried
Research Manager
Glenn.Gottfried@ipsos.com

Connor Leckey
Research Assistant
Connor.Leckey@ipsos.com

For more information

3 Thomas More Square
London
E1W 1YW

t: +44 (0)20 3059 5000

www.ipsos-mori.com
http://twitter.com/IpsosMORI

About Ipsos MORI's Social Research Institute