

COMMUNICATIONS
CONSUMER
PANEL



Online personal data: the consumer perspective

Communications Consumer Panel research report

May 2011

Contents

- Introduction..... 2
- Executive summary 3
- 1. The online offer and the use of personal data 8
- 2. Benefits and risks for consumers 12
- 3. Consumers’ views 17
- 4. Implications of the research findings 36

Introduction

Almost three-quarters (74%) of the UK population now have broadband at home and consumers have access to a vast range of online services and applications¹. Many of these are free at the point of use, but they are often funded indirectly by the data that consumers provide about themselves and the websites they visit.

Consumers generate personal data every time they go online. Sometimes they knowingly provide it to third parties - but sometimes without realising. Even where consumers know that they are supplying personal data, they generally do not realise that they are part of a lucrative and complex value chain, an online information industry.

For consumers, providing personal data can have significant benefits in the form of services and applications that are more tailored to their needs, or that they might otherwise have to pay for. But there are also risks - that consumers disclose personal information without understanding how it is used or by whom, that data are misused, and that the law does not keep pace with industry developments or consumers' expectations.

The issue of online privacy and data management has been the subject of much debate in recent years - and many stakeholders are actively considering what the appropriate responses should be. We hope that this report will stimulate further debate of these issues, taking into account what consumers and citizens need and expect from the management of data and their privacy.

We have made suggestions in this report about how to protect the interests of consumers and citizens. This is an ongoing debate and we look forward to discussing with those expert stakeholders in this field how best to ensure that these conditions are fulfilled. In doing so, we want to ensure that consumers can make an informed decision about sharing their personal data online and maintain the levels of privacy with which they are comfortable.

Bob Warner
Acting Chair, Communications Consumer Panel

¹Ofcom Technology Tracker, Wave 1 2011

http://www.ofcom.org.uk/static/marketresearch/statistics/main_set.pdf

Executive summary

Supplying personal data online

Three-quarters of the UK population now have broadband at home², using the internet to share their thoughts, ideas and information, and UK consumers conduct more transactions online, and spend more than consumers in any other major European country³. For them, providing personal data can have significant benefits in the form of services and applications that are more tailored to their needs, or that they might otherwise have to pay for. But there are also risks - that consumers disclose personal information without understanding how it is used or by whom, that data are misused, and that the law does not keep pace with industry developments or consumers' expectations.

A lack of trust and understanding among users could become a barrier to the continued development of innovative services and applications, and the benefits for consumers that they bring.

How concerned are consumers about data gathering? And what steps, if any, do they take to exercise control over the collection of their data?

Consumers' views

Against this backdrop, the Panel decided to carry out quantitative and qualitative research with consumers to understand:

- the extent to which consumers are aware of the various methods of collecting data in the online environment;
- the extent to which consumers are prepared to share their own data and what they expect in return;
- consumer awareness of ways in which they can protect their online data, and their use of such methods;
- among those using a social networking site, their use of privacy settings and understanding of how personal data on such sites can be accessed and used by third parties; and

²http://www.ofcom.org.uk/static/marketresearch/statistics/main_set.pdf

³See Ofcom's International Communications Market Report 2010 (ICMR), p217 http://stakeholders.ofcom.org.uk/binaries/research/cmr/753567/icmr/ICMR_2010.pdf

Online personal data: the consumer perspective

- attitudes towards what is currently being done to protect personal online data.

Just over half (52%) of UK internet users have no top-of-mind concerns when using the internet. The largest top-of-mind concern related to safety of personal details/ID theft -26% of respondents said spontaneously that they were concerned about these issues, followed by 'privacy issues' (14%). When prompted, six in ten consumers said they were concerned about privacy online. Just over one in four of those who use the internet on their mobile phone were more concerned about privacy when using their mobile phone than when using a PC, laptop or tablet.

Consumers can only take responsibility if they know how their data are being used online. There was a high level of awareness that companies collect customers' personal information by asking them to register details with them, and choosing to opt in or out of receiving marketing information (85%), but there was less awareness of passive methods used by companies to collect information. Sixty-four per cent of consumers were aware that cookies are used to collect data about the websites they visit; 59% were aware that companies can gather information from personal profiles on social networking websites (rising to 68% of internet users with a social networking profile); and 45% were aware that mobile phone apps can also collect personal information. Awareness was higher among those who use the internet on their mobile phone (53%).

Consumers also need to understand the benefits of sharing their personal data. Otherwise they will not be able to make an informed decision between, on the one hand, withholding their data and protecting their privacy, and on the other hand, sharing their data and receiving benefits. The research findings suggest that the decisions consumers make might be influenced by how direct they perceive the benefits to be. Only a small minority of respondents were always happy for the methods of data collection we asked about to be used for any reason. In general, younger age groups were more relaxed about this. Respondents were slightly more comfortable if their data was collected as a result of registering with a company or by accepting cookies if this was from a company/brand they trusted. But neither receiving discounts/special offers nor relevant adverts/information increased people's comfort with these methods.

Levels of concern were lower if the personal information was being used by companies to develop new business and services (31% had a high level of concern) than if it was being sold to third parties for them to target the consumer with products/services (here, 79% had a high level of concern).

Online personal data: the consumer perspective

Respondents had relatively high levels of awareness of the types of methods that could be used to protect their information online, although those surveyed were more aware of reactive methods (e.g. opting out of marketing (83%) or reading a company's terms and conditions (78%)) rather than proactive means (e.g. blocking cookies(68%) to protect their personal details. However, use of these methods varied significantly. Again, reactive methods were used much more - 73% of internet users said they regularly opted out of receiving marketing/information from companies and 69% regularly opted out of sharing information with partner companies of the one they were interacting with. And looking at more proactive methods, 50% of respondents said they regularly read companies' privacy statements to inform their judgements, and 43% said they changed the cookies setting on their browser.

Those surveyed were more comfortable about their data being used when they had control over whether this happened, and knew how the data would be used. Sharing financial information such as bank details, information from social networking sites and mobile numbers were the causes of most concern. Nearly nine in ten were highly concerned about providing, or companies being able to collect, credit card or debit card details.

The majority of social networking site users said they used privacy settings, and understood that if privacy settings are not set to 'private', anyone is able to access their information. However, 16% were not aware that information on open profiles could be seen by anyone, including companies, and 27% were not aware that this information could be used as the basis of targeted advertising. Nearly two-thirds (64%) of social network users said that they had a high level of concern about the use of information from profiles by companies.

While 12% of respondents felt that enough was currently being done to protect their information online, 22% were unaware of what was being done. Sixty-six percent of internet users felt more should be done to protect their personal information on the internet.

Twenty-one per cent of people felt that it was solely their own responsibility to look after their data, while 17% felt this responsibility should be shared with the companies collecting the information, the government and an independent organisation.

The qualitative research explored participants' views about the provision of data to companies, both offline and online. When asked directly, people thought there was not much difference between the loyalty cards in shops and use of data online, but there was something about the human touch that made a difference. Personally handing over the card to someone seems to give people a greater sense of

Online personal data: the consumer perspective

trust/control than online, where the exchange of data is happening in the background, often automatically and out of sight.

Participants in the research commented:

“It’s basically the same, but with a card you actually get to speak to someone whereas on the internet you give it to a server. But the information they collect is the same. I would say it was the same but I do prefer it when it comes from a person and not just through my laptop. There’s nothing wrong with it happening online but it’s just my opinion that I like the human touch.” (Male, 35-44 years old, Edinburgh)

“I suppose realistically when you think about it they’re the same. In fact the loyalty cards are probably worse because they collect more information about you. I haven’t thought about it before but they are similar....I tend not to think about how they use my information. I tend to think about how they use my information online more than through the cards though. That’s because there’s potentially more people who can access the information. I feel that with the card it should be protected better but I’m under no illusions, I know that that information is also stored on a computer somewhere.” (Male, 35-44 years old, Halifax)

The qualitative research also echoed the range of views found in the quantitative study:

- ***“Normally when I am on these sites I won’t click on the adverts to see what they are offering. But I am happy for them to use my information to tailor the ads.” (Female, 45-55 years old, Merseyside)***
- ***““It depends, if they are going to send me offers that I’ll be interested in like discounts or new things that they have then it’s better that they have my details so they can send them to me.” (Male, 16-24 years old, Leicester)***
- ***“I hate when you can’t get to a certain page without opting in or registering. I don’t like not knowing what they want my information for, especially if it is not a website that I am familiar with.” (Male, 35-44 years old, Edinburgh)***
- ***“I don’t mind so much if one company has a piece of information but it’s when they start joining it together that I don’t like it. Even if they ask for your permission it’s the principle that bothers me.” (Male, 35-44 years old, Birmingham)***
- ***“No, I didn’t know about this. I don’t think it is ok for companies to do this. If I haven’t clicked an option then I don’t want this to happen. There isn’t really a reason why I don’t want it, but if I was just minding my own business there is no reason for them to be targeting me with adverts.” (Male, 16-24 years old, Walsall)***

Conclusions

The report is intended to inform policymakers, as they develop solutions, policies, and potential laws governing privacy, and to guide and motivate industry as it develops more robust and effective best practice and self-regulatory guidelines.

Online personal data: the consumer perspective

Consumers can only take responsibility if they know how their data are being collected and processed online. The Panel considers that companies should improve consumers' awareness of how their data are collected and used, and provide straightforward information for consumers.

In summary, the Panel considers that consumers will only be genuinely empowered if they have:

1. information to allow them to make an informed decision about the implications of releasing their data;
2. control over the use of their data;
3. reassurance that companies will always minimise the amount of data that they collect, store it securely, retain it for no longer than is necessary and consider whether to check with consumers after a set period of time whether they still wish their data to be retained; and
4. confidence that companies will follow the rules and manage personal data responsibly, and that if they do not, they will face robust enforcement action.

The Panel looks forward to discussing with stakeholders how best to ensure that these conditions are fulfilled. In doing so, we want to ensure that consumers can make an informed decision about sharing their personal data online and maintain the levels of privacy with which they are comfortable.

1. The online offer and the use of personal data

The internet plays an integral role in many people's lives. Consumers can use a vast number of online services and applications, with new ones developing all the time. Increasingly, public services are also being delivered online. In examining how personal data are collected and used online, it is important to take into account the benefits which the internet offers - for individual consumers and for society at large.

The internet has improved the efficiency of services such as shopping, searching for services and communication. It has also created new services, such as photo-sharing and music downloading. UK consumers have enthusiastically adopted online shopping, conducting more transactions online, and spending more, than consumers in any other major European country⁴.

Unlike traditional media such as television and radio, the internet is a two-way medium. People are not just consuming online content and conducting transactions. They are sharing thoughts, opinions and information too - and UK consumers have been quick to move onto social networking services, with 62 per cent of internet users having at least one social networking profile in October 2010⁵. This number has grown from a very small base in a relatively short period of time - membership of Facebook was opened to the general public in 2006. By November 2010 it had an estimated 26.3million UK visitors⁶.

The UK is increasingly an 'always online' culture, a trend which is accelerating with the dramatic rise in the use of mobile phones to access the internet. Technological and design developments mean that mobile phones now provide a convenient way of using the internet on the move. Consumers can use smartphones to access many

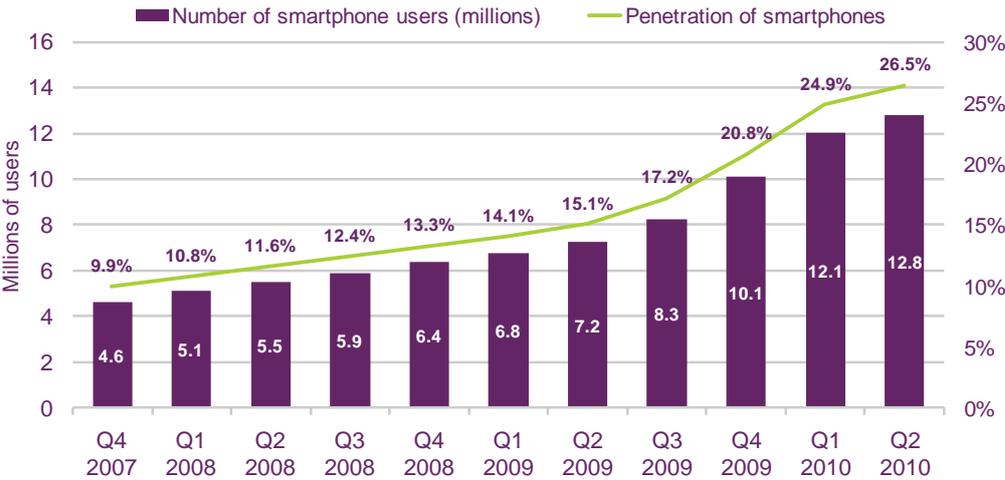
⁴See Ofcom's *International Communications Market Report 2010* (ICMR), p217 http://stakeholders.ofcom.org.uk/binaries/research/cmr/753567/icmr/ICMR_2010.pdf

⁵ See Ofcom's *International Communications Market Report 2010* (ICMR), p238: http://stakeholders.ofcom.org.uk/binaries/research/cmr/753567/icmr/ICMR_2010.pdf

⁶ The site was launched in 2004. Before 2006 it was restricted to academic institutions. See <http://www.facebook.com/press/info.php?timeline> for a timeline.

of the services and applications they are accustomed to using via personal computers, as well as new ones that use the internet in innovative ways. Smartphone applications use data about where someone is to provide them with information about services available nearby, such as restaurants or hotels. Figure 1 shows how quickly the number of smartphone users has increased, almost trebling in less than three years.

Figure 1: Use of smartphones in the UK



Source: ComScore, Mobilens, Dec 2007- May 2010, in Ofcom’s *Communications Market* report (CMR) 2010 Fig 5,19.

But not everyone is experiencing the benefits of the services that the internet can bring. In particular, certain groups of consumers, such as older and disabled people, are less likely to be online and, if they are, are less likely to be using online services and applications to the same extent⁷.

Enabling consumers to manage their personal data effectively is important, both to encourage wider digital participation, and to promote e-commerce and continued innovation.

Online advertising

A significant feature of the online world is just how cost-effective and easy it is for companies to collect personal data and convert it into valuable information. Personal data are also collected offline and used by companies - for example to

⁷ <http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/digi-participation/2010-metrics/metrics-bulletin-2010.pdf>

Online personal data: the consumer perspective

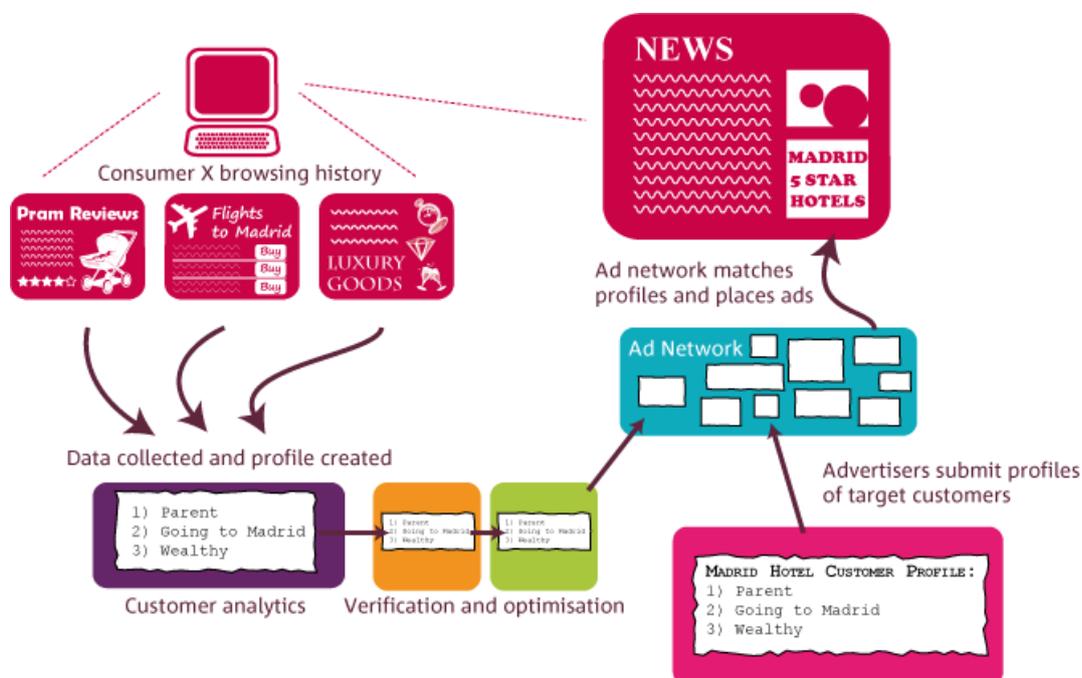
carry out marketing activity. But data available online enables advertising and services to be tailored much more rapidly and precisely to individual interests.

Personal data plays an important role in the online advertising industry. In the UK the online advertising market made up 26% (£4.1bn) of the £15.7bn overall advertising market.⁸ It is now the second biggest source of advertising revenue after TV, overtaking traditional media such as newspapers and radio. Internet advertising constitutes a larger share of the overall advertising mix in the UK than in any other country Ofcom looked at in its *International Communications Market Report 2010*⁹.

Advertisers can also use consumers' personal data to filter the online audience and find people they think are most likely to want their products. This 'targeted advertising' is much more cost-effective than ordinary display advertising. One variant is 'behaviourally targeted adverts' (BTAs).

Figure 2 provides an illustration of how personal data can be collected and used online. It shows how details of the websites that a consumer visits can be collected and used to develop a profile of that particular person. This can then be used to supply adverts for products or services that he or she is likely to be interested in.

Figure 2: Targeting adverts using data about websites visited



⁸Advertising Association/Warc Expenditure

⁹ See Ofcom's International Communications Market Review (ICMR), p 24

http://stakeholders.ofcom.org.uk/binaries/research/cmr/753567/icmr/ICMR_2010.pdf

Targeted advertising is proving to be an effective means for advertisers to reach potential customers. A 2010 study by the Network Advertising Initiative (NAI) stated that BTAs were clicked on 670% more often than ordinary display adverts, presumably because they were more relevant to users' tastes and wants¹⁰. This study also found that, in terms of conversion rates, (the percentage of people who acted on an advert), BTAs were 2.4 times more effective than regular adverts. BTAs attract a premium, but despite the difference in price, they are cost-effective for advertisers.

¹⁰ Network Advertising Initiative http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf

2. Benefits and risks for consumers

Companies clearly benefit from being able to gather and process personal data, and there are also benefits for consumers. In this section we examine the benefits in more detail. We then examine the risks which consumers may face.

Consumer benefits

One of the main benefits for consumers of companies collecting personal data is that it helps to keep content free at the point of use. Free content has underpinned the internet's success and enabled it to grow quickly. Although it is not strictly true to call online content 'free', since so much of it is paid for through advertising revenue, the absence of up-front costs allows people to access much online content regardless of their individual circumstances. This is also quite often the case with smartphone applications; developers offer free, ad-supported versions of an application alongside the paid-for premium version without adverts (and usually with greater functionality).

As well as receiving more targeted advertising, consumers can benefit from more personalised recommendations and services. Some online businesses use data about their customers to send out targeted offers or recommendations. Examples include Amazon UK's email offers which are based on items the user has previously looked at on the main website, and Google's search engine can personalise search results based on how the user has previously responded to search results.

Other online businesses use personal information to create personalised services that rely on a regular process of feedback to improve them. Last.fm's personal 'radio' service learns users' musical preferences based on what they choose to listen to. It also finds more songs that the individual might like by looking at the profiles of other users with similar preferences.

So personal data helps to fund free content and deliver more personalised services. It is also the basis of the social networking phenomenon, which relies on the exchange of personal data. Users of these services gain more from them the more they are willing to share. For example, by submitting their tastes and preferences to Facebook (on top of basic demographic data) consumers can access news feeds

about brands, artists and events that they have told Facebook they are interested in by clicking the 'like' button. The news feeds can include behind-the-scenes news, special offers and exclusives. In return, the brands, artists and event organisers receive information on the people who 'like' them and can then connect with supporters in a way that increases loyalty towards them. Facebook says that the average user becomes a fan of four pages a month, while Inside Facebook reports Coke as currently the most 'liked' brand and Eminem the most 'liked' artist worldwide¹¹.

This system has expanded beyond the confines of the social networks themselves and is now incorporated in the wider web. Many websites allow users to indicate, via a 'like' button, to their social network that they are interested in a given news item or product webpage that is hosted externally. This increases their sense of connection to their wider social network and also means that they can receive tailored updates on the page in question if, for example, the news report is updated with new information or if a product drops in price. More than 2.5 million websites have integrated with Facebook in this way.

The latest wave of social network services show that, in some cases at least, consumers are willing to share more and more personal information, even when it is potentially sensitive. New services, such as 'Swipely', link to the user's credit card so that they can instantaneously share their buying behaviour with their peers to show what they bought and where from. The process of sharing this information, and the reaction to it, feeds back via the social network to various interested companies, including the retailer and other retailers of similar or complementary goods. The users enjoy recommendations from their peers and, potentially, incentives to participate more fully, for example by writing a review of their purchase. Other new social networks link to real-world data. 'Bump' tracks users' licence plate numbers in order to provide services linked to their location.

Smartphones also enable personal data to be used to provide innovative applications. Applications can use location-based data to provide information about services available nearby, such as restaurants or hotels.

So the ability of consumers to share, and for companies to gather, personal data online can provide substantial benefits and enable a richer sense of participation by fuelling the development of social networks.

¹¹ Correct as of May 2011. Source: <http://www.insidefacebook.com/2011/05/04/the-25-most-liked-pages-on-facebook-spring-2011/>

Consumer risks

Research carried out previously by the Panel shows that online privacy and security are of concern to some consumers¹². In the Panel's 2009 report *No one should miss out: consumers say what they want from the Digital Future*, participants:

- indicated that they were generally seeking more protection where possible, particularly with respect to the security of their data but also in relation to their privacy as users of online services
- recognised the potential benefits of information-sharing but indicated that they would embrace communications services fully only if they trusted companies, service providers and government to treat their personal information with care.

The need for consumers to be able to manage the potential risks online was also highlighted by the research review which the Panel carried out to develop its consumer framework for digital participation¹³. Once consumers are connected to the internet, they can enjoy the benefits fully only if they can also manage the potential risks.

There are potential risks attached to the sharing and collecting of personal data. In the last few years, the media have reported a number of cases of personal data being mislaid or collected inadvertently. There is a risk that online companies may misuse or mishandle the personal data they hold and that individual details, e.g. email addresses, may be disclosed inadvertently or that data is not stored securely. The disclosure of location information is a particular concern in the case of children.

There is also a risk that consumers are not fully aware of the potential implications of their decisions when they benefit from 'free' services or applications online. For example, many consumers use services that are free at the point of use, such as clip-art and screensaver sites, or reference sites such as dictionaries, and generally do not realise that in the process they may be downloading tracking cookies or software that enable companies to collect their personal data.

¹² See the Panel's research report *No one should miss out: consumers say what they want from the digital future* on its website:

http://www.communicationsconsumerpanel.org.uk/No%20one%20should%20miss%20out_digital%20future%20research%20report.pdf

¹³ See the Panel's report *Delivering digital participation: the consumer perspective* on the Panel's website: <http://www.communicationsconsumerpanel.org.uk/smartweb/digital-participation/the-consumer-framework-for-digital-participation>

Online personal data: the consumer perspective

The Panel's hypothesis is that the level of personal data that is collected and monetised via the internet is not widely known. As a result, consumers may not be making informed decisions about withholding their data and protecting their privacy, or sharing data and obtaining benefits.

Even when consumers are aware that they are providing personal information to an online business, they are often not fully aware of what happens to it afterwards. While people may choose to provide data to a particular website they trust, they may not realise that their data may be passed on to third parties.

Companies generally explain how they protect consumers' privacy in their terms and conditions and privacy statements. Consumers often sign up to these terms and conditions when they sign up for services. However, not all consumers read, and some may not fully understand, these terms and conditions or privacy statements because of the length of the documents and the technical language they tend to use. The result is that while the companies are technically being transparent, in practice their policies might not be understood by the people who are affected by them. Facebook has responded to such criticism by developing a new policy that explains more simply how it handles consumers' data and how this is shared with third parties.

It is also important to examine how the gathering and processing of personal data can affect people's privacy. When people use online services they often consent, explicitly or implicitly, to allow the services access to what they would normally consider private information. Things become more problematic if people feel that they have no choice but to relinquish elements of their privacy in order to make full use of the internet.

Personal data can be collected from nearly all online activity. That makes it very difficult for people to opt out completely. The fact that small bits of data from different sources can be aggregated to form a more complete picture of an individual makes reaching an informed decision even more difficult.

A potential risk is that if there were a greater level of public concern about how personal data are collected online it could deter the development of innovative services and applications, and the benefits for consumers that they bring.

Another privacy issue stems from the way people tend to use search engines. People rely on these services to navigate the internet, so they occupy a central role online. In general many items that people search for will, in themselves, be relatively innocuous, for example the names of online clothes retailers or concert listings. Others will be more sensitive, for example if they relate to a person's

medical record. While there are intrinsic privacy issues with someone else knowing such sensitive information, they are less severe if they cannot be directly linked back to the person concerned. However, it is also common for people to search for terms like their name, or to include their home postcode to identify local businesses. Where people do this, it becomes possible for sensitive but apparently anonymous information to be linked back to an individual.

Clearly, the ways in which personal data can be collected online create risks for consumers, as well as benefits, not least because it is often unclear to consumers what data they are providing, to whom, and what they are getting in return.

There is much debate in Europe and the United States about how the rules governing the collection and protection of personal data online should evolve. In this report, we have not taken a view about the extent to which the current rules protect consumers adequately, or the efficacy of the new measures which are under discussion. We hope, however, that the report will inform the policy debate. It is important to note that whatever rules are in place, consumers need to have confidence that companies are actually following the rules and managing personal data responsibly, and that if they do not, they will face robust enforcement action.

3. Consumers' views

In November 2010 the Panel decided to commission research to investigate consumer understanding and awareness of the monetisation of personal data on the internet. In January 2011 the Panel commissioned Accent, an independent market research agency, to undertake research into this subject.

Objectives

The key objectives for this research were:

- to understand the extent to which consumers are aware of the various methods of collecting data in the online environment;
- to understand the extent to which consumers are prepared to share their own data and what they expect in return;
- to understand consumer awareness of ways in which they can protect their online data, and their use of such methods;
- among those using a social networking site, their use of privacy settings and understanding of how personal data on such sites can be accessed and used by third parties; and
- to explore attitudes towards what is currently being done to protect personal online data.

Research methodology and sample

The research used both quantitative and qualitative methods:

- 1,000 telephone interviews with a representative sample of UK internet users aged 16+.
- Ten in-depth telephone interviews, lasting approximately 30 minutes each.

All fieldwork was completed in February 2011.

Differences between sub-groups (e.g. age, gender, socio-economic group, those accessing the internet via their mobile phone) are noted in the report only when they are significantly different from the total sample. We have reported differences at the 99% confidence level; this means that if we repeated the survey 100 times we would expect the results to fall into the confidence range 99 times. Where subgroups are not identified or discussed, no statistically significant differences were apparent.

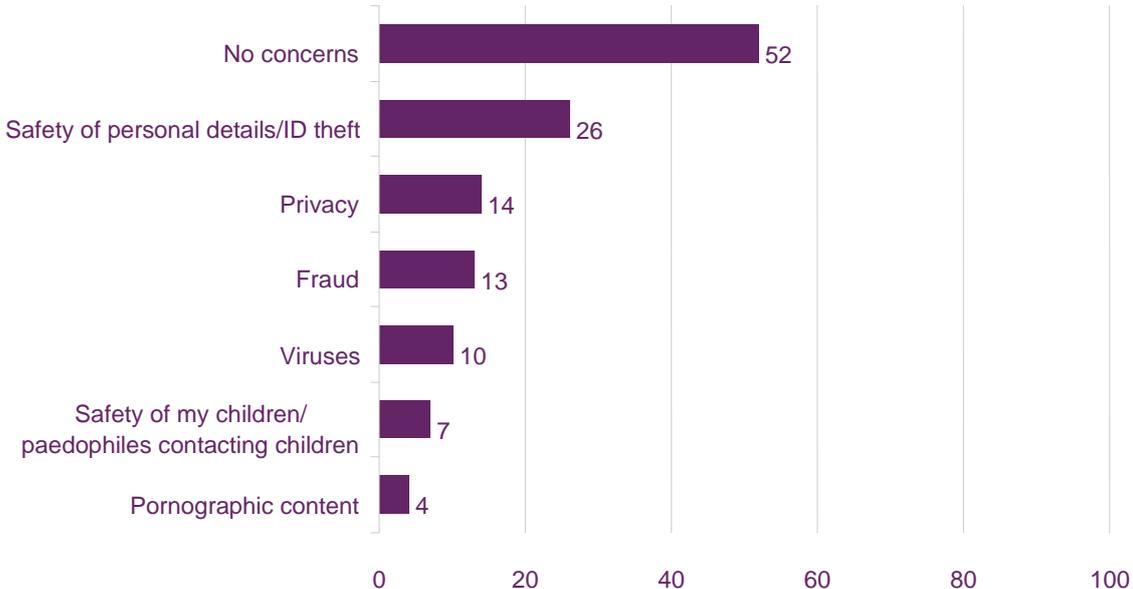
Full details of the research methodology can be found in Annex A.

In presenting the findings we have included quotes from the qualitative interviews where they are useful in illustrating the findings of the quantitative research.

Concerns when using the internet

Consumers were first asked whether they had any particular concerns when using the internet, in order to understand levels of unprompted, top-of-mind concerns (see Figure 3).

Figure 3: Spontaneous concerns when using the internet

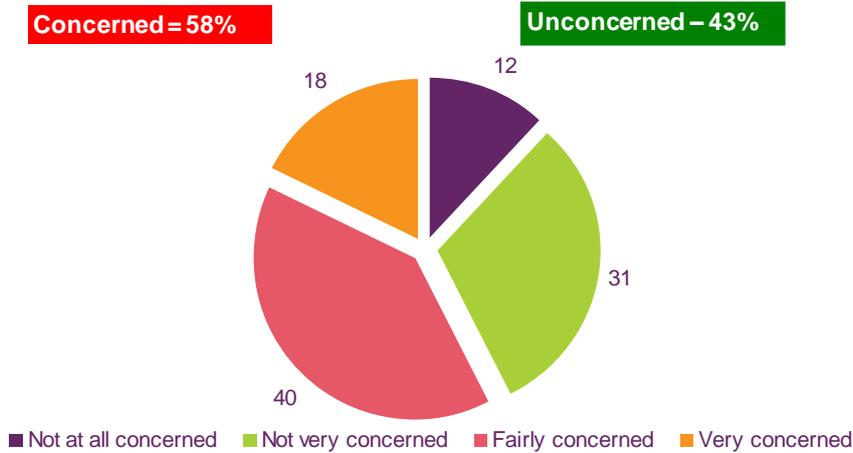


Q9. Thinking about using the internet in general, do you have any particular concerns when using the internet?
Base: All respondents (1022)

Just over half (52%) of UK internet users have no top-of-mind concerns when using the internet. The largest top-of-mind concern related to safety of personal details/ID theft, with just over a quarter (26%) of internet users spontaneously mentioning this. Concern about privacy issues was mentioned by 14% of internet users.

Internet users were then asked: “When using the internet, how concerned are you about your privacy online?”(Figure 4).

Figure 4: Prompted concern about privacy on the internet

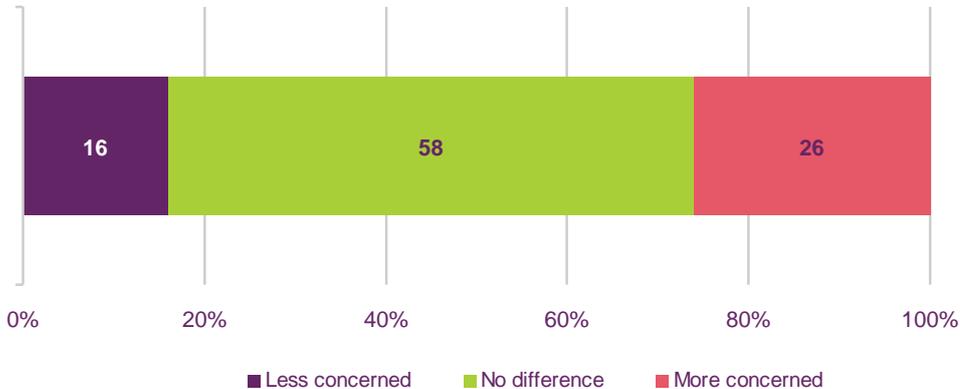


Q10. Generally speaking, when you use the internet, how concerned are you about your privacy on line?
 Base: All respondents (1022)

Overall, 58% said they were concerned, with 18% saying they were ‘very concerned’. One-third said they were ‘not very concerned’, and just over one in ten (12%) were not at all concerned.

Those consumers who used the internet on their mobile phone were asked whether they were more or less concerned about their privacy online when using their mobile phone compared to using a PC, laptop or tablet (see figure 5). Just over a quarter (26%) of those who use their mobile phone to access the internet are more concerned about their online privacy when using this device. Almost three in five (58%) said it made no difference, and about one in six (16%) said they were less concerned.

Figure 5: More or less concerned about privacy issues when accessing the internet via a mobile phone

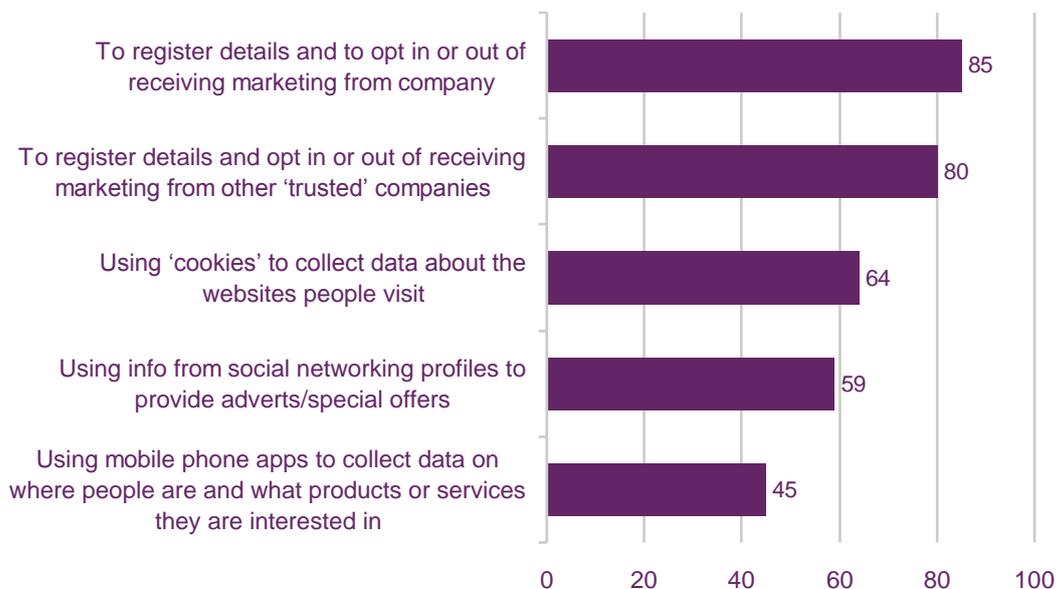


Q11. Are you more or less concerned about privacy issues when you use your mobile phone to access the internet compared to when you use a PC, laptop or tablet?
 Base: Those who access the internet via mobile phone (212)

Sharing personal information: awareness and attitudes

Internet users were read out a list of five ways in which companies can collect information about people online, and were asked to say which, if any, they had heard of.

Figure 6: Awareness of ways in which companies can collect information on the internet about people



Q22. There are many ways in which companies can collect information about people on the internet. Which, if any, of the following have you heard of?
Base: All respondents (1,023)

As shown in Figure 6 above, of the five ways of collecting information online, the most well-known were 'opting in/out of marketing information from that company' (85%) and 'opting in/out of marketing information from other 'trusted' companies' (80%). Those aged 25-24 and those in socio-economic group AB were most aware of these two methods.

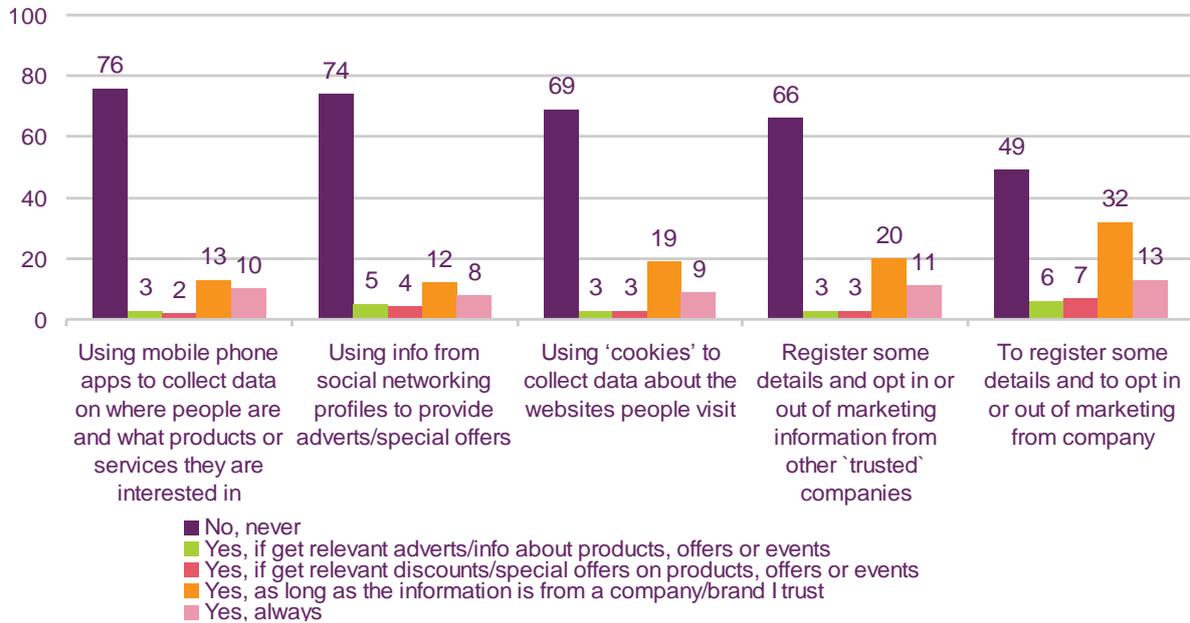
Three in five (59%) of all internet users were aware that companies can use information from social networking profiles to target adverts and special offers. This rises to 68% of internet users with a social networking profile.

'Companies using mobile phone applications to collect data' was the least well-known method, with 45% of internet users saying they were aware of this. Awareness was higher among those who use the internet on their mobile phone (53%).

Overall, those who used the internet every day, and those who were concerned about their privacy online, were more aware of these methods than those who used the internet less frequently and those who were unconcerned about their privacy online. In contrast, internet users less likely to be aware are those aged over 65 and in socio-economic group DE.

For each method that they were aware of, respondents were asked the degree to which they were happy for information to be collected about them.

Figure 7: Level of happiness for companies to collect information



Q23. And are you happy for this method to be used to collect information about you?

Base: All who have heard of each collection method

Note: Percentages do not add up to 100%, as multicode available for yes, if get relevant adverts, yes, if get relevant discounts/ special offers and yes, as long as the information is from a company or brand I trust

Overall, there were considerable reservations about companies collecting information in the ways shown in Figure 7, and the majority of people said they were ‘never happy’ for companies to collect information about them in these ways. Those who said they were ‘very concerned’ about their privacy on the internet were more likely to claim to be ‘never happy’ for these methods to be used.

Internet users were most accepting of ‘registering some details and opting in or out of marketing from a company’. While half (49%) said they were ‘never happy’ for this method to be used, a third (32%) thought it was acceptable, so long as it was by a company or brand that they trusted, and 13% were always happy for this method to be used.

“I would prefer to choose whether I was going to receive information or not so that would mean I would tick the box if I wanted stuff from them.” (Male, 16-24 years old, Leicester)

“Well, normally I think that when I’m on a website they will ask me if they can we send me marketing information, I won’t do that, I always un-tick the box. I don’t want them to take information from me using cookies either. If I want to give my information to certain companies I want it to be my choice, I don’t like cookies because they just automatically take your information.” (Female, 45-54 years old, Merseyside)

Online personal data: the consumer perspective

A small minority of people who had heard of each of the methods said they were 'always happy' for each of these to be used to collect their information or 'happy as long as they received something in return (e.g. adverts/special offers)'.

“Normally when I am on these sites I won’t click on the adverts to see what they are offering. But I am happy for them to use my information to tailor the ads.” (Female, 45-54 years old, Merseyside)

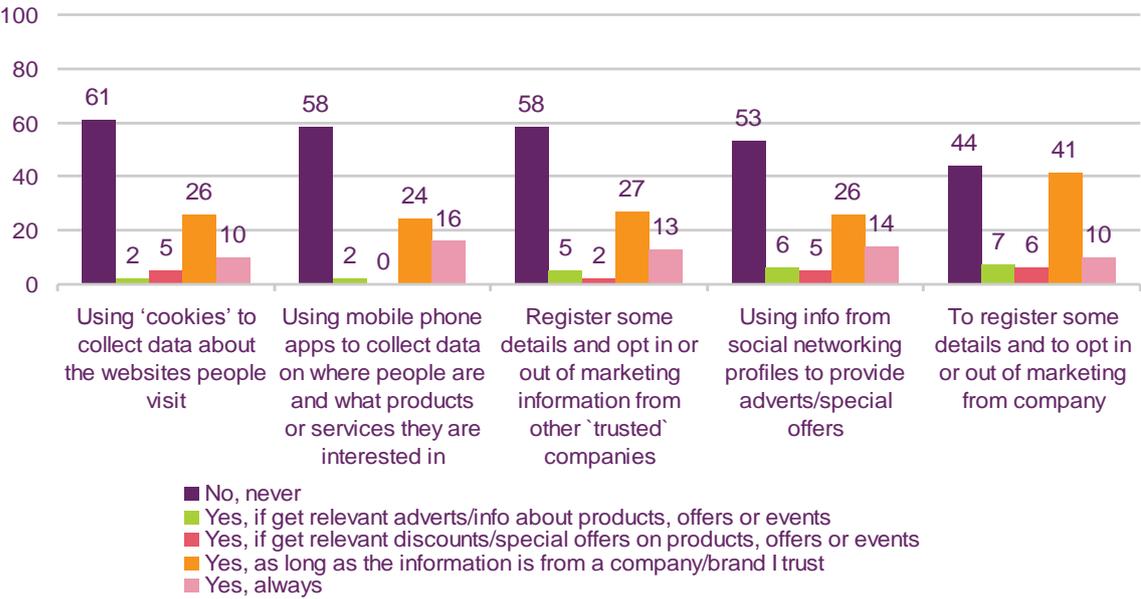
“It depends, if they are going to send me offers that I’ll be interested in, like discounts or new things that they have, then it’s better that they have my details so they can send them to me.”(Male, 16-24 years old, Leicester)

“If the advertising is a little bit more targeted because they have a cookie from the last time I was there and they know that I bought such and such, I don’t have a problem with that.” (Male, 35-44 years old, Birmingham)

Of the five methods of collecting data, internet users were most likely to say they were 'never happy' about 'companies using mobile phone applications' and 'information from social networking profiles' (76% and 74% respectively of all those aware of each method saying they were 'never' happy for their information to be collected in this way). For both of these methods, the proportion who said they were 'never happy' decreased among those who were directly affected: two-thirds (69%) of those with a social networking site profile said they were 'never happy' for companies to use information from their social networking site, and 70% of those who access the internet via their mobile phone said they were 'never happy' for companies to use location-based information.

In general, although the majority of 16-24s said they were 'never happy' for companies to collect their personal information in these ways, this age group is more accepting than the over-25s. Figure 8, below, shows attitudes towards companies using each of the ways of collecting information among those aged 16-24 years who had heard of each of the methods.

Figure 8: Levels of happiness for companies to collect information: 16-24 year olds aware of each method

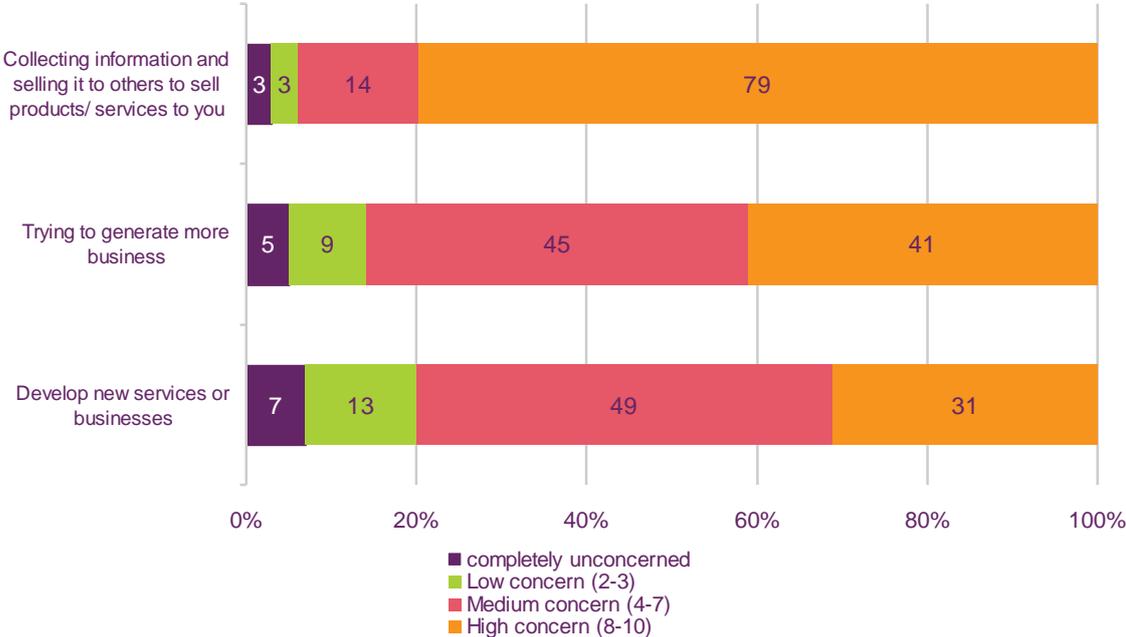


Q23. And are you happy for this method to be used to collect information about you?
 Base: All who have heard of each collection method, aged 16-24
 Note: Percentages do not add up to 100%, as multicode available for yes, if get relevant adverts, yes, if get relevant discounts/ special offers and yes, as long as the information is from a company or brand I trust

As can be seen in Figure 8, the higher level of acceptance among 16-24s is mainly because a higher proportion of this group said they were happy for their information to be collected 'as long as the information is collected by a company or brand I trust'. This was particularly true for registering some details and opting in or out of marketing from such a company.

Respondents were then read out three statements about why companies might want to collect people's personal information, and were asked their level of concern over companies using their personal information in this way.

Figure 9: Level of concern about reasons why companies collect information online



Q24. I am going to read out three statements and I would like you to tell me how concerned you feel with companies using your personal information in this way?
 Base: All respondents (1,022)

Figure 9 shows that, overall, the highest level of concern was caused by companies selling on the information they had collected, so that third parties could target consumers with products and services. This finding tallied with research commissioned by the Office of Fair Trading in 2010¹⁴. There was greater acceptance of companies using personal information to generate more business and to develop new services. Men are significantly more likely than women to have a lower level of concern about these ways of using information.

These concerns were echoed in the qualitative interviews. There was a general understanding that companies and individuals can benefit from using customers’ information. However, passing information on to third parties was contentious and for most respondents was less acceptable than companies using the information themselves.

In addition to online ways that companies may collect information about individuals the qualitative research also explored views about the provision of data to companies offline, via loyalty cards and loyalty schemes in shops. Very few people had thought about any synergy between online and offline methods before. When asked to consider it, overall, people did not see much difference between the loyalty card schemes in the high street and the online activity discussed. However,

¹⁴Online Targeting of Advertising and Prices, Office of Fair Trading, May 2010
http://www.offt.gov.uk/shared_offt/business_leaflets/659703/OFT1231.pdf

Online personal data: the consumer perspective

with offline activity, there was something about personal choice and the human touch involved in handing over a card to someone that gave people a greater sense of trust and control over the data provided. In the online environment, such activity was seen as happening automatically, out of sight and therefore more out of their control.

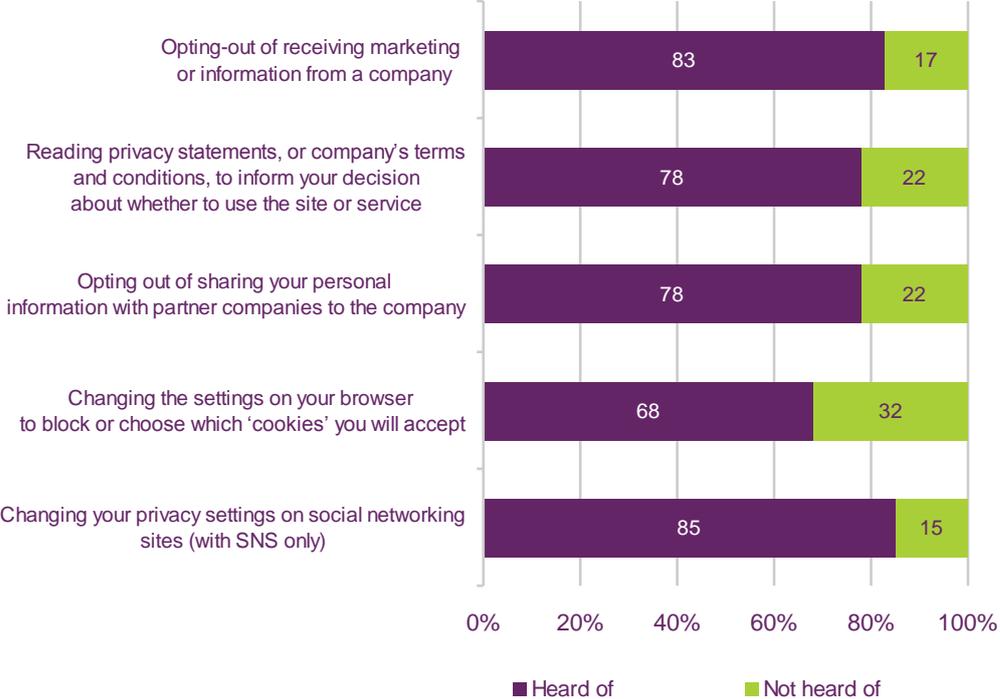
“It’s basically the same, but with a card you actually get to speak to someone whereas on the internet you give it to a server. But the information they collect is the same. I would say it was the same but I do prefer it when it comes from a person and not just through my laptop. There’s nothing wrong with it happening online but it’s just my opinion that I like the human touch.” (Male, 35-44 years old, Edinburgh)

“I suppose realistically when you think about it they’re the same. In fact the loyalty cards are probably worse because they collect more information about you. I haven’t thought about it before but they are similar.... I tend not to think about how they use my information. I tend to think about how they use my information online more than through the cards though. That’s because there’s potentially more people who can access the information. I feel that with the card it should be protected better but I’m under no illusions, I know that that information is also stored on a computer somewhere.” (Male, 35-44 years old, Halifax)

Awareness and use of methods to control personal data

Internet users were read out various ways in which people can control what is done with, and who has access to, their personal information online, and asked about their awareness of each one (Figure 10).

Figure 10: Awareness of methods to control personal data



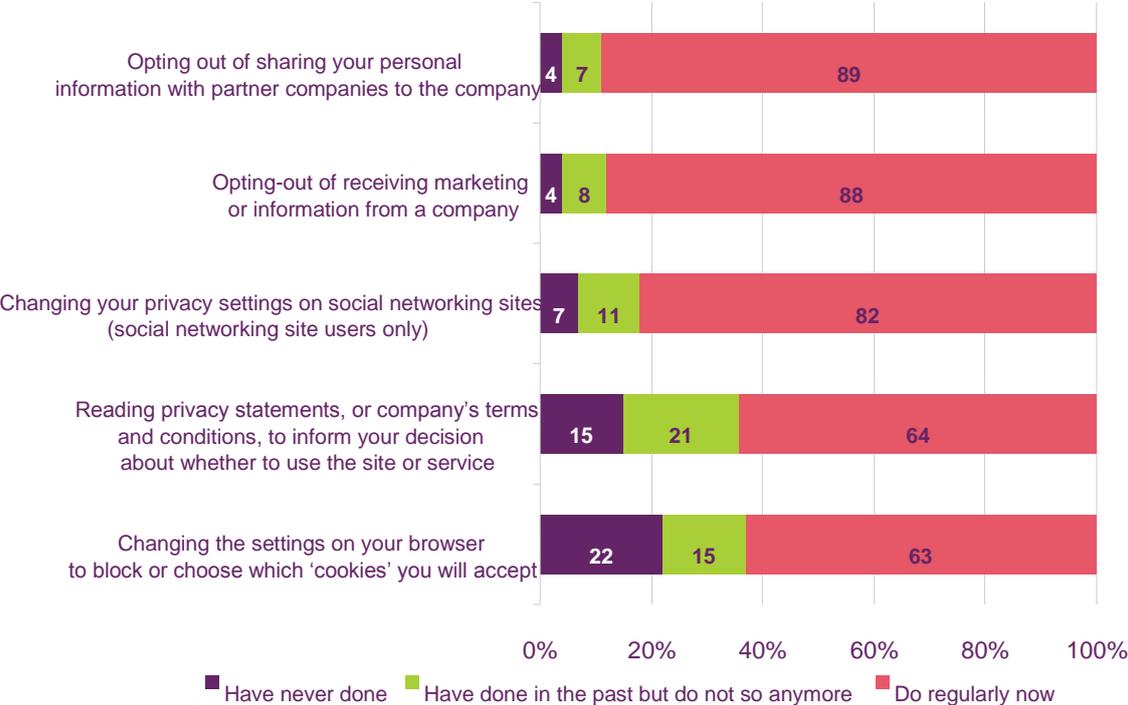
Q25. Similar to collecting personal information, there are also many ways in which people can control what is done with and who has access to their personal information. Which, if any, of the following have you heard of? Base: All respondents (1,022)

‘Opting out of receiving marketing or information’ received the highest level of awareness, with over four in five (83%) having heard of this method. This is followed by ‘reading companies’ privacy statements or terms and conditions’ and ‘opting out of sharing information with partner companies’ (both 78% awareness). Those in socio-economic group AB are more aware of these three ways of controlling personal information online than other socio-economic groups.

Eighty-five per cent of those with a social networking site profile were aware of the ability to change privacy settings on social networking sites.

For each of the methods that they had heard of, internet users were asked whether they personally used it.

Figure 11: Use of methods to control personal data, among those aware of each method



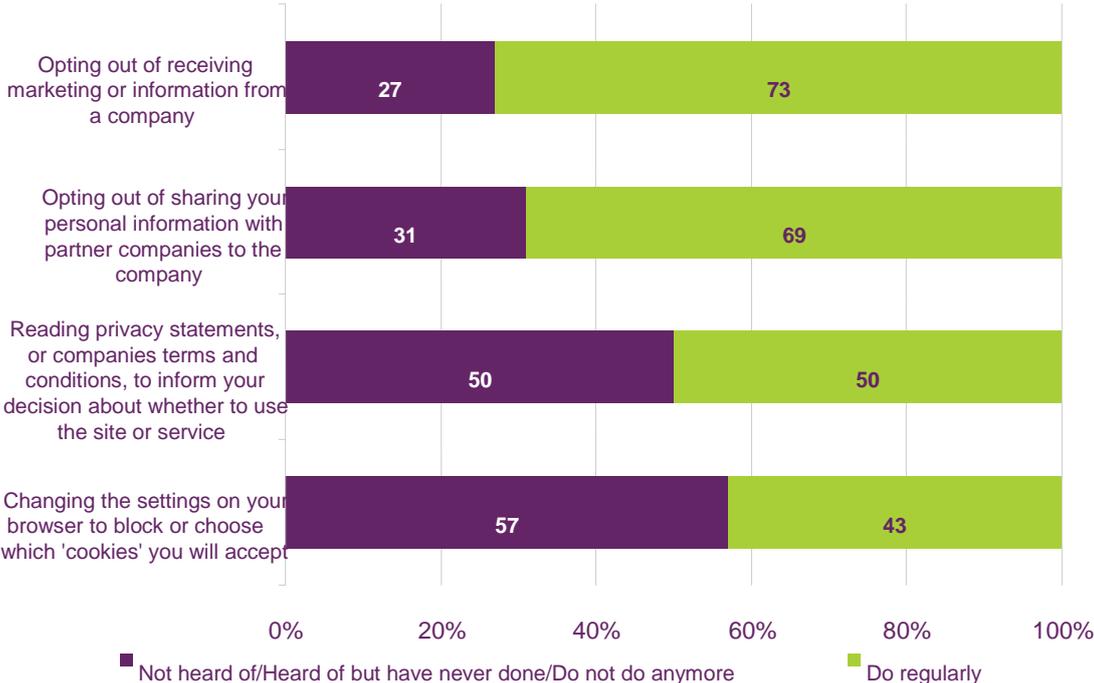
Base: All respondents who have heard of a method.
 Q26. Which of these methods do you use personally?

Figure 11 shows that ‘opting out of sharing personal information with partner companies’ and ‘opting out of receiving marketing information’ are the most frequently used, with almost nine in ten internet users who had heard of each method saying they regularly used each of these methods. Those aged 25-34 are more likely than other ages to use these two methods. Eighty-two per cent of those with a social networking site profile who are aware that privacy settings can be changed said that they regularly changed their privacy settings, although 7% said they had never changed them. Sixty-four per cent of users who were aware of privacy statements or terms and conditions said that they regularly read them, and 63% of those who were aware that browser settings can be changed to accept/reject cookies said that they did this regularly.

In Figure 12, below, we examine the use of these methods among all internet users - not just those who said they were aware of the methods. This shows that 73% of all internet users said they regularly opted out of receiving marketing information and 69% said they regularly opted out of sharing their personal information with partner companies.

Half of all internet users (50%) said they regularly read companies’ privacy statements or terms and conditions, and 43% said they adjusted the cookies settings on their browser.

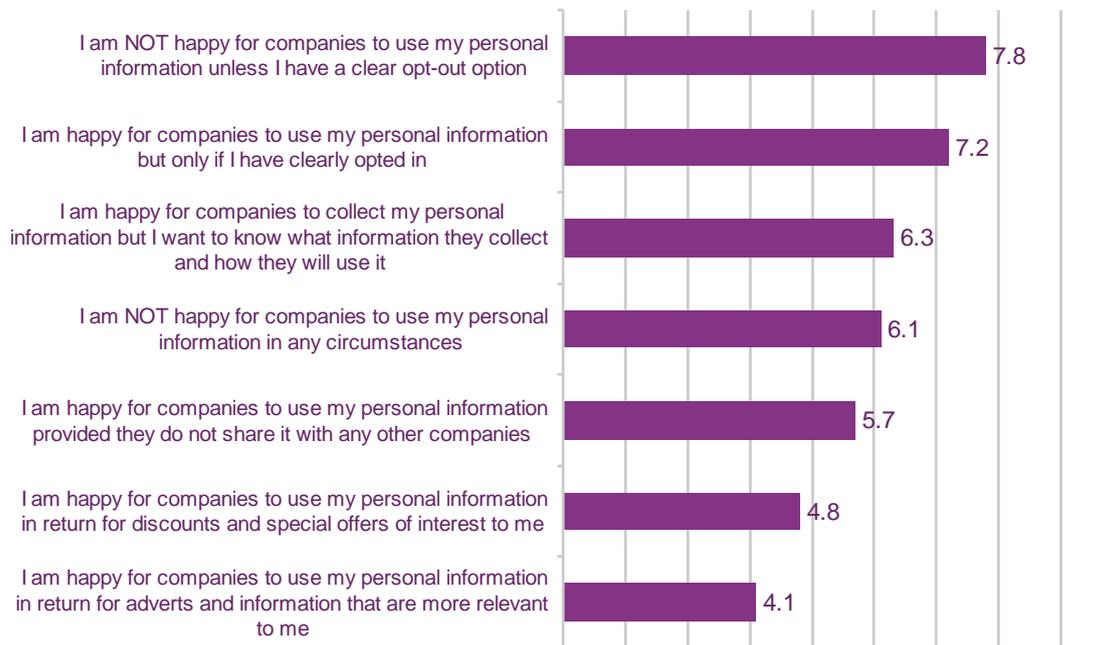
Figure 12: Use of methods to control personal data, among all internet users



Q26. Which of these methods do you use personally?
 Base: All respondents (1,022)
 Note: The statement 'changing your privacy setting on social networking sites' is not included, as not relevant for non social networking site users

Internet users were then read seven statements about attitudes towards companies using individuals’ personal information, and were asked the extent to which they agreed (10) or disagreed (1) with each statement. Figure 13, below, shows the average score out of ten for each statement.

Figure 13: Attitudes towards companies' use of personal information



Q27. Each statement describes 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: All respondents (1,022)

Internet users were most comfortable about their data being used when they felt in control, through clear opt-in and opt-out options. Internet users were also more comfortable about their information being used by companies when they were clearly informed about how the information would be used.

“I hate when you can’t get to a certain page without opting in or registering. I don’t like not knowing what they want my information for, especially if it is not a website that I am familiar with.” (Male, 35-44 years old, Edinburgh)

“It depends, if they are going to send me offers that I’ll be interested in like discounts or new things that they have then it’s better that they have my details so they can send them to me. I prefer to choose whether I was going to receive information or not, so that would mean I would tick the box if I wanted stuff from them.” (Male, 16-24 years old, Leicester)

“I don’t mind so much if one company has a piece of information but it’s when they start joining it together that I don’t like it. Even if they ask for your permission it’s the principle that bothers me.” (Male, 35-44 years old, Birmingham)

In the qualitative interviews, when respondents were asked about the appeal of special offers, discounts and adverts, while these were seen to be generally acceptable (in moderation) there was no great desire for them. Some said they did not need this kind of targeted activity, since they would look for (and expect to find) whatever they needed themselves. Others however, did feel that online

advertising would happen regardless, so they might as well have adverts and offers that had some relevance:

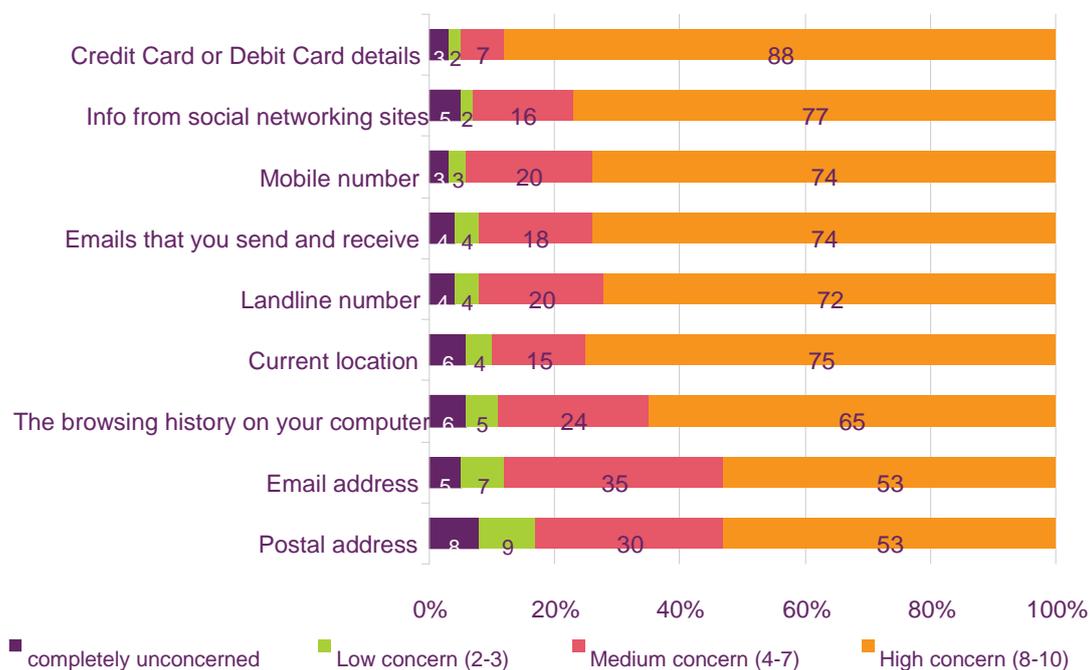
***“If I have got to see all this rubbish I may as well see rubbish that is potentially of benefit to me. I’m in the middle of buying a house online so seeing stuff that says ‘new mortgage rate’ is at least relevant.”
(Male, 35-44 years old, London)***

Some felt that often these activities were poorly targeted and so often lacked relevance.

“The learning mechanisms behind sites like this aren’t quite there yet... because you like yellow they will suggest you like orange but they are two completely different things.” (Male, 35-44 years old, London)

***“Amazon does annoy me sometimes because they send emails/marketing messages about things that to most people would be fully unconnected to what I’ve bought, but Amazon has managed to find a connection.”
(Male, 35-44 years old, Holywell)***

Figure 14: Level of concern about providing different information to companies



Q28. Again on a scale of 1 – 10, where this time 1 is completely unconcerned and 10 is extremely concerned, in general how concerned are you about providing (or: companies being able to collect) the following data
Base: All respondents (1,022)

Figure 14, above, shows that, overall, there were high levels of concern over sharing all of the different types of personal data discussed, with the highest levels

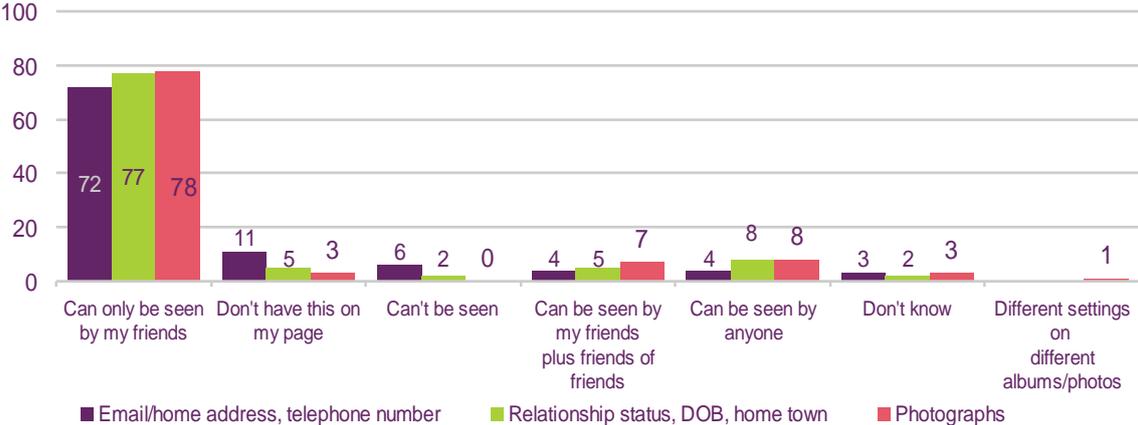
of concern associated with providing credit/debit card details (88%). Sharing email and postal addresses were the two types of information that people showed least concern about (although just over half of respondents showed high levels of concern). In the qualitative interviews there was an indication that for some people, company correspondence by email was less invasive and easier to manage than post:

“I don’t mind emails because you can just quickly and easily delete them.” (Male, 25-34 years old, Lincoln)

Social networking sites

Internet users who have a social networking site profile were asked questions about privacy settings on their profile page. Figure 15 shows privacy settings used by people in the survey with a profile on the social networking site Facebook (sample sizes for all other social networking sites were too low to analyse the data).

Figure 15: Privacy settings used on Facebook



Q29. Which of the following statements best describes how you feel about what is currently being done to protect your personal information when using the internet?
 Base: Those with a facebook profile (606)

Overall, the majority of people said their information could be seen only by ‘my friends’. A very low level of people said their information could be seen by anyone.

This was reflected in the qualitative interviews; the combination of privacy settings and a self-imposed limit on the level of personal details on their profile made most respondents feel unconcerned about their privacy on Facebook or on other social networking sites.

Figure 16: Awareness of personal information being openly available if not set to private

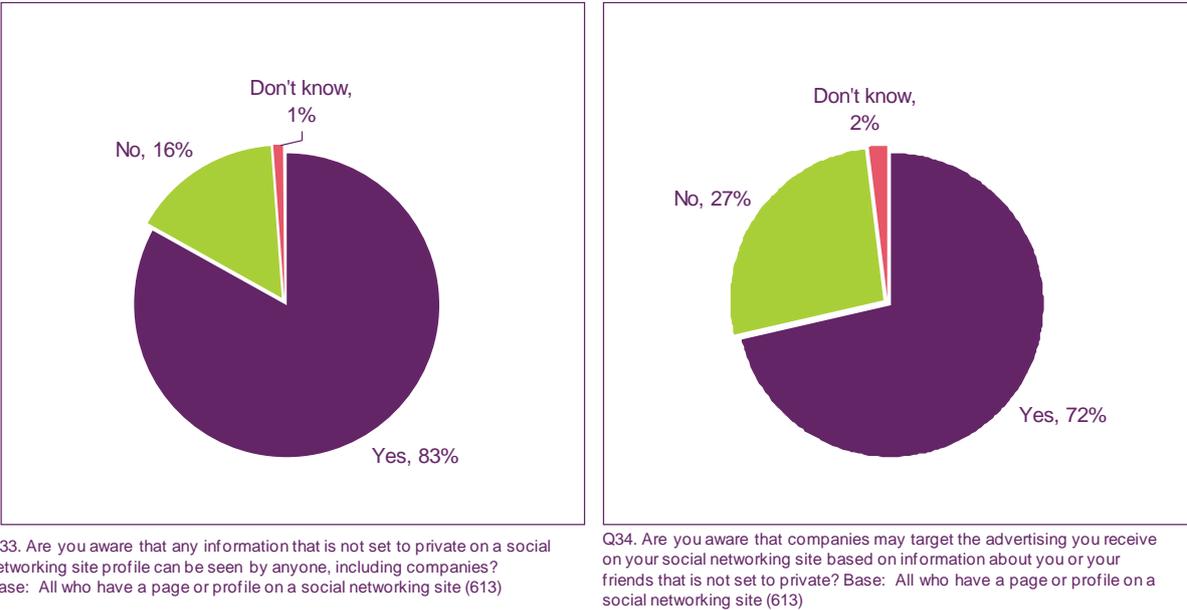
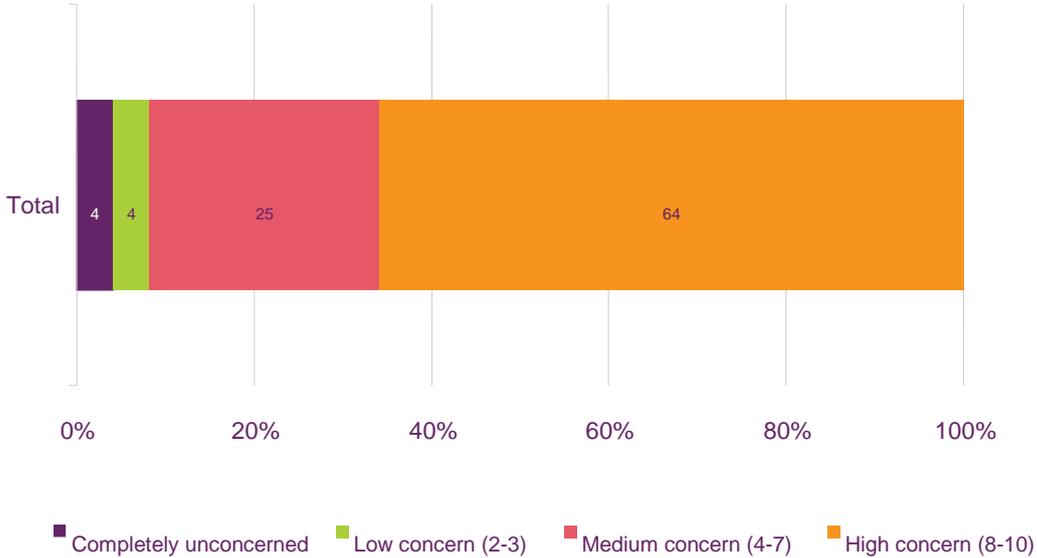


Figure 16 shows that there is high awareness that if privacy settings on social networking sites are not set to private, the information can be seen and used by anyone, including companies. However, a quarter (27%) of social network site users said they were not aware that this information could be used by companies to target advertising.

In the qualitative interviews, most people were not aware (or had never considered) that if someone’s social networking site profile is not set to private, companies can access the profile. The fact that companies could then use that information was something most respondents had thought about even less, or were not aware of.

Those with a page or profile on a social networking site were asked how concerned they were that companies are able to use the personal information on their social networking profile (Figure 17).

Figure 17: Level of concern about companies’ ability to use information from social networking sites



Q35. How concerned you are about the fact that companies are able to use your personal information?
Base: All who have a page or profile on a social networking site (613)
NB: figures do not total 100 due to rounding down

Nearly two-thirds of social networking site users said they were highly concerned. Concern tends to increase with age and socio-economic status.

Some concern was also raised in the qualitative interviews, with some people feeling that this was inappropriate:

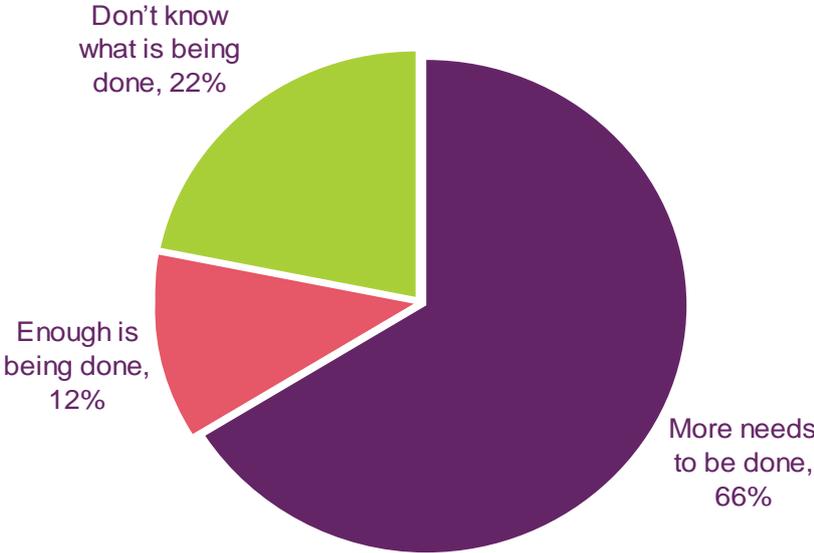
“No, I didn’t know about this. I don’t think it is ok for companies to do this. If I haven’t clicked an option then I don’t want this to happen. There isn’t really a reason why I don’t want it, but if I was just minding my own business there is no reason for them to be targeting me with adverts.” (Male, 16-24 years old, Walsall)

“I wouldn’t want people who aren’t on my friends list to see that information [personal details such as address]. I’m not really concerned about people seeing my photos.” (Female, 35-44 years old, Belfast)

Level of protection

Internet users were asked how they felt about what is currently being done to protect their personal information when using the internet, and who they think should be responsible for ensuring that individuals’ personal information is safeguarded online.

Figure 18: Attitudes towards current level of protection online



Q29. Which of the following statements best describes how you feel about what is currently being done to protect your personal information when using the internet?
Base: All respondents (1,022)

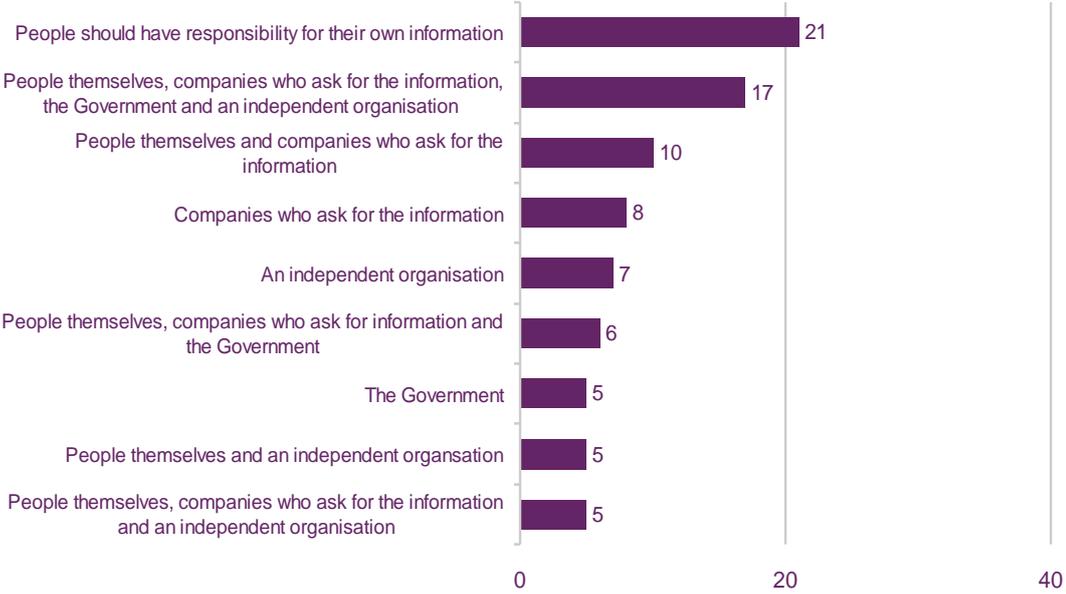
Figure 18 shows that two-thirds (66%) of internet users felt that more should be done to protect their personal information on the internet. More than a fifth (22%) said they did not know what was being done, and just over one in ten (12%) thought that enough was currently being done.

“I still don’t understand how people get hold of my email address I keep getting emails from a certain company trying to sell me cloths and perfume and things like that. I’ve never clicked on anything to do with them and I don’t know how to stop getting them.” (Male, 35-44 years old, Holywell)

“I think that as much is being done as can be done. At the end of the day it is up to me to protect my data.” (Male, 35-44 years old, Birmingham)

Respondents were asked who they thought should be responsible for ensuring that personal information is looked after according to people’s wishes. Figure 19 shows that, while one in five (21%) felt people should have sole responsibility for their own information, many felt that responsibility should be shared.

Figure 19: Who should have responsibility for ensuring that people’s personal information is looked after in accordance with their wishes



Q30. Who do you think should have responsibility for ensuring people’s personal information is looked after and used in accordance with their wishes?
 Base: All respondents (1,022)
 Note: All other combination of responses account for less than 5% of respondents

There was a feeling that there should be more clarity about how information is used, and more assurances around data protection.

“People should have responsibility for their own information. But I do think that things can be done to protect people’s information more. The companies need to let the people know if their information is being used and how it is being used. There should be something that appears on the side or something that lets the person know about it.” (Male, 16-24 years old, Leicester)

“I think it’s up to me to look after my own information as much as I can. I think that’s the case unless the companies can be held responsible for gathering information and passing that information on by legal recompense. I think the Government has too much on their hands at the moment so I don’t know who should take responsibility for it.” (Male, 35-44 years old, London)

“If I was giving someone information I would expect it to be confidential.... I don’t think anyone should be able to get my information from a company. If they need information about me then they should come and ask me for it.” (Male, 35-44 years old, Holywell)

4. Implications of the research findings

The Panel's view is that companies should improve consumers' awareness of how their data are collected and used, by being much more open about:

- what data are collected;
- how data are collected;
- how long data are kept for;
- why data are shared with third parties (including for commercial benefit); and
- how companies minimise the risks of personal data being misused.

This should not mean making privacy policies longer and more complicated. Companies should be able to explain how they protect people's privacy in a straightforward way that makes sense to consumers.

The Panel is also of the view that the existing ways in which consumers can manage the use of their data are insufficient. So we welcome industry initiatives, such as browsers that incorporate a 'do not track' option and the introduction of an 'icon' in display ads in Europe to enable consumers to identify behavioural advertising and opt out if they wish. Consumers should also be able to reverse decisions that they have made to share personal data. For this reason, we think it is important to explore how a 'right to be forgotten' or a 'right to have personal data deleted' could be implemented.

However, there will always be a limit to the extent to which consumers can be expected to take responsibility for controlling their data and the situation will become potentially more complex for consumers in future e.g. with the increasing adoption of cloud technology. The ways in which technology can be used to collect data are constantly evolving and the tools available to consumers will always lag behind. So, in parallel with raising awareness of how data are collected, and improving the means of controlling this, the Panel thinks that more effort should be devoted to minimising the amount of data that is collected and limiting the time it is held for. Companies should only collect and retain data to the extent that it is strictly necessary to deliver a particular service or application.

Online personal data: the consumer perspective

In summary, the Panel considers that consumers will only be genuinely empowered if they have:

1. information to allow them to make an informed decision about the implications of releasing their data;
2. control over the use of their data;
3. reassurance that companies will always minimise the amount of data that they collect, store it securely, retain it for no longer than is necessary - and consider whether to check with consumers after a set period of time whether they still wish their data to be retained; and
4. confidence that companies will follow the rules and manage personal data responsibly, and that if they do not, they will face robust enforcement action.

The Panel looks forward to discussing with stakeholders how best to ensure that these conditions are fulfilled. In doing so, we want to ensure that consumers can make an informed decision about whether to experience the benefits of sharing their personal data online and maintain the levels of privacy with which they are comfortable.