

**Being online: an investigation of
people's habits and attitudes**

June 2013

Acknowledgements

Thanks to the members of the general public who participated in our discussion groups, to all the project team at Ofcom and everyone at Ipsos MORI who helped with recruitment, fieldwork and analysis of findings.

Contents

	Key findings	3
1	Introduction.....	8
	1.1 Background	8
	1.2 Research objectives	8
	1.3 Key areas covered by the research	10
	1.4 Methodology and participants.....	10
	1.5 Analysis	11
	1.6 A note on presentation and interpretation of qualitative data.....	11
2	Experiences of the internet	14
	3.1 The role of the internet	14
	3.2 Current and future engagement.....	18
3	Online behaviour and trust.....	20
	4.1 Search and information gathering.....	21
	4.2 Online shopping.....	21
	4.3 Communication and social networking	27
	4.4 Online banking.....	29
	4.5 Citizen-related content.....	32
4	Personal data security issues.....	35
	5.1 Levels of awareness.....	36
	5.2 Consent and consequences	39
	5.3 Typologies and case studies	44
5	Rights and responsibilities.....	49
	6.1 Online behaviour	50
	6.2 Citizen rights and responsibilities	52
6	Future trends	61
	7.1 Relationship between humans and technology	61
	7.2 Safety, security and privacy in the future	62
7	Appendix	65

Key findings

Key findings

Ipsos MORI was commissioned by Ofcom to conduct this research and to prepare a report to inform its thinking on consumers' and citizens' behaviour in the context of different aspects of their internet experience. Ofcom has a statutory duty to further the interests of citizens in relation to communications matters. Ofcom is also guided by a regulatory duty to promote media literacy, and to carry out research in this area. It is on this basis that this report was commissioned.

This section of the report summarises the most important findings from the research, extracting the key insights and core messages that emerged through our conversations with participants.

People's attitudes towards the internet, and the role it played in their lives, varied widely, dictated primarily by levels of digital literacy (i.e. people's general confidence and competence in going online). For the **highly digitally literate** the internet had become one of their main ways of engaging with the world, used daily to access a broad range of services and information. For those with **medium digital literacy** the internet was a key part of their lives and they had become adept at using it for distinct tasks. Those with **low digital literacy** performed a limited range of tasks and tended to find it difficult to learn new things.

1) **Trade-offs emerged as a key contributor to people's online engagement**

People often weighed up the benefits and drawbacks when deciding whether to do an activity online. Whether someone decided to perform an online task was often determined by whether the perceived difficulty and effort required was sufficiently outweighed by the perceived benefits; typically speed, convenience or cost. For example, in deciding whether to buy something, particularly on a website which the user had not heard of before, the potential risk of the transaction was typically traded off against the financial benefit of getting the lowest price. This process often occurred subconsciously, but was more of a conscious process for the lower-literacy respondents, and for the medium-literacy respondents when they tried something for the first time.

Often a variety of factors came into play during the thought process that people went through when deciding whether or not to carry out an activity online. These included their previous experience of performing the activity, the experiences of friends / family, stories in the media, peer reviews of a product or service (on shopping sites, social networking or review sites), and any information and visual cues provided by the website itself. They weighed up all, or some of these factors when making the trade-off (either consciously or subconsciously) between benefits and drawbacks, and deciding whether or not to proceed with an activity online.

Confidence in going online was a key factor in whether someone felt able to access the full potential of the web. So, for some, even if they understood the basics of how to surf the web, and had the means to do so, their concerns, particularly around security and privacy, might hold them back.

2) There was a lack of awareness of how to stay safe online, and many misconceptions about what constituted 'safe' behaviour online. This often led to contradictory behaviour.

Participants adopted different measures to stay safe online (e.g. looking for the green padlock or 'https' in the browser bar, using verified methods of payment, installing antivirus software). It became evident through the research that participants did not understand how the mechanisms of various safety measures worked, which in turn meant that they often failed to use them in a consistent way. For example, they might have antivirus software installed on their PC, and believe that this provides general security online, but then fail to use verified methods of payment (they would just enter their debit card details when asked, and so on).

There were other contradictions in participants' attitudes towards security online. The purpose of their online engagement often influenced their behaviour with regard to security and trust: for example, some individuals happily shopped online but rejected online banking due to security concerns. The cause of this behaviour appears to be that when shopping online, participants were focused on acquiring the product or service, whereas participants banking online were much more conscious of their financial information being 'up online'.

It was clear that people rely on their instincts to assess what to trust online. For example, many subconsciously look for visual clues that a website is legitimate, and judge whether to engage based on the general 'look and feel' of the website design. A sense of connection with another person online can also make people feel more secure, whether this is via peer reviews or by 'speaking' to a customer service representative by email.

3) There was a lack of understanding of how personal data is stored, used and transferred online. Many were happy for companies to use their data if they gave consent, but there were some concerns as to the consequences of this.

Most participants had at best only a vague impression of what happened to their personal data online, and many had not previously thought much about this. Many participants understood that their details would be passed on, but did not tend to dwell on this, as they did not understand the mechanisms of how this happens, and they saw it as impossible to prevent. They did, however, express concern about consequences that would affect them directly (for example, they did not want to be spammed with email or to receive unsolicited texts from unknown companies).

Stories in the media or from friends were key factors in shaping perceptions of who to trust with their personal information online, particularly for those who were less digitally literate. Negative stories had made these participants much more wary of conducting the activity in question online: e.g. stories of friends being defrauded online would make them far less inclined to shop online themselves. One of the biggest concerns was identity theft, or having financial details stolen.

Once again, trade-offs proved key: participants would input their personal information or agree to terms and conditions if this 'stood in the way' of them getting what they wanted, whether this was a product available from only one website, or simply a product at the best price. Other trade-offs were more passive, but involved the same principle. For example, participants said they would willingly hand over information about themselves, as with loyalty cards or discount schemes, in exchange for the

financial benefit. However, informed consent was key – people wanted to at least be told that their data was being passed on. Attribution of data was also a key factor: if the data was non-attributable then passing it on was less of an issue for participants.

People did not have comprehensive strategies relating to their personal data, but tended to employ a more piecemeal set of methods. These included avoiding 'save details' requests; not allowing their details to be shared with third parties; and deleting browser history and cookies. Some said they gave out partially incorrect data, and some had separate email (and bank) accounts for transactions or potentially unsafe sites.

4) There was a broad assumption that online rights and responsibilities should be the same as those offline. However, participants admitted that this was an assumption on their part.

Most people were entirely unaware of their online rights. When asked, they believed they should be the same as rights in the offline world, although they were not aware whether this was in fact the case, or indeed why they might make such an assumption.

Similarly, with regard to behaviour and social norms online, most participants said that they did not appreciate why standards should be any different online to offline. They acknowledged that people did in fact behave differently online, although probing was required before they admitted that this also applied to their own behaviour. Generally, participants felt that people were less inhibited, more honest, but also more argumentative online, as they could 'hide behind their screens' and avoid accountability.

When debating what should and shouldn't be allowed online, participants weighed up the potential for online content to cause harm against the principle of free speech. They defined harmful content as anything involving illegality, victimisation or bullying. They distinguished this from generally offensive comments, which they felt to be largely subjective in nature.

People felt that individuals had a responsibility to behave in a socially acceptable way online, and that websites themselves should monitor and address offensive, particularly victimising, comments, while still aiming to preserve free speech. Participants expressed the view that government should step in only in cases where the law was being broken: they broadly felt that what was illegal offline should also be illegal online and that the crimes should be treated similarly, carrying the same penalties in each case.

5) Participants foresaw a future increasingly dominated by the internet.

Respondents thought that, inevitably, the internet would become increasingly dominant. This shift online was not generally perceived to be problematic, as long as the changes were seen to be beneficial to some. This might include a more individually tailored internet experience in exchange for providing personal information, with customised products and services being offered by companies, leading in turn to greater customer loyalty.

A further positive prediction was greater harmony between humans and technology. Participants imagined the devices we use becoming more integrated with our lives, and

expected that such a symbiotic state would become a reality in the relatively near future. The always-on, almost touchable nature of the internet was predicted to become an even greater reality: most foresaw a future with total access to all information, for free, which everyone would constantly interact with, without ever disconnecting. While such predictions were met with sadness by some, who lamented the demise of more traditional means of communication, participants were broadly resigned to this vision of the future. Even participants with the lowest digital literacy recognised that they would need to move with the flow of technology, or risk being left behind or alienated.

1. Introduction

1. Introduction

1.1 Background

Ofcom commissioned this exploratory piece of qualitative research at the beginning of 2013 in order to inform its understanding of people's internet use in different contexts and across different levels of digital literacy. The study was intended to provide detail on the different attitudes and behaviours people have towards various topics including internet security, e-commerce and privacy online.

1.2 Research objectives

The overriding aim of this study was to inform current thinking on consumer and citizen behaviour in the context of different aspects of the internet experience.

To successfully meet this aim, it was important to achieve a detailed understanding of users' attitudes and behaviour across a range of core topics, and to capture a range of perspectives including a user/individual perspective and a citizen/society perspective.

Recruitment

To explore the different drivers and barriers behind participants' attitudes towards the internet, the research took into account the different levels of *digital literacy*, separated into low, medium and high. Participants were recruited on the basis of 'pen portrait' descriptions of each level, provided below.

Low digital literacy

These are people who consider themselves to be relatively new to the online world, and only really began to engage with basic online activities within the last year or so. They are likely to be older, and/or likely to fall within the DE socio-economic group, but not exclusively so. Some might own their own PC/laptop/tablet, or at least have access to one within their household, while others might go online through publicly-available computers (for example, at the library, learning centres and so forth).

These people tend to go online for functional reasons and to carry out basic activities (for example to check and send an email, or to look at social networking sites such as Facebook), but do not know how to carry out other tasks such as uploading a picture or video to the internet other than through these social networking sites. At present being online is not central to their daily lives, but they might go online to keep in touch with others. Some participants in this group may own smartphones, but might not know how to use them for internet searching, or be too scared to do so; some use their smartphone or tablet to go online, but only for basic tasks. They use their mobile phones mainly for making calls/texts..

Those in this category may be frustrated about their limited online abilities and want to learn more, but they are unsure of how to do this. Some people in this

group might simply be satisfied with their limited skill set and not want the online world to 'take over their life'.

Medium digital literacy

These are people who are competent at undertaking a number of online activities, ranging from basic tasks such as sending an email, using social networking sites and using search engines through to more challenging tasks such as uploading pictures, internet shopping and filling out online forms. Tasks such as installing a browser, keeping a blog or installing programmes are, for some, outside their comfort zone, while for others, this is not something they have previously done, or would have the confidence to do.

These people are likely to own their own PC/laptop/tablet, and many will also use a computer for work. Most of them are satisfied that they know enough to get by online, but are conscious that if they really wanted to, there is more they could learn.

People with medium digital literacy are more reliant upon the online world to help them carry out day-to-day tasks, and to keep in touch with others. They are more likely to have smartphones, and to use them for more than simply calling and texting (they are likely to also use the camera, applications, and go online). They are aware that there is probably more they could do on these devices, but they have yet to master these skills. This group includes all ages (18+ years) and all socio-economic groups.

High digital literacy

These are people who are very confident in undertaking most online tasks. Sending emails, updating social networks, photos and/or videos are done so often that they are no longer considered to be a 'task' in themselves. They are likely to have experimented with blogging and, for some, creating and maintaining their own websites. Installing programmes is seen as a straightforward task, as are carrying out more advanced actions such as using multiple tabs on browsers, deleting search history and cookies and syncing more than one device.

People within this group are 'tech-savvy', and are more likely to own multiple devices that allow them to go online. Being online is second nature to them and they rely on the internet in many aspects of their lives (such as communicating, buying products, contributing to forums, blogs and websites). They are unable to imagine life without the internet.

For these people, staying 'ahead of the curve' and getting the maximum experience from being online is where they want to be; they are open to learning new skills and opportunities as and when new technological developments appear. They are likely to be younger (18-40) but not exclusively so, and are more likely to be in the ABC1/C2 socio-economic groups.

It is important to note that participants were recruited on their self-declared level of digital literacy, following a conversation about their levels of confidence, frequency of internet use and competence online.

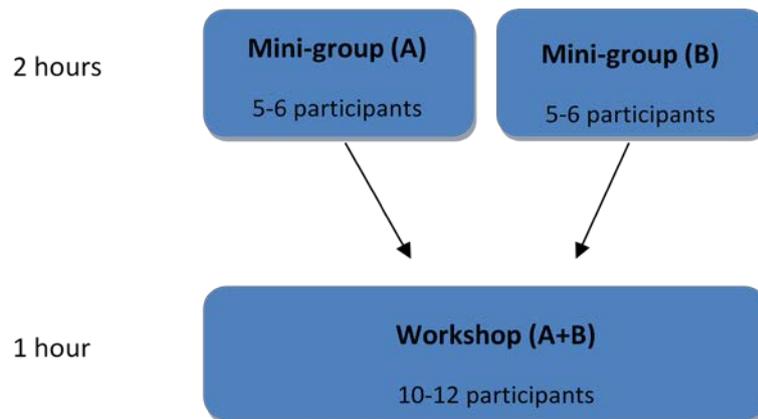
1.3 Key areas covered by the research

There were six key areas of focus:

- **Experiences of the internet**
 - Why people use the internet and its role in their lives: This included device ownership, usage and online confidence levels. It also covered drivers of and barriers to internet use, and whether the internet had replaced any other activities.
- **Online behaviour and trust**
 - How people engage in e-commerce: This included what e-commerce means to consumers, the barriers to using specific sites and the potential pitfalls to buying and selling online.
 - How people decide whether to trust: This included the most important factors when deciding whether to trust a website or search engine and general concerns about security online, including people's understanding and thoughts relating to government /civic sites.
- **Personal data security issues**
 - People's awareness and concern about their personal data: This looked at awareness of how personal data was captured and used, and levels of concern around such practices, including understanding of cookies and how protected their data was.
- **Rights and responsibilities**
 - This topic helped us to understand people's knowledge and understanding of their citizen rights. It explored what citizens should do, whom they could contact if anything went wrong and who was ultimately responsible for resolving any problems. It also explored views on the moral norms of internet use in terms of what was acceptable behaviour.
- **Future trends**
 - Ideas about the future of the internet: This aimed to understand what would be people's ideal internet experience, and to review the direction in which the internet is heading.

1.4 Methodology and participants

Given the exploratory nature of this study, a qualitative approach was used, combining mini-groups of different levels of digital literacy which then combined into a workshop for a joint discussion on matters relating to society and citizenship.



Discussion groups were conducted in six separate locations across the UK: St. Albans, Leamington Spa, Grimsby, Glasgow, Cardiff and the pilot workshop conducted in the Ipsos offices in London (which has been incorporated into the final findings). Details of the discussion groups are included in the appendices. The locations were picked to ensure good geographical coverage and to include people living in a range of different types of location (urban, rural and suburban). Discussions included a mix of ages and socio-economic groups, with each mini-group representing different levels of digital literacy.

In addition to discussion groups, we asked all the participants to keep a diary of their online activity in the week leading up to the group. The respondents noted when they were online and what tasks they were undertaking. We also asked them to think about why they chose to do each activity online, as opposed to offline.

Fieldwork took place between 22 January and 4 February 2013. All discussion groups and interviews were audio-recorded and a guarantee of anonymity was given to those who took part.

1.5 Analysis

An integrated approach was taken to the analysis, combining the findings from across all audiences. This report focuses on the experiences of medium digital literacy users, although we have highlighted the differences where low and high literacy users had notably different attitudes or experiences.

1.6 A note on presentation and interpretation of qualitative data

Qualitative research approaches are used to shed light on why people hold particular views, rather than how many people hold those views. The results are intended to be *illustrative* rather than statistically reliable and, as such, do not permit statements to be made about the extent to which something is happening.

Given the qualitative nature of the current study, this report aims to provide detailed and exploratory findings that *give insight* into the perceptions, feelings and behaviours of people surrounding internet use rather than conclusions from a robust, quantifiably valid sample.

It is not always possible in qualitative research to provide a precise or useful indication of the prevalence of a certain view, due to the relatively small number of participants generally involved (as compared with the larger respondent bases involved with quantitative studies.) We therefore state the *strength* of feeling about a particular point rather than the number of people who have expressed that thought. We favour phrases such as 'a few' or 'a limited number' to reflect views which were mentioned infrequently and 'many' or 'most' when views are more common. Where views apply only to a subset of participants, for example those with low digital literacy or younger users, we have highlighted this in the relevant text. Any proportions used in our reporting (such as a 'couple' or 'handful' of participants), should always be considered indicative, rather than exact.

Verbatim comments have been included in this report to illustrate and highlight key points which are either shared by a large number of participants or which reflect the strong views of a smaller subset. Where verbatim quotes are used, they have been anonymised and attributed with gender, location and low/medium/high digital literacy. This has not always been possible when quotes were taken from the workshop section where levels of literacy were combined.

E.g. Female, St Albans, Medium

Another consideration in the interpretation of qualitative data is the role of *perceptions*. Different outlooks on an issue make up a considerable proportion of the evidence presented in this study; while these perceptions may not always be factually accurate, they represent the truth for those who hold these views.

2. Experiences of the internet

2. Experiences of the internet

This chapter provides an overview of participants' varying experiences of the internet and their behaviour online. We look not just at the role the internet plays in participants' lives, but also at the role they would like it to play, drawing on case studies to illustrate these themes.

Key findings

The **role that the internet plays** in people's lives **varied widely**, primarily dictated by their levels of **digital literacy**.

For those with **high and medium** digital literacy, the internet was integrated into their lives and either was, or was fast becoming, their primary way to make purchases and contact friends. For these users the internet was a **tool of convenience**, allowing them **quickly and easily** to perform tasks which were considered to require more effort offline (e.g., price comparison). Online activities were dominated by **information seeking** and **shopping**, particularly using the wealth of information available online for product and price comparisons.

Among those with **low digital literacy**, however, being competent online was felt to be a **requirement**, to the extent that they sometimes felt as though they were being **'forced' online**. Those with lower digital literacy often felt that online communication was replacing more valuable face-to-face contact, and lamented this fact. The key online activity for this group was **information-seeking**, as it was perceived to be relatively **safe** and **easy** to perform.

However, digital literacy gave way to some exceptions in terms of behavioural patterns: a few **highly digitally literate** people still had particular activities that they preferred to carry out offline (for example, visiting the local branch of their bank in person because the staff are friendly) and a few **less digitally literate** people used high-tech devices such as tablets (albeit for simple and limited uses, such as playing games).

2.1 The role of the internet in people's day-to-day lives varied widely

There were marked differences in participants' relationships with the internet. High and medium digital literacy users tended to share the same broad outlook: that the internet is predominantly a convenient and central aspect of their lives. The internet is often perceived to be the only way to engage with some companies and services, or at least the most efficient way, as it avoids the need to wait on a phone line or in a queue.

'Oh, it's far easier. There's no hassle. There's no queues.'

Male, Glasgow, Medium

Some of those with low digital literacy, however, actually felt inconvenienced if information they wanted was *only* available online, and saw themselves as effectively being forced online. Digital literacy is increasingly becoming a requirement; for example, several parents note that their child's school communicates with them

exclusively online, and likewise, goods or utilities are often more expensive if paid for offline.

'You ring a hotel and they tell you 'If you book online it's cheaper than booking direct'. It's £100 a night, but then they'll say, 'But if you book online it's £80'. And it's amazing, so you're talking to them but you have to go online.'

Male, St Albans, Medium

Natalie (low digital literacy) – Feeling pressured to be online

Natalie, 37, is a single mother and homemaker and comes from a disadvantaged background. She admits that she knows very little about computers and feels nervous about using them. Her internet use is limited mainly to activities that she cannot carry out offline: checking email (which her ten year-old daughter helps her with) and receiving communication from her daughter's school.

'Every Friday we have a newsletter of what's going on with the school. They used to send them by leaflets but now they're on email. So that's one of the reasons why I really go on [the computer] because I don't work in computers, I don't do anything like that so I don't really use the computer at all, not much.'

However, Natalie remains nervous about going online and what happens to the information she enters. She is affected strongly by stories she hears from friends about things going wrong online; for example, a false scare story about personal information being exposed via Facebook:

'Somebody told me a while ago that all your inbox stuff was going to be on your front page or something like that. All your private [information] is going to be on your wall, and stuff like that.'

Natalie therefore feels safer doing things the way she has always done them, offline. For example, she has never bought or sold any goods online, preferring to go to the shops instead, as this is what she has always done. Her preference for staying offline stems not only from security concerns, but a lack of skills and experience around computers in general. Although her daughter helps her with emails, Natalie feels that she often lacks patience as a teacher. As a result Natalie will only engage with very basic tasks such as email, with her daughter's help.

For medium and high digital literacy users, because the internet had become so integral to their lives, they tended to feel that it was now essential, in their personal, and often professional, life. This integration also led to them potentially feeling as though they could not avoid it, or even that they were 'addicted' to using it. 'Addictive' behaviour included using it when they did not actually feel it was necessary or using it repeatedly for the same task, such as when on holiday or 'pointlessly' checking social networking sites.

'It's addictive. I need to log on every day.'

Female, London, Medium

Among more digitally literate users, integrating internet use into their life tended to be combined with their use of multiple devices; desktops/laptops/tablets/smartphones, all of which meant that a medium or high digital literacy user was always only a short step away from being online.

Roy (high digital literacy) – Online makes sense

Roy is 30, and works in retail; technology and the internet are central to his life. He is used to being able to perform hundreds of activities without having to leave the house, and feels hugely inconvenienced if he is not able to do so.

'It's easier, there's more choice, it's more convenient, you can shop from the comfort of your own home, you can get options for delivery.'

Roy interacts with companies and services almost exclusively online, and through multiple devices, on a daily basis. For example, he no longer buys a printed newspaper; instead, he reads books and the news primarily on his iPad. He banks online, and contacts his credit card company by email when he is going abroad.

Roy uses smartphone apps for reporting gas and electricity readings for which he receives Nectar points. He does, however, get frustrated by online limitations; for example, that he cannot increase his overdraft limit at his bank online, and he plans to move to a solely online provider. Recently he used email to arrange for the local council to pick up some rubbish from his garden, and would not ever try to call them, as he finds himself having to wait a long time on the phone.

'I've got no contact with the local authority offline.'

Beyond interacting with companies and services, he uses the internet for searching for information, and downloading and streaming television and music. Conversely, although he is on social networking sites he does not tend to go on them regularly, preferring instead to email or call his friends.

Roy is not overly concerned with security issues online. He recognises that there is a risk associated with entering his personal data online and performing activities such as banking, but he perceives this to be relatively small, and one which is greatly offset by the benefits that online transactions provide for him. He has not encountered any problems with online security and if he did so in the future he would probably 'chalk it up to experience' and continue undeterred with his usual level of online activity.

For participants with lower digital literacy, their internet use was quite narrow in scope; they tended to try new things only if they were prompted to do so by others. Less digitally literate users, whilst they may actually have access to several devices, including smartphones, were not necessarily using them to anything like their full potential. Limited digital literacy was also illustrated by a lack of competence across devices; for example, only being comfortable accessing the internet via mobile.

'Technology does baffle me if it's not on my phone.'

Female, Grimsby, Medium

Jim – Technology is a struggle

Jim, 56, is semi-retired and has only started using computers in the last few years. He worries that he has fallen behind the rest of society and wonders if he will ever be able to catch up.

'You try to keep up appearances; you don't want to be seen as living

in the 'Dark Ages'.'

Jim has found that knowing how to use a computer has now become almost a social requirement.

'I felt very ashamed actually at one stage when I couldn't keep up. I felt a stigma of not being able to use a computer at all when I was at work and it did become a little bit of a joke, and that was quite unpleasant.'

Jim has a desktop which he uses for word processing, email and browsing websites, but, because of his lack of confidence with technology and the internet, he does not use his computer to its full potential. In particular, he does not engage in online shopping or banking, feeling that such activities are beyond his capabilities, and that he could accidentally end up buying the wrong thing. He also has a smartphone, which he does not use for anything other than calls and the occasional text. In general he is not *exploratory* as he is too concerned that he will do something wrong.

'I suspect I'm a bit of a technophobe actually, I always think I'm going to break something or ruin something; I've never been particularly adept with anything technical.'

Jim's concerns around security relate not so much to the malicious actions of others (e.g. hackers obtaining his personal information) but more to his own lack of skills and making a mistake which he will not be able to rectify. He tends only to perform activities which he has been shown how to do. For Jim, learning something new about technology is effortful and involves unfamiliar concepts and terminology which are not easy to remember.

'I did actually go on a course to get the basic skills and I did, I was shown how to do these things but then I never did them so I forgot how to do them.'

Jim found recently that his concerns about his own abilities were justified when his computer crashed and, because he did not know to back up information, he lost all his documents.

Like Natalie he appreciates that everyday activities are moving increasingly online, and while he makes more of an active effort to keep up with the change, he is similarly held back by a lack of confidence and ability.

2.2 People saw it as inevitable that an increasing number of daily activities would move online in the near future

Among those with low and medium digital literacy there was a mix of views towards the role of the internet. Most were inclined to see its potential and would have liked to become competent to a much greater degree. However, there were a few who saw the internet as having a predominantly negative effect on people and society, and did not wish to deepen their understanding. There were also those who were not necessarily positive about the 'digital revolution' but who felt that they must try to keep up or they would be left behind.

'Well if you can't beat it, you've got to join it haven't you?'

Male, London, Low

'It's the way of the world isn't it, technology?'

Female, London, Low

Typically, high digital literacy users expected that, within reason, all engagement with businesses or services could be conducted online. However, several high digital literacy users wanted to keep the option of using the telephone or face-to-face interaction. For example, one high digital literacy participant in Glasgow did not bank online because he liked going into his local branch, as he had done for 20 years, and where he knew the staff by name. Likewise, several high digital literacy users still liked to read books and newspapers, rather than always engaging with their digital equivalents.

3. Online behaviour and trust

3. Online behaviour and trust

This chapter provides an overview of some of the typical activities participants perform online. Looking across levels of digital literacy, it explores participants' attitudes and behaviour towards several core online activities including, in broad order of prevalence;

- search and information gathering,
- e-commerce,
- communications and social networking,
- online banking, and;
- public services online.

It examines the role of trust when conducting these activities online, as well as the relative importance of credibility; for example, which websites or sources of information are perceived to be credible, and how this affects behaviour.

The chapter also identifies some of the different types of user, who respond in very different ways when they encounter problems online. These range from those who are easily put off going online if they encounter problems to those who are not at all discouraged from transacting online, even if they have encountered problems.

Key findings

Information-seeking was the activity that dominated participants' internet use, closely followed by **shopping**. These two activities were key for most participants, even those with lower digital literacy. Trade-offs emerged as being important: it became apparent that people **weighed up benefits and drawbacks** (often subconsciously) when deciding whether to engage in an activity online, and shopping and information-seeking were generally perceived as having the best ratio of benefits to drawbacks; hence making them the most prevalent.

Information-seeking in particular was seen as a **low-risk** online activity, and one with several important benefits to its offline alternative, such as speed, convenience and breadth of results. E-commerce also formed a core part of participants' online activity and their experience of this played a large part in determining their overall experience of going online. It was typical for those who were new to online shopping to opt for websites belonging to **high street retailers**. This was partly to do with people being more trusting of what is familiar, but also because, if any problems occurred, these could be **addressed in person** in the store.

When it came to **shopping safely online**, participants took a **diverse range of measures**, ranging from going by the general '**look and feel**' of a website, to checking to see if there was a **padlock** symbol in the address bar or even simply a picture of a padlock anywhere on the site. Peer reviews had become a core part of the online shopping experience and the official product description had become only the first stage in deciding whether to make a purchase. This was often the case even for those with low digital literacy. Participants' approaches to online security were often **ad-hoc, improvised, and inconsistently applied**.

Online civic activities were **infrequently performed** but there was also a lack of awareness of other ways to pursue these needs. For example, although people did not regularly access online information about their local council, such as recycling arrangements, they often found it difficult to suggest alternative ways of obtaining such information.

3.1 Information seeking was widely perceived to have the best ratio of benefits to drawbacks, making it the most prevalent activity online

Searching for information was stated to be one of the simplest activities to do online, and the effort required to learn how to do it was often felt to be easily outweighed by the benefits of speed, convenience, and the breadth of information available. Also, because this was typically the most frequently repeated online activity, even low digital literacy participants quickly became familiar with it, and were relatively confident searching for information online. And while not everyone knew what a 'search engine' was, all had heard of Google and used it frequently to search.

Participants felt that searching for information was the safest activity to do online because there was a perception that they were not required to input any personal information as they were 'just looking'. This was particularly the case among low and medium digital literacy groups. Participants felt they could generally click on any link until they were asked to input personal information on a site, and at that point they proceeded with more care.

Generally participants assessed the credibility of search results by looking at the relevance of the results, or the website address, and preferred to click on familiar and/or big brand sites. Among low and medium digital literacy participants there was agreement that it was better to only use the first page of search results, as these 'are the most popular' and after that 'it gets diluted' or could even be 'dangerous' as they believed that the further the results were from the first page, the more likely it was that the websites would contain viruses or spyware. There was little awareness that the 's' in https indicated that the site was more likely to be secure, although some had heard of this.

When participants were prompted to look closely at web addresses, several concluded that they would consider addresses containing numbers, or extra text, to be unsafe. For example, they would consider www.myhair382gum.com (a fictional example) unsafe but www.ghd.com would not raise concern. However it is unlikely that without prompted scrutiny many would have made this distinction. Government-related websites did inspire confidence, and anything with .gov or .org was generally considered safe.

3.2 The convenience and cost savings of shopping online outweighed its potential risks for most participants, making it another core activity

People's attitudes towards going online generally tended to be heavily influenced by their experience of online shopping. Medium and high digital literacy users had become adept at commercial transactions and said they were comfortable identifying good deals from trustworthy sources. Many participants said that online shopping allowed them conveniently to access a wide range of goods, including items that were not available offline, and, by using online reviews, to make informed purchases.

Participants' online habits were dominated to a large extent by big brands

With larger brands, participants felt there was 'safety in numbers', so that a popular site used by millions was perceived as being more secure than a small independent one.

'Big corporate companies and sites and brands don't get hacked because they have got the money to pay for the right programmers, to pay for the right programming.'

Male, St Albans, Medium

Larger brands were believed to have better security in place and to be more willing and able to cover costs should anything go wrong. Relying on big brands as a 'safety blanket' meant users felt they did not have to be on the alert for potential scams.

If low digital literacy users engaged in shopping online, it tended to be through the websites of familiar high street stores, unless the item was unusual and could not be found on the high street. For many less digitally literate users, a good introduction to the world of non-high street shopping was often through websites that had been recommended by their friends and family. Generally, medium and high digital literacy users had reached the point where they felt comfortable buying online, even from retailers they had not used before, as they had learned to discern which websites appeared official, and therefore trustworthy, and which appeared to be potentially harmful.

Low digital literacy users, who were the most cautious online, tended to search for information (for example, comparing products or holidays), but were much less willing to input their card details online. As mentioned earlier, they often accompanied their online activity with offline activity, such as going to see the item to 'make sure it was fine' and then buying it, either online or from the shop. For several participants, the only way they would buy online was from a high street store, so they could return the product in person if necessary.

Lucy – Shopping online should be avoided

Lucy is an 18-year-old student who uses the internet regularly but lacks confidence doing some things online. She appreciates certain positive aspects of the internet, particularly in relation to searching for information for her studies, and sees the benefits of the internet from a civic perspective:

'I studied politics and on one of the Government or Parliament websites they have a real-time, timeline kind of thing, which shows current legislations that are being proposed and where they are and what House they're in and if they're being vetoed and what's going on. And that's amazing. [...] Since I did that exam I keep looking at it still, just because it's actually really interesting.'

While quite confident in using the internet to search for information, Lucy is less sure when it comes to transactions. She only shops on two websites, and this is because these retailers have no 'real world' equivalent. While she is relatively comfortable buying from these sellers, she becomes overwhelmed when things don't go to plan:

'I never send anything back so I've got a collection of things, which I've received online, which don't fit. So I've ended up just giving them away or something because it's easier than sending them back.'

She struggles similarly with selling online:

'I've got a lot of clothes, a lot of clothes and I was like, yeah I've got to sell some. And I took a picture of it, it took me about 40 minutes to upload the picture but I did it. And then it was just asking me to do more things and provide stuff and it was completely beyond me, and again I was looking for a help service and there was just nothing there. I was calling up my friends, I don't know how to do this, help me. And then I was just like, that's it, I'm just going to have to be a hoarder.'

On one occasion Lucy had to buy a plane ticket online as part of a group holiday, and mistakenly purchased the wrong flight. This experience shook her confidence, and as a result she is now hesitant to explore buying from different vendors, particularly 'big ticket' items where the financial risk is greatest.

'Yeah, it scared me. And once you've clicked confirm, that's it.'

So, while less digitally literate users were making use of the wealth of information available for shopping, they were often less inclined than those who were more digitally literate to actually buy things online. This often seemed to be due to security concerns, or because they had experienced, or knew of people who had experienced, negative experiences when shopping online, such as buying holidays through companies which then closed down. An ongoing concern for participants with lower digital literacy was that their financial details would be stolen by hackers.

'There are so many people that are so good at computers that can hack it in a minute and if everything's stored online and

it's not policed regularly and safeguarded regularly it's hard for the person to trust what's online.'

Female, St Albans, Medium

'Once you put something into the cyber world it's done. If Gary McKinnon can hack into the Pentagon anyone can do that, that fundamentally shows that it's possible.'

Male, St Albans, Medium

Peer reviews were a valuable part of the online shopping process

When deciding what item to buy, it was very common for participants, including those with low digital literacy, to use product reviews; by specialists on dedicated review websites, but principally from user reviews, either on the website selling the item or on forums elsewhere, including Twitter.

'All you've got to do is see what people are tweeting about them and then you're going to get your feedback.'

Female, St Albans, Medium

Official product descriptions were therefore only one stage in deciding what to buy, and were also often given less weight because this was seen as just the 'sales pitch'. Peer reviews of products and websites had become for many an essential element of making the right purchase, and were sometimes the only way to verify the authenticity or quality of certain items.

'I was looking to buy some UGG boots. Now there are only certain websites that you will get real UGGs ... But then there are some of these smaller unofficial ones, they're actually fake UGGs, and I had to do all the research through the forums and whatnot because I was like, how can you get UGGs for 70 quid? No way.'

Female, St Albans, Medium

However, while reviews were important, they were not taken as the 'final word', and one person's opinion of a product would not necessarily determine whether or not it was purchased.

'I take it with a bit of a pinch of salt though because everybody likes different things.'

Female, Cardiff, Medium

Suspiciousness was aroused if there were a significantly large number of positive reviews, or if reviews were entirely positive. Also, if a brand or product had a large number of Facebook 'likes', while it was deemed more credible, this was also closely associated with marketing, and so online reviews were preferred.

There were no shared norms of what people do to stay safe online

There are a varied and contradictory range of methods that people employ to protect themselves.

- Almost all judge the look and feel of a site based on 'gut instinct'
- Many look for verified methods of payment such as PayPal or Verified by Visa
- A few look out for features such as 'https' and the green padlock

These methods are rarely employed consistently. For example, a person might have an antivirus program installed on their PC and believe that this keeps them safe, but then fail to use verified methods of payment (they would enter in debit card details when asked, etc).

Typically participants had an instinctive sense that a well put-together website, in terms of layout, look and feel, would be trustworthy. 'Amateur' web design would be the first feature to arouse suspicion. It appears that for many, the professionalism of site design was the key indicator of trust and they did not feel the need to look for other information beyond this.

For those that went beyond the look and feel of a website, there were a number of things that they looked for when deciding whether to trust a site. Verified payment features such as Checkout with Amazon, Verified by Visa, and particularly PayPal were associated with trustworthiness, and were seen as being a secure intermediary between the consumer and the company. A few also mentioned looking for an SSL certificate or whether the website was MasterCard security verified. The green padlock symbol in the address bar was also mentioned by a few, but there was little understanding of its significance. Overall, a lack of understanding of *how* these various mechanisms work to keep people safe meant that they were rarely used with any consistency.

In addition, a number of key points aroused suspicion, including requests for irrelevant information when transacting, such as date of birth, National Insurance number or even telephone number. One participant explained that he would be suspicious of a website if it did not have any advertising on it, as this would be a sign that it was not genuine. The quality of the advertising (for instance, if it looked 'professional' and was from a known brand) was for some an indicator of credibility. Believing it would help protect them if anything went wrong, a few participants had also taken photos or screen shots of order confirmations to prove they had purchased an item.

Users sometimes used offline contact details to ascertain the trustworthiness of a website. This might be by telephoning, although one medium digital literacy woman had even written to a company she found online, using recorded post, and because she received a written reply she took the company to be genuine.

Jackie (medium digital literacy) – A victim of fraud

Jackie is 26 and was in the midst of preparing for her wedding when she was defrauded online. Jackie is usually very careful with online shopping, preferring to rely on well-known brands, or on sites which use PayPal. On this occasion she had come across a wedding dress website which had really good deals on it. She emailed the company a description of the wedding dress she wanted, and they confirmed by email that they could send it. Having felt that she had now 'talked' with the company she believed that it was genuine, and was reassured by the constant

flow of communication she received from the site.

'They said 'Ok, we've received your order' ... I then got an email to let me know that not only had they got my order, it's been cleared, they're sending it out, so I knew it wasn't that bad.'

The website itself also had some security-related graphics which she took to be valid, but unfortunately this was not the case.

'It said 'secure transactions', there was a couple of bolts at the top saying that your transactions will be safe. So that made me feel reassured ... It came, but there wasn't anything in the box.'

Other mechanisms for staying safe online

Generally, where possible, participants tended to avoid buying online from abroad, presuming that if something went wrong, it would be much more of an ordeal to return the item and to get a refund. Import restrictions and taxes also put some participants off, especially if they had experienced these issues. For example, one participant had made a purchase of hair straighteners from Hong Kong, which were then seized by customs for failing an electrical safety test. He had paid by PayPal, but they would not refund him as the company had sent him the items. He just left it as he thought it was his fault, so 'learned his lesson' not to purchase from abroad. Another participant explained her story:

'I was on this website looking for Armani perfume, and it was a good price, not too ridiculously low, so I didn't think twice about ordering it ... but as soon as I smelt it I knew it wasn't ... So I actually phoned them, they were in Poland ... and I said, I know that this isn't an authentic perfume and they said, we're terribly sorry if you send it back to us we'll refund you. So I sent it back and I never got anything back, I just couldn't get hold of them again at all.'

Female, Cardiff, Medium

Several high literacy users found that a healthy scepticism was the best approach to avoid being scammed.

'Don't believe every offer you see, if it's too good to be true it probably is.'

Male, Glasgow, High

Often, however, people felt that there was no foolproof way to establish which websites to trust, so online transactions had a degree of 'faith' to them.

'It's a wing and a prayer, it really just is.'

Female, St Albans, Medium

'You have to have a bit of faith ... I think the fraudsters are getting much more clever, and the trouble is they're bound to become so smart in regard to duplication of official websites that unless you are very familiar with the formats and layouts ... We could all have problems. And I think that is fundamental.'

Male, St Albans, Medium

For transactions which were presumed to be unsafe (which for some users is all transactions) some considered using a credit card preferable to using debit cards (because credit cards provide protection for purchases over £100), although many did not distinguish between these two ways of making a purchase. A couple of participants had gone to the length of having a dedicated online buying bank account with limited funds and no overdraft to avoid the risk of having all of their money stolen.

People's behaviour is often contradictory and characterised by trade-offs

Participants sometimes set aside safety measures if the perceived benefit of a transaction was sufficiently great, such as finding a product at a much cheaper price. This focus on the end reward often led to people engaging in contradictory behaviour, such as resisting all online banking to avoid making their finances accessible to others online, yet at the same time being willing to shop online, despite this requiring inputting their financial details, sometimes into websites whose authenticity they could not verify.

It is worth reiterating that safety measures were used inconsistently, and in reality there was no 'checklist' that users went through to assess the trustworthiness of each site. This inconsistency stemmed from both a lack of understanding and also a belief that the methods they had been using had been working adequately so far to protect them, so they should stick to them. This set of personal beliefs resulted in participants sometimes putting total reliance on specific features, such as the website having a padlock symbol, while failing to recognise potential warning signs, such as being asked for a passport number in an inappropriate context.

3.3 Online communication and social networking were thought to be valuable by some, but were not seen to have sufficient benefits to be adopted by all

Email widely adopted as an entry-level activity

Email was perceived as a quick and useful form of communication by most people. This, coupled with the fact that it was seen as being one of the simplest and lower-risk online activities, meant that there was a favourable trade-off between benefits and drawbacks, so email had been widely adopted. Along with online searching and browsing, email tended to be the bare minimum that someone with low digital literacy would use the internet for.

'I can just about do emails.'

Female, London, Low

Participants tended to ignore messages from unfamiliar sources or those they were not expecting, being conscious of phishing (although they did not tend to use this phrase),

although not all users were aware of such scams. A few participants mentioned not clicking on a link in an email to go to the bank's website, as frauds can be conducted this way, but rather find the bank's website directly. Generally, however, participants saw unsolicited emails from unfamiliar sources as on a par with cold calling, that is to say; they should not be trusted.

'I'd only really look at emails that are sent to me if it's a company I've used.'

Female, St Albans, Medium

Social networking had been widely adopted, but some limited their activity due to privacy or security concerns

Many participants used social networking sites, particularly Facebook, and they quickly found them to be an integral, and time-consuming, method of communication and a 'go to' source of entertainment, or at least diversion. For most participants, any potential risks and disadvantages of using social networking were relatively insignificant and outweighed by the perceived advantages (a quick, convenient and fun way to make connections and keep in touch with friends). Even if they had minor concerns, the trade-off for them was a favourable one and they would continue to use these sites.

Several participants, however, rejected social networking sites on principle when making their trade-offs between benefits and drawbacks. This was mostly because they preferred not to socialise and share their information in such an apparently public way; they felt that the very nature of the sites would compromise their privacy.

'I don't do Facebook, I don't believe in people seeing what you do with all your life or whatever you do. I just think that your life is private and I want to keep it that way.'

Female, St Albans, Medium

There was also a concern that, once online, their information was 'out there' and could be passed on, and that to really keep something private it needed to be kept offline.

'I don't like to give too much information to people, because I feel at the end of the day you never know where it's actually going to end up at.'

Male, St Albans, Medium

Participants also noted that, once available online, the information could be there 'forever'. There were widespread concerns about how this might affect young people, who might unwisely post inappropriate comments or pictures on social networking sites. A few (particularly lower digital literacy participants) had fears about security as well as privacy. For example, some were concerned about status updates giving away the fact that they were on holiday, which could make it easier for others to burgle them.

'My sister puts things on there like 'Off to my uncle tomorrow for three weeks'. And I say to her, you shouldn't put that

information on there because you don't want everyone to know that your house is going to be empty for three weeks.'

Female, Cardiff, Medium

To combat concerns about privacy and security, a handful of participants had taken to using false information such as dates of birth or using their middle name, although many had never considered doing this.

A primary concern about social networking sites was being contacted by fraudulent people, or those who might otherwise wish the user harm. A few people expressed concerns about vulnerable people and children being contacted in this way, either by bullies or by predatory adults.

'A person I used to know a couple of years ago, her daughter was like 12, 13 then and some of the profile photos she was putting on of herself all done up and the clothes she was wearing, I was like oh my God do you know she's on being seen by goodness knows who like that?'

Female, Cardiff, Medium

3.4 The benefits and drawbacks of online banking were often perceived as evenly matched; this proved a divisive activity among participants

Participants had strong views regarding online banking, both for and against. The benefits expressed included convenience and the ability to avoid queues.

'When you work in different jobs, different cut-off periods, different pay scales, you want to know that your money's in your bank if you've got direct debits coming out or if you've got bills to pay. You're not having to run to the cash point every five seconds.'

Male, London, Low

Other participants were very cautious about online banking, and simply refused to engage with it. This may have been due to unfamiliarity, but security concerns were frequently mentioned; specifically the idea that, by banking online, their finances were now accessible or even 'located' online, making them more vulnerable.

'I was very sceptical; I'd been into the bank, I'd spent ages deliberating whether to go online, it was a bit like doing the MMR job, I was there for hours talking about it.'

Female, London, Low

'I just don't trust [online banking]. People can hack into anything. I don't like the idea of getting hacked into and I'm worried that they might take more out than I've got ... if

somebody hacked in and takes my overdraft allowance what am I going to do to pay it?’

Female, Grimsby, Medium

‘If somebody hacks your computer for whatever reason, and they’ve got your details, it’s something that you can avoid and not put yourself at risk, which is preferable to [banking] online.’

Male, Leamington Spa, Low

Participants’ refusal to bank online, and their concerns about people accessing their finances were often in apparent tension with their other practices. They might, for example, be happy to enter their financial details online when shopping and might also have PayPal, iTunes and/or Amazon accounts. It therefore appeared that participants did not perceive entering card details, or using PayPal, as being as risky as banking online. PayPal, for instance, was perceived as safe, and if something went wrong with a credit card purchase, participants felt that they had some measure of protection from the card issuer.

‘If it doesn’t have PayPal or Verified by Visa I won’t shop on the site.’

Male, Grimsby, Medium

Melanie (medium digital literacy) – Limited online by a lack of trust

Melanie is 41 and a full time mother to two children. She goes online most days. She will check her social networking account almost daily and has also been doing a lot of browsing and searching recently since she is organising her wedding. She uses a laptop and a smartphone to go online. Melanie embodies quite a few contradictions in her online behaviour. Although she initially claims not to shop online, on probing it becomes evident that not only does she shop, but she also does her banking online.

‘I do trust it, I’m with NatWest, I go online, check my account all the time. I’ve done transfers on it, but then went into the branch as well and checked, I’m very suspicious ... I get all nervous and think, oh, and then I scurry along and go and make sure it’s OK.’

She also reveals that she does her grocery shopping online:

‘It’s really convenient because I’ve got one up the road and they deliver free. I plucked up the courage, pushed buy and everything went through fine on my account, I was very brave, and since then I’ve carried on using it, I trust it.’

Melanie says that she trusts this particular retailer because she is able to contact it in person.

'They're local as well, so I always feel so I always feel if I've got a problem I could always go in to the store. Online, I don't know who these people are, they're behind an email address or a website.'

She also cites the fact that the service has been so far reliable.

'Nothing's made me not trust them. I've always had good service, there's never been a problem.'

While this inconsistency was rooted primarily in a difference in perception, there was also a sense that the trade-off was more favourable in the case of shopping: the benefits (i.e. the product in question, probably also at a cheaper price) very often outweighed any perceived security risks. In the case of online banking, the benefits are less tangible (e.g. avoiding queues); so if the person had security concerns, these would be more likely to prevent him or her from doing the activity online.

Through analysis of participant behaviour and comments relating to banking, it emerged that participants were more focused on matters of security than when they were doing online shopping; in the latter case they were more likely to be thinking about their purchase, or about delivery or refund policies, and so on. Entering card details was simply a part of the process, whereas with online banking the focus is solely on finance and personal information, and putting this information 'up online'. Participants therefore associated online banking as being higher risk than online shopping and with far more at stake if something went wrong, such as all their financial information being leaked or stolen.

Another factor affecting participants' differing attitudes to shopping and banking online is that they sometimes saw their online shopping transaction as an isolated element of their finances, which could be 'quarantined off' if the security were compromised, unlike banking where *all* of someone's financial details and financial history was available. This was particularly the case for those using verified methods of payment such as PayPal, which were seen as separate from their main bank accounts.

Others positively wanted to keep banking face-to-face simply because it was what they were used to; they preferred having a physical paying-in book and pieces of paper as it felt more reassuring than a 'virtual' transaction. This applied particularly to the older generation who themselves admitted that it was partly a generational matter.

'It seems more official when it's all on paper ... It's probably just down to having the physical bank book in my hand and saying that's mine. If I'd been born 40 years later, that probably wouldn't bother me, but it's just the physical thing, you've had a bank book since you were a child.'

Male, Leamington Spa, Low

For those with lower digital literacy there was also the issue of lacking confidence and competence online, and they therefore saw online banking as a particularly difficult activity.

'I just thought, knowing me I'd probably mess it up.'

Female, Leamington Spa, Low

3.5 Many used online public services infrequently; were unaware of offline alternatives, and placed high levels of trust in this type of website

'Public services online' includes content or interactions relevant to people as citizens, for example concerning local services such as schools and libraries, and local news. Citizen activities include job hunting, house hunting, reviews of local schools, and news and weather reports.

In terms of the value that participants placed on being able to access citizen-related information online, they simply expected that it would be available online, and if it were not, people felt inconvenienced and did not know what other avenues to explore for the same information.

Some low and medium digital literacy users, however, felt strongly that there should still be a face-to-face or telephone option as they did not want to be 'forced online' and some felt that speaking to someone was the only way to get their point across or to understand, say, a local authority's rules and regulations.

While participants often had to be prompted to think of citizen-related uses of the internet, there were a few who felt passionately about the capacity of the internet to support activism:

'Petitions. I belong to a lot of animal welfare groups and recently we petitioned our MPs to try and discourage Canada from culling the seal cubs and it was so effective that they actually put the cull off. And now we're trying to stop the badger cull.'

Female, Cardiff, Medium

Participants tended to seek out local information like gym or restaurant opening times and menus. Some less digitally literate participants were unaware that such information was available online. For most, however, it was difficult for them to remember or imagine how this information could be accessed without the internet, with resources such as the Yellow Pages or the Thomson Local book being all but ignored, particularly among more frequent users of the internet. Using maps on devices, especially mobile phones, was another embedded online behaviour, as was getting local travel information, such as train or bus times.

There were high levels of trust around citizen-type information. The UK government websites, especially those with '.gov' in the web address, were considered by all to be trustworthy. Among medium and higher literacy users, there was considerable engagement with government services; paying council tax and doing tax returns online were commonly-cited activities, which done online were felt to be quick, easy, and avoided the need to contact HMRC by phone.

'It's the speed: click a button, got my information, move on.'

Female, Glasgow, Medium

One area where participants were more sceptical about the public benefit of the internet was self-diagnosis of health problems. While some felt that the internet

functioned well and informed them accurately, others felt that there was too great a danger of misdiagnosis, even from trusted sites like NHS Direct.

'You go online, about say, for men, prostate cancer, you learn a lot but you can actually worry yourself into a grave. You can actually overwhelm yourself by too much information.'

Male, St Albans, Medium

Overall, the trade-off between the benefits and drawbacks of conducting citizen activities online was largely a positive one, particularly in terms of convenience. Participants carried out these activities relatively infrequently online, mainly because they needed to do them less often, in comparison with other online activities such as information-seeking and shopping.

4. Personal data security issues

4. Personal data security issues

This chapter explores participants' differing levels of awareness and concern about how their personal data is captured and used, including their understanding of cookies and their perceptions of how their data are protected. This chapter also presents some typologies illustrating participants' differing approaches to data protection.

Key findings

Participants admitted to a **lack of understanding** of how their personal data are stored, used and transferred online. Many were happy for companies to use their data, with their consent, but some were concerned about the **consequences** of this.

Participants lacked awareness: concern was expressed only after prompting

Overall there was **little spontaneous thought or concern** given to online data issues. Most of those who expressed concern did so only when their attention was drawn to it. Even on prompting, many were unconcerned about their data being shared among companies, feeling that no great harm would come to them, and that by co-operating with the companies who want to use their data, they would be able to **benefit from more personalised offers or financial incentives**. Others were concerned, but it was common for even these participants to feel apathetic about how their data are shared with companies, feeling such matters to be **beyond their control**. Most had **little or no awareness** of how and why their information was **used, stored and transferred online**, and many participants lacked any real understanding of cookies and targeted advertising. There was a widespread assumption that **personal details were sold on**, sometimes even if they took measures to prevent this (e.g. 'unticking the box' to allow contact from third parties).

Participants expressed that informed consent should be sought: consequences were key

Participants said that **transparency** was important: they wanted their **consent** to be sought before their details were sold to third parties, or at least to be **informed** of this. They felt that they ought to have **ownership** over their personal information. While participants had previously given little thought to this topic, the greatest concern on prompting related to the **consequences** of data storage and transfer. Nearly all participants found unsolicited emails and text messages to be **invasive and annoying** (but nevertheless **inevitable**, since it wouldn't stop them using sites and services that they needed online). The most common methods used by those seeking to protect their data online, and thereby themselves, included using **payment methods** like PayPal or credit cards as these were felt to offer more protection should something go wrong. Unticking 'share my details' boxes was another commonly mentioned method. Others had more idiosyncratic approaches to staying safe online. But most participants did not have full strategies; they had **individual and fragmented approaches** to keeping their data secure, perhaps paying attention to just one or two factors.

4.1 Participants lacked awareness: they expressed concern only on prompting

Generally, participants had only vague ideas about what happens to personal data online, and whether they are stored securely. These issues were not at the forefront of participants' minds as they browsed online; **many had not considered them at all**, and most expressing a concern did so only when prompted.

But many were **conscious that their personal information was being used in ways which they had never knowingly agreed to**, such as for contacting them with unsolicited marketing emails, or using targeted adverts. Typically, participants had come to accept the situation because they did not understand the **mechanisms** behind this use of their data; for example, how their data was first captured, or how it had been passed on. Some had become unhappily resigned to this issue, and felt that they were not able to rein in this use of their personal information. Others were relatively relaxed about it, and felt that receiving such marketing was a fair exchange for engaging with companies. This was particularly the case for younger users, for whom this was simply 'the way of the world'.

When asked hypothetically whether they would be willing to sell access to personal information such as their Facebook account, several participants stated that they would, but seemed unsure of what this would involve or indeed why such information would be of value to a company.

'Everyone would sell their email for £10 off their next shop.'

Male, Grimsby, Medium

There was widespread lack of knowledge of the role that cookies play

While participants are more aware of cookies due to recent EU legislation¹ requiring websites to be more explicit about their use, across all levels of digital literacy there was only patchy awareness of the role that cookies actually play.

'It always says at the top, this website will use cookies, I don't know what that is.'

Female, London, Low

'No, no those things that keep popping up, they drive me mad. I didn't understand what it was but, I think it's a tracking, it tracks something.'

Male, London, Low

'I notice [the first time] I go onto something and they say please make sure that cookies are enabled, but I don't know how you enable them or disable them, I've got no idea.'

Female, Cardiff, Medium

¹ Introduced in 2011, see: http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies.aspx

So for many, cookies were not affecting their overall browsing behaviour; they simply tried to get rid of the pop-up that was obstructing them from viewing the website. Those who did have some understanding of cookies generally believed that a cookie 'just remembers you' when you visit a website. Typically, participants lacked an association between cookies, and how targeted advertisements appear, although some did make this connection, and often perceived cookies as malicious software:

'They want to know you, they want to advertise, they want you to buy, they want to know who you are, what you do, that's a cookie ... It's like a little spy on your shoulder that literally goes 'Oh I see you like that today'.'

Female, St Albans, Medium

'I would say a cookie is a virus that takes in all the information that's around it and shares it.'

Female, St Albans, Medium

These individuals often make an effort to remove the cookies from their computer, with some participants even installing software to do this automatically.

Jane (medium digital literacy) – No trust of cookies

Jane is 26 and works in education. She has the latest smartphone and tablet, and a powerful laptop. She uses the internet daily, mainly responding to emails. Jane has clearly thought about all kinds of security issues. She recently stopped her smartphone and tablet from connecting, because she does not want all of her personal information available if her tablet falls into the wrong hands.

She does however still shop online, although she prefers to use sites where she can pay by PayPal, which she trusts, as it acts as a secure intermediary between her and the online retailer.

'PayPal don't give out your actual information, it's like the person in the middle from your personal details, and that's why I like it.'

But Jane is concerned about whether her information is stored properly on other sites.

'If there was someone to police it properly and someone who went in, and it's a hard job, but actually goes in and actually polices where our information's kept, I think it would be more reassuring ... There is so many people that are so good at computers that can hack it in a minute and if everything's stored online and it's not policed regularly and safeguarded regularly it's hard for the person to trust what's online.'

In particular she is concerned about cookies and clears them from her smartphone many times a day.

'OK, so when I'm using my phone and my iPad the ones that I'd use, like cookies from certain things to make it a little bit easier would be

like your Facebook, like the cookies that come along with that. There's cookies on I allow them but then I go and I delete them again after the use of my phone because I don't want them to stay there for long. Literally I do it at least four times a day.'

Jane's general security fears may stem from a bad experience she had when a website that she had only used once started taking unauthorised payments from her bank.

'There are places that I don't trust with my information and because literally someone's gone into my account and [my bank] had to help me sort that out; it made me really nervous about a couple of websites.'

Jane still shops online, and if a website doesn't use PayPal she has found an approach which suits her security concerns:

'If it's new to me and I want to get something from it, I use an account that is really dormant and I don't have a lot of money in, just the essential for what I'm going to pay for. And I use that for a couple of times and see exactly if I have any issues.'

Targeted advertising was not fully understood, but did not raise concerns since it was seen to have potential value

Many participants were **accepting of targeted advertisements**, despite not knowing how they worked, because they made life more convenient (e.g. if the advertisements showed them offers that were relevant to them).

'Or at the bottom you get people who viewed this also viewed these and a long thing of like something you might like, because somebody else viewed the same thing ... it's better than recommending stuff that I don't care about.'

Male, Cardiff, Medium

For such participants **these adverts did not raise data protection concerns**, despite it being evident that some information about them had been passed on without their knowledge. If they thought about data protection at all, they often assumed that, because the brands advertising are typically well-established, they would have equipped their IT systems to ensure that personal information used for targeted advertising would be stored securely. Accordingly, such users did not make any efforts to avoid targeted advertising, as they saw it as benign.

'I think it's quite clever because it's like how adverts for your TV are catered for the kind of people that they think watch Coronation Street. So it's kind of like personalising your adverts on your laptop because they can't advertise the way TV does, I suppose. It's clever.'

Female, Cardiff, Medium

Other participants were more concerned about targeted advertising, although they also did not necessarily attempt to avoid it. This was because they did not understand how it was happening in the first place, or because they were resigned to the idea that their data had already been passed on; that their information was now out in the 'ether' and it was now too late to try to make any serious effort to protect it. Targeted advertising had simply become **an irritation that they had to deal with**:

'It's just being put in your face and it's annoying if you're not particularly wanting to look at that at that particular time.'

Male, Cardiff, Medium

Some, however, find the occurrence of targeted advertising **sinister** and **mysterious**.

'I found it intrusive. Very intrusive. It's Big Brother isn't it? ... It creeps me out. I'll be there looking at a pair of shoes and then for the next two weeks every website I go on shows me that pair, advertising. And it's the scariest thing ever, I thought I was going crazy. I thought I was being, well I am being stalked.'

Female, London, Low

4.2 Participants stated that informed consent should be sought: consequences are key

When prompted, people attached a variety of concerns to giving out personal data

Although data security was rarely top of mind, when exploring this topic in discussions a broad range of concerns emerged. These ranged from the more serious, such as identity theft and having money stolen, to the inconvenience of cold calls and emails. For some, the **principle of their data being passed or sold on without their consent** is their main complaint. While they did not fully understand the mechanisms of exactly how their details were passed on, some were well aware of the consequences of having personal information shared or sold on:

'Since my partner went on [a payday loan site] the amount of companies that are sending her text messages, emails, we'll offer you this, we can offer you that.'

Male, Grimsby, Medium

Calls and messages about Payment Protection Insurance received particular mention. Some participants were not sure what to do to avoid receiving spam marketing, and even those who did know stated that it is not always free of charge to do so. Certainly many felt that websites were needlessly collecting data, and this made them suspicious about the ultimate purpose of this.

'A lot of websites now though, to use them, to shop in them they'll make you register with them first and that's when they

get the extra details that they don't need like your telephone number and stuff like that or, you know.'

Male, Grimsby, Medium

For the more concerned participants, registering on websites, and allowing sites to save information like their bank card details, felt risky – they feared that their personal information was vulnerable to being accessed by those for whom it was not intended.

For **low digital literacy users**, their concerns tended to be based on 'scare' stories in the media, as well as their friends' and their own experience.

Lauren (medium digital literacy) – Experiences of compromised security

Lauren is 40 years old and a mature student. She uses the internet very frequently, particularly on her smartphone since she lacks confidence with computers and finds this the easiest device to navigate. Although a reasonably heavy internet user, Lauren takes steps to protect herself online, following several negative incidents:

'If [my phone] didn't have a bionic antivirus on it I wouldn't be using it. I've had my PayPal hacked, my internet, my eBay attacked, my Facebook attacked. So I will not go on the internet if it was not, it hasn't got secure on the website then I won't go on.'

Each time that a negative incident like this has occurred, Lauren has taken the necessary steps to rectify the problem:

'The first time it was through my PayPal account so I've messed about getting through to PayPal and then they finally sorted it after the hassles. But then [the second time was] through the bank when I'd bought something online not realising I'd put my card details in and then all of a sudden there were other payments going out. So I went into the bank and I said, excuse me, I've not bought this, don't use this company any more. I bought one thing. So they've said, 'Oh, yes, we have got them on the list of fraudulent companies, here's your refund.'

Although she resents this inconvenience and has become more aware of online security as a result, the experience has not deterred her from using the internet. She has sorted out the problem, brushed herself off, and continued from a position of greater awareness:

'If it's not got a padlock and says Secured by Visa I will not entertain it. It's got to be in big, bold letters saying, we are secure, we are not going to rob your money.'

Medium and high digital literacy users have similar attitudes; as their internet use broadens to include transacting with a wider range of websites, they have inevitably had the occasional bad experience, with their data being misused, or accounts being hacked. Generally, however, as these more digitally-literate users have become used to the benefits of the internet, their attitude has been to '**get back on the horse**' after running into such difficulties.

Several participants, across the levels of digital literacy, simply **assumed that their data would be used by companies for legitimate purposes**; for example, if they were asked to provide their phone number, this would be so that the company could contact them, not in order to sell it on.

'You'd think they'd just use it for deliveries, if they need to contact you.'

Female, Grimsby, Medium

Participants did not think much about why companies might want this information or how they might have used it; for example, they may not associate entering data on one website with spam emails and other unsolicited marketing from another site.

Suspensions may only be aroused when the information asked for appears to be out of context so, while participants were happy to provide their passport number when booking a flight, if the same information were required when shopping online, this would 'ring alarm bells'.

The ability for data to be attributable is a key factor in willingness to share

An important difference was whether or not the personal data being passed on was attributable, enabling **it to provide a direct connection to an individual**; this might be their name or phone number, but could also include their bank details or National Insurance number. Typically, if the data was not attributable, they thought it was less of an issue, although on reflection they felt that they should still be asked for permission before it was passed on, as a courtesy. For some this was the case even if their data was being used for legitimate purposes such as non-attributable medical data being used by the NHS and government to develop new treatments or public health initiatives, a scenario which is explored in Chapter 6.

Participants were **unhappy at the idea of attributable data being sold** on to third parties for commercial purposes, although they often had the sense that this had occurred at some point, and that this was why they were receiving various unsolicited marketing and spam. There was, however, only patchy understanding of who or what was collecting the personal information and then selling it, and little notion of who was buying it and why it was of value.

They also made distinctions between attributable data types, to explain which type would be most worrying if it were to be leaked or fall into 'the wrong hands':

- IP addresses were typically of least concern (although a few did classify these as attributable information which links back to them);
- Next in order of concern - their contact details (name, address, telephone number)
- Medical details and financial details caused the most concern, being seen as potentially the most damaging. Likewise, passport and National Insurance numbers were felt to be information that it is very important to avoid giving out carelessly, the latter two largely in case of identity theft.

'If you've got my date of birth, and my medical history, that's enough to identify me as far as I'm concerned.'

Female, Glasgow, Medium

'Once you give certain things like your National Insurance and passport number, they can, they know everything but everything about what you do.'

Male, St Albans, Medium

Users take measures to minimise the extent to which personal data is known or shared

While there were some, typically low digital literacy users, who avoided providing any personal data when they went online, and some who were entirely unconcerned, there were others between these two extremes who took a range of measures to minimise the extent to which their data was known and shared:

- The most common was **to avoid the 'save details' or 'remember me'** options in order to prevent a website permanently storing their information.
- Participants also typically **avoided the 'share my details with third parties'** option, and they were also confident that doing this would effectively protect their data.
- Some **deleted their web browsing history** and cookies regularly. Another, albeit less common, strategy was for some participants to give **partially incorrect information** to avoid identifying themselves fully; for example, providing a fake date of birth or phone number.
- A few also had a **separate email account** for dealing with websites which they thought would lead to them being spammed.
- One participant, with medium digital literacy, had set his computer to clear all of his browsing data and cookies every time he signed off his computer, in case his laptop fell into the wrong hands.

While many participants were using these measures to avoid unwanted consequences, it was generally only the less digitally literate users whose concerns about data were reducing their overall usage or significantly changing what they were prepared to do online.

'That's why I never give out my personal email, ever ... I've got another one that I give out.'

Male, St Albans, Medium

People make trade-offs when considering whether to share data

Although some participants were happy simply to give out their information to any website, they more typically tended to make **conscious trade-offs** when deciding whether to provide personal data. As a rule, participants were **willing to input their details for the convenience of using online services**.

'Yeah it is worth it; you weigh up the pros and the cons and you think, well, to be honest, yeah. If you could trust the company or whatever then you don't mind.'

Male, London, Low

Typically, users often traded the security or privacy of their personal data in order to get a particularly **good deal**; for example, participants might be enticed by online offers into buying from an unknown website, as in the case of the woman who purchased her wedding dress from a site in the US that she had not used before, because it was such a good price, although it did turn out unfortunately to be a scam. Others, in seeking riskier deals, such as buying from a poorly reviewed website, made extra efforts to protect themselves, such as by using a credit card rather than a debit card, for the added protection that credit cards provide.

Often participants had come to accept a degree of 'hassle' resulting from going online, particularly from e-commerce, and **expected unwanted follow-up contact and third-party marketing, seeing it as unavoidable**.

'Even recognised websites, sometimes I put my emails in and I say to myself, oh no, this is going to be a nightmare, because I just get bombarded with presents and 'You win for free' and I've got people calling me, 'Oh you've registered online, do you want a free DVD?' I said, there's no such thing free, what do I need to do? Oh you just have to switch your gas, I said, well the DVD is not free then.'

Male, St Albans, Medium

'I was just looking at some kind of baby website once, right, and they told me to put my mobile phone number in, so they were going to send me a text message with a code that I had to put in to get onto the website. So I done it, and it was a couple of weeks later, I got a phone call from somebody asking who my gas and electricity was with and if I wanted to change it.'

Female, Glasgow, Medium

Loyalty cards are an example of a transaction in which many participants were willing to provide their data and in return they received some benefit in terms of discounts or points. But awareness of this trade-off was not universal and many were unaware of the mechanisms behind loyalty cards, with one participant believing that they were used only for helping with stock control. Some participants also noted that for some services, such as getting a credit card, it was a pre-requisite to reveal personal

information. If this information was then sold on, there was a **feeling of powerlessness** about this.

'In order for you to get anywhere you've to put that information out there, right? And what they do with that information, God knows. They could easily, we've heard about stories where they sell it to other companies and stuff like that. But you're almost powerless to all that kind of stuff really.'

Male, London, Low

'I do feel any site you have to join and you have to give them your name, address, phone numbers; I think nowadays you're saying to yourself, look, don't be silly, it doesn't matter; Facebook will sell it. It doesn't matter who you register with. Even those jobs sites I'm on, I'm getting things from other job sites that I never even knew about.'

Male, Glasgow, Medium

4.3 Typologies and case studies

By observing the range of approaches participants have when engaging in online transactions and providing data, it is possible to build up typologies of users who behave in similar ways. These range from those who are very cautious in their interaction, to those who avoid only specific types of websites, all the way to those who are almost undiscerning in where they will enter their personal data and try to buy from. In this section we present four different typologies and accompanying case studies.

Brushing it off

This typology is common among medium or high digital literacy users and represents many of our participants. They have had enough positive experiences online that if they experience a loss they would usually write it, with no reduction in their online purchasing behaviour, apart from possibly avoiding the 'problem' website. Occasional problems are seen as the price consumers pay for the convenience of buying online at the best prices, and they take care to avoid them in the future. They are not particularly concerned about financial details being stolen, or identity theft, seeing these things as very rare.

David (high digital literacy)

David, 32, is happy shopping online and putting his details into voucher sites. He says he will carry on providing his personal data until something seriously bad, such as having his identity stolen, happens.

'It just doesn't bother me. It's just a horror story, isn't it? If it does happen, if you know someone it's happened to, then fair enough, I think you'd be a bit more cagey but it hasn't happened to me so I don't care ... I'll just stick it all in. If something happens then fair

enough.'

He feels that it is statistically unlikely that anything bad will happen to him because of how he behaves online.

'The thing is as well is, what you've got to remember is, I know it's big horror stories but it rarely happens. It genuinely rarely happens. You've got to think how often do you actually use the internet anyway? It's every day for me.'

David does not think that his online transactions are any riskier than his offline transactions, and he does not feel that his use of the internet is significantly increasing his chances of his data being misused.

'If someone's going to defraud you it doesn't necessarily mean it will be because of what you've done online. Anyway, your banks do protect you for that. If you say, look, this is what's happened they do, you do get it all back.'

This is not to say that David's experience of going online has always been smooth; he's bought products which he has had to return, but this mainly means that he tries to buy quality products when he can, rather than going for the cheapest.

Once bitten, twice shy

This typology is most common among low digital literacy users. They tend to belong to the C2 or DE socio-economic groups, where financial losses are likely to have more of an impact than other groups. They are more nervous online and more reluctant to purchase items. When something goes wrong they feel their fears have been confirmed, and they become more mistrustful of the web than ever, and avoid all online transactions.

Marion (low digital literacy)

Marion, 46, treats the online world with considerably more caution than the offline world. She is loath to enter personal data, especially financial details, online.

'I got the telephone number off the internet and I actually phoned them up and gave them my credit number. I didn't put it online. I didn't trust it online because not just them can get it. I don't know but I imagine that people who want to can also get it.'

Marion feels that using the internet leaves her much more exposed to problems like identity theft.

'If people are going to steal your identity they'll get it off the internet. And they can't get it off you, they'll get it off the next person on the internet. They weren't going to mess about phoning up your bank or doing.'

Marion does receive spam and unsolicited texts and assumes that at some point her information

has been sold on, leaving her even less inclined to input her details online. Marion's rules are not without exceptions; there are a handful of websites she does trust, despite not having any way to tell which websites have passed on her details:

'Unless it's a company I've used loads, where some of them, a big company, like Next, I would leave my details on it. Because I've had it a long time and never had any problem with it. They've got a secure website.'

The cavalier

These are likely to be low or medium digital literacy young people. They will do everything online, using websites and services almost without discernment, and will consequently get spammed and even defrauded online. This does not, however, alter their behaviour, which continues unchanged.

Alan (medium digital literacy)

Alan is a 26 year old retail manager who uses the internet fairly regularly and is unconcerned about many aspects that others find potentially troubling, such as safety and security. He accesses the internet primarily using his iPhone, using it mostly to do his banking and place bets online. He is unconcerned about security when doing online banking and speaks of the benefits of being able to do this on his iPhone:

'You don't have to wait for somebody to answer your call. You don't literally have to leave the house, so it's got lots of benefits.'

Alan is quite happy to enter his personal details online (for example, telephone number, email address) whenever they are required. When confronted with terms and conditions he will generally click to agree to whatever is needed by the web page in question. He has never experienced any security threats or problems as a result of this, with the exception of junk emails which he does not read:

'I just click and past it, just yes, yes, there are X wee box. [I get a lot of junk mail but] I don't even read it. I just, I never have. But I've never had any real problems with it, cutting past it.'

Alan gets approximately 30 junk emails daily, as well as sales text messages sent to his iPhone. This is, however, only a minor annoyance to him, and doesn't affect his carefree attitude and behaviour online. He is aware that his details are being sold on (since he is contacted by many apparently unrelated companies) but is content to simply delete junk emails and not answer his phone. Even when his computer was infected with a virus as a result of his online activity, he simply had it cleared and continued as before.

The conspiracy theorist

A minority typology, these are likely to be older males who are very opposed to the idea of their data being shared. They may believe that the government is monitoring all communication, emails and phone calls, for key words which could indicate illegal or terrorist activities. They are highly resistant to sharing information about themselves. In all transactions they go to great lengths to ensure that the person or

company they are dealing with is legitimate.

Martin (medium digital literacy)

Martin claims to be a very suspicious person. He states that he is unwilling to provide his details online, and is aware that even his IP address is information which could easily be linked back to him by someone who knew what they were doing. He says that if he can avoid it he tends not to use his real details but rather provides made-up information.

He is very aware of the 'thirst' companies have for his information, and worries about others accessing information about him or his wife through the iPad:

'When I was setting my wife's iPad up and I was going to put Chrome on it, and it suddenly come up with a page, and I started reading. The usual, everybody just ticks a box, but I thought I'm going to read this, and I cannot believe that you're giving them access, so they can access your camera in your iPad any time they want.'

He also highlighted the potentially confusing way that data protection options can be presented:

'It used to be, even my laptop, you had to tick the boxes, but now I noticed my wife's iPad, you've to untick the boxes.'

He is meticulous about 'vetting' which programmes he allows onto his computer.

'I do [read the terms and conditions]. I started reading everything, and it really made me suspicious ... I've got a pal that actually puts a plaster on top of his laptop camera because he doesn't trust it.'

Martin also refused to put Google Chrome on his wife's iPad as he was concerned that Google would be able to watch what she was doing:

'The three headings came up saying that they could get access to your camera in your iPad. They can access anything. Anything you key into the iPad, you're giving them permission to access.'

Recently Martin sold his daughter's bed through Gumtree, but, as ever, he was on guard:

'I'm a very suspicious person, very, very suspicious, God help people who speak to me on the phone. Sometimes some people say to me, you are working for the FBI? I say, no, I'm not, I'm just very careful. And that's what I do, I'll just speak to people and if I don't like the sound of their voice I don't care about the money, I don't care about anything else, I just move on.'

However, despite all of his security concerns and the measures he takes to protect himself online, it became evident that Martin in fact enters a considerable amount of information online, for shopping and even banking:

"I basically do most things on my laptop [...] Do quite a bit on it, basically do all my banking on it, do all my, paying my bills on it, do shopping on it."

5. Rights and responsibilities

5. Rights and responsibilities

This section looks at some of the social norms of internet use. It begins by exploring how participants felt that people's online behaviour differs from their behaviour offline and the reasons for this. It then examines questions around rights and responsibilities online, using scenarios to draw out the range of opinion on what is 'proper behaviour' online.

Key findings

There was a broad assumption that **online rights and responsibilities should be the same as those offline**. However, participants recognised that this was an **assumption** of their part, and that they were **unaware** of what their rights actually were.

In general it was felt that the internet is a **place of freedom**, where people are at liberty to express views; however, in turn, others are at liberty to create or join spaces where certain views won't be tolerated. Participants were not concerned that a site might reject or silence certain comments, as long as **moderation policies** were explained. However, as the use of social networking sites, particularly Facebook, had begun to feel almost obligatory, some found themselves in **unfamiliar social environments** in which openness and public 'over-sharing' were encouraged.

Participants were less confident about the **official recourse** available to address inappropriate or immoral behaviour online. Offline, they broadly knew what to do if someone was behaving badly, but online they were far less sure. The online world was seen as rather like a **foreign country** where what is permissible is unknown and the lines of accountability are **unclear**. In this instance people responded in broadly three ways; they may:

- 1) **take extra care** because they feel that there is no official recourse if things go wrong, an approach which can act as a barrier to further activity;
- 2) **act as normally as possible** maintaining accordance to their sense of what is acceptable behaviour offline; or
- 3) **take advantage of the apparent freedoms** by acting with less regard for others and for the societal conventions that exist offline. This approach can be harmful to others but also, ultimately, to the person posting themselves.

High-profile cases illustrating possible **consequences** of posting on Twitter or Facebook had given some insight into what is permissible, and had encouraged participants to think more about their own and others' responsibilities online, although such piecemeal news coverage had not led them to build up a comprehensive picture of what is and what is not officially permissible.

Overall, people wanted the internet to remain a place of freedom, **constrained only by what is legal**, although they believed that **websites should also take responsibility** in ensuring that exchanges are not harmful, even if not illegal.

5.1 Participants recognised that people behaved differently online to offline

Participants acknowledged that communication, particularly on social networking sites and online forums, tended to be **less inhibited** by the social norms present in offline dealings. They felt that people generally communicated less responsibly, and with **less regard for the consequences**. Participants also noted that online communication (again particularly on social networking sites and forums) tended toward debate which often became **aggressive or abusive**. But despite all these downsides, participants felt that the same lack of inhibition served to encourage people to be **open and honest**, and allow them to speak their mind with confidence.

Typically, most participants were at first unwilling to admit that they themselves behaved differently online, although this was eventually teased out in discussion. Those who maintained that their behaviour did not differ when they went online tended to be less digitally literate users, and it may well be that they had not done enough online to have developed an online persona or manner. Even these users, however, tended to notice that others did behave differently online.

Participants expressed that the internet encourages honesty and openness

It was common for participants to note that the internet provided an opportunity for people to be honest in what they think and feel.

'It's your chance to say exactly what you think.'²

Male, Grimsby

They also observed that people tended to be very open about their lives, even on social networking sites where they were not at all anonymous. This was noted particularly by **older users** who themselves **tended to maintain greater privacy**, especially when compared to the youngest users who were used to living an 'open life'.

Some felt that because dealings with others online are somewhat removed, this also allowed people to **act in a more confident way**.

'Because you're not face-to-face you'll be more confident. Face to face you can see the reaction in somebody's eyes.'

Male, Grimsby, Medium

'I think it's like drivers. You're sitting in your car and you're, in the safety, and you don't realise that people are round about you. You're in that 'my wee world' mentality; you'd never have the nerve if you were facing somebody.'

Female, Glasgow, Medium

² Some comments in this section do not include digital literacy information as they have been taken from the combined workshop sections and so transcribers could not identify the level of digital literacy of the speaker.

This confidence could be used for good, where people would be positively brave in standing up to views that are offensive or bigoted, but at the same time it could lead people to victimise others or be offensive.

Greater openness online may lead to arguments and abuse

In a social space where people tend to be more open, flippant, and controversial this can naturally lead to arguments. Participants noted that there is an **overall 'tone' of internet communication**, particularly social networking and forums as opposed to email, which can **unintentionally encourage misunderstanding and argument**. Firstly, people tended to contact each other online for a specific reason, rather than just a 'catch-up' and so there is less reassuring small talk. As well as comments being more transactional, they also tend to be more blunt; or curt; participants noted that this tone could easily be seen as sharp or aggressive. Indeed, some participants felt that **online communication could easily lead to arguments** because comments were more likely to be interpreted wrongly, due either to problems with conveying the right tone, or because comments were poorly expressed or poorly understood.

People can also be **intentionally argumentative** online, and several felt that the medium both encourages and sustains argument:

'If you want to rant about something if you do it in person it's just all gone and there's loads of emotion behind it but if you're on Facebook because you can't really get the emotion out it'll just keep building and building and you get really malicious.'

Male, Grimsby, Medium

Online communication also tends to prolong arguments as people are allowed the time to think up responses, and no-one wants to be seen to be publically defeated in an argument.

'How many times have you had an argument with someone and half an hour later you'll be sat there thinking ... I wish I'd said that, that would have sounded real good. With Facebook you can do that.'

Male, Grimsby, Medium

The **lack of accountability** was also felt to encourage people to express over-the-top and deliberately controversial opinions which they may not even really hold.

'My niece, I've actually threatened to block her from my Facebook because she is vulgar. But the thing is I know for a fact she is the sweetest, gentlest little thing and you know for a fact you will not see her walking down the street swearing her head off. It brings out the worst in people.'

Female, Grimsby, Medium

'It's not really real. It's not you.'

Male, Glasgow, Medium

Offline, people may be more likely to back down, make compromises for the sake of relationships and to smooth social interactions, whereas if someone is anonymously posting online there is no need to do this; nor is there any risk of physical response, so people can say whatever they like to whomever they like, and enjoy the confrontation caused.

'When you see the things people write online, I think it's much easier to be nasty and they forget about the real people on the other end of the website.'

Female, Cardiff

'I am more rude online, definitely. I will put whatever I want on Facebook. I don't care. If people don't want to read it, don't read it. My mum phones me up ... at least once a month and tells me off.'

Female, Grimsby, Medium

5.2 Citizen rights and responsibilities online should be the same as those offline

A consensus seemed to emerge over what can be considered appropriate online behaviour. This included the following:

- **People are morally obliged to consider the possible ramifications** before posting anything online, particularly on publically viewable sites, and if in doubt, caution should be urged.
- There was consensus that illegal material online should be dealt with accordingly with investigations by police and prosecution. There was also consensus that **illegal matters should be monitored by the government**.
- There was, however, a debate over whether **inaccurate comments** should be considered potentially libellous, or **malicious views** considered as illegal hate speech, with some feeling that this would be too restrictive on free speech. This was especially the case for websites which do not market themselves as a news website or claim any other similar authority. Rather, several felt that **websites should regulate themselves** on these and similar matters.

Regarding the ability to complain or to receive fair treatment, many were concerned that the internet felt completely unregulated; a 'wild west'. It was certainly felt that, if there are already official procedures, these needed to be much more well-known.

Participants looked at the following various hypothetical scenarios to gauge where they felt the rights and responsibilities lay online. People's reactions and moral standpoints on these issues were varied and nuanced, depending on the specific scenario tested; hence it is not feasible to make generalised conclusions.

1) Twitter allegations

“TWITTER INFIDELITY ALLEGATIONS RAGE ON”

Via public messages typed on Twitter, a person falsely declares that they have witnessed their friend being unfaithful to his wife. Discuss the rights and responsibilities of the people involved in this case if a) the target is a celebrity and b) the target is a ‘regular person’.

There was a feeling that **people should take personal responsibility for their actions**. Participants tended to feel that if someone is going online to write something, especially to make an accusation, they should take more care to check the facts, before going ‘on record’. Some even felt that Twitter should not be used for such personal matters in the first place; as not only are tweets publicly viewable but they can remain viewable permanently.

‘The problem is that the record is permanent. It’s not just a conversation between you and me, it’s for everyone to see.’

Male, Leamington Spa

Thinking about the consequences of posting such material, some believed that the person posting should be dealt with by the website’s own internal procedures; perhaps requiring the person posting to write a public apology or to have their Twitter account shut down. Others felt that there ought to be stronger deterrents in place, because, once published, ‘the damage has already been done’ and an innocent person has had their reputation tarnished. Some believed that such claims meant that the person posting could be sued for libel (one participant mentioned the case of Lord McAlpine suing Twitter users over child abuse allegations) and some thought that this should happen more.

‘We are all publishers now, and we need to be aware of that.’

Female, Cardiff

It was also felt that recourse to legal action should be available to everyone and not just well-known people who are protecting their reputation, although many stated that, in reality, a celebrity is much more likely to be able and inclined to take action, due to their status and wealth. One man had relevant experience of libellous comments being made about him:

‘On Facebook my ex and her current partner have posted some really sick stuff about me and my family. I took screenshots of the stuff he say so I’d have proof to take to my lawyer in my custody case ... I didn’t retaliate, I just thought ‘If you want to be an idiot’. People who say horrible things online just end up looking like idiots.’

Male, Grimsby

In contrast, some felt that, due to the very nature of social networking, comments made on sites like Twitter are understood to be ‘throwaway’ and that there should not be any legal ramifications for flippant, ill-informed, or even malicious comments of this sort.

The consequences should rather come either from the community itself, where people would be shunned or criticised for making malicious or careless comments, or from official moderators of the website who could remove comments or accounts.

So, while it was felt that there is certainly a need for people to take moral responsibility for their actions online and to be careful about what they say for the sake of others, there was **disagreement as to what should be done if this does not happen**. There was, however, a consensus that people should be better educated about the possible implications of putting accusations online, and perhaps even that users of social networking sites should have to agree to reasonable 'house rules' which are then monitored and enforced.

2) Facebook pictures

"WOMAN DENIED JOB INTERVIEW OVER FACEBOOK PICS"

Friend A puts up photos of their birthday party on Facebook. Some of the photos show one of her friends (Friend B) behaving in a drunk and inappropriate way at the party. Friend B has recently applied for a job. Their prospective employer does a search for her on Facebook and comes across the photos, since her profile is not private. Based on these photos, the employer decides not to interview Friend B.

In this example, participants tended to apportion blame to all parties: Friend A, Friend B and the employer. It was felt that Friend A should have first checked with Friend B if she was happy with the pictures being put up, and then, in turn Friend B should have declined out of prudence. Even if Friend B was happy for the pictures to be put up, it is felt that she should have been more vigilant about her privacy settings.

Others took a different tack, stating that the inappropriate behaviour was the issue in the first place:

'You need to be responsible for your own actions; if you are OK to act like that then you should be OK to take the consequences of anything that comes of these actions.'

Female, Cardiff

Although participants recognised that some employers make such checks, they tended to feel that they should not behave so intrusively in the first place, and nor should they have reacted to photos of someone in a private context. Although some participants left open the possibility that in some cases the inappropriate private activity could 'overflow' into the person's professional life, and the employer would need to know this.

Many social network users were familiar with the problem of having unflattering or inappropriate photos put up and several had reported photos of themselves, which had been taken down shortly afterwards. Often participants tended to believe that any pictures of themselves belonged to them, that they had total rights over them, and they could always ask Facebook to take them down.

For less digitally literate users this presented more of a concern, as they were often unfamiliar with how to get a photo taken down, and many were conscious that merely un-tagging themselves still leaves the photo there to be seen by others. One woman gave the example of her daughter putting up a picture up of her and how she was still

unhappy about it. Those who were not aware of privacy settings assume that Facebook profiles are public anyway, and so caution should always be used when deciding what to put online.

Finally, some felt that no-one should want to work for an employer who routinely invades their employees' privacy, as a matter of course.

'You shouldn't care what other people think, the only people who are reading this stuff are idiots so you shouldn't care if they see anything of you up on any site or not.'

Female, St Albans

3) Medical details leaked

"MEDICAL DETAILS LEAKED AFTER GP SELLS PATIENT INFORMATION"

A GP surgery decides to sell some of the personal health data it holds on their patients to a commercial pharmaceutical company. The pharmaceutical company use this data in their research to develop new drugs to treat cancer and heart disease. The surgery gets some financial reward, which it uses for the benefit of surgery users. There is then a breach of data security and the medical data is made available to all online.

A key piece of information which most participants needed to assess fully with this scenario was whether the health data was *anonymised* or not. This was because non-anonymised medical data could be stigmatising or embarrassing, although many felt that, **if anonymised, it became 'just information'**.

If the data was assumed to be anonymised, typically participants did not have a moral objection to it being shared as it was being done for the greater good of curing disease and to improve services which they, and people in their community, use. The fact that such information could be leaked was, however, felt to be disgraceful; it was taken to reveal negligence. If, however, it was assumed that the data was not anonymised, then participants felt outraged not just by the leak but also by such information having been sold on to a private company by a surgery without consent.

On the issue of consent, even for anonymised medical details, many felt that the GP surgery should have asked the patients, or ensured that they signed a form which explained how their data might be used, and allowed them to opt out. Participants felt that there was an implicit presumption that the surgery has been entrusted to keep this sensitive information safe, so any possible risk to this security ought to be checked with the patient. To fail to do this undermines the trusting relationship between the doctor and patient. So, although participants generally were actually **happy for their anonymised data to be used for what they considered to be good purposes**, they were still **concerned about the loss of control of their data**, and **would like to have given clear consent** for each possible use, or at least have been informed about it.

Other participants were more torn, feeling that medical data which can benefit the surgery itself and even lead to medical breakthroughs, should not have such restrictions on use (although again it should still be anonymised). These participants

tended to feel that asking for permission would be a 'nice to have' courtesy, but not required.

Finally, there were a few, especially those belonging to the Conspiracy Theorist segment, who were not at all happy for their anonymised information to be passed on in this way, and especially not in a commercial transaction with a pharmaceutical business, which they saw as typically unethical, and liable only to use their data ultimately to make profit.

'Essentially the health organisation that sold on my details has stolen from me. That is my data and my information and they have taken it against my free will. I would give it to a company if they had asked but this is in breach of the confidentiality laws.'

Male, Glasgow

4) Government censorship of websites

“UK GOVERNMENT INTRODUCES NEW LAW RESTRICTING ACCESS TO CERTAIN WEB PAGES”

Following the introduction of new laws to monitor the content of web pages, websites that contain content that is considered to be illegal, harmful or offensive have either had their content modified/deleted or access to the website has been blocked.

Participants were **content with the government monitoring websites for illegal and harmful activities and assumed that this was already happening**. Several had come across upsetting material online, which had affected them personally; these were mainly younger respondents whose friends or wider acquaintances had posted violent or pornographic images or footage, seemingly to 'get a reaction', or in the hope that people would join in with their moral outrage. One participant, however, noted that he did not wish to see such material in the first place.

'Seeing horrible things in the flesh scars you. It's so extreme and you can't get the images out of your head.'

Male, Grimsby

However, with regard to offensive content, participants were less sure that this should be the government's concern. This was either because they thought 'offensive' was deemed to be a subjective concept, or because being merely offensive wasn't a sufficient reason to censor something on the internet, which was felt by many to be a bastion of free speech.

'The thing is I'm entitled to my opinion. That's the beauty of the internet.'

Female, Grimsby

Some felt that government monitoring of all websites was 'a bit big brother', and that the government might use this power to try to hide critical content or leaked information. The Conspiracy Theorists believed that this was already happening and also that the government was monitoring most (if not all) of what goes on online and in phone calls, so that certain words (e.g. 'Jihad') flag up a conversation to be analysed.

Overall however, there was **approval of the idea of the government extending its role in protecting the public** from harm, both offline and online, with the provision that it is **guided by what is illegal rather than what might merely be considered offensive**. Middle-aged and older participants were particularly concerned that children be protected from harm online.

5) Community moderator scheme

"ONLINE COMMUNITY MODERATOR SCHEME LAUNCHED"

A charity is launching an appeal to encourage more people to volunteer as moderators on popular websites, forums and blogs, as they want to encourage positive online behaviour. Their role would be to monitor anti-social comments and report abuse, as well as encourage and reward good behaviour. A number of websites have signed up to the scheme, including both government and privately-run companies.

Participants were aware that communication online, particularly between strangers, can often become overly aggressive or abusive, and young people in particular tended to have experienced this directly. Although it was felt that individuals should be capable of being respectful of others without having to be 'told off' by officials, given the realities, **measures to curb poor behaviour were broadly approved of**.

'I guess this might have come about to try and prevent negative communications online. Internet bullying is on the up, so they might want to stop that.'

Male, Grimsby

Some spoke of abuse online as an ever-present phenomenon.

'My friend posted graphic footage of violence in Yemen; to try and open people's eyes up to atrocities going on out there. But it opened him up for a lot of racist abuse ... On YouTube videos you see one extremely malicious comment for every video on there.'

Male, Grimsby

Participants did, however, make **distinctions to define the kind of comments that should be blocked**. Victimising or bullying comments directed at innocent people should be addressed severely.

'But some people should be silenced. It's the way you say things. There are some things I see online that are so malicious; it's horrible ... There are 'keyboard warriors' that think that they are hard, posting horrible comments and hiding behind their keyboard ... They do it for attention, they get a kick out of the reaction. It's like a bully in a playground.'

Male, Grimsby

But aggressive disagreements and insults due to difference of opinion were felt to be less serious. Respondents thought that the idea of **rewarding positive behaviour** was problematic, as it would be difficult to get a consensus about what constitutes 'positive behaviour' online. Some suggested 'constructive feedback, which is balanced, fair, impartial, and helpful to others, while still honest'. Others felt that this was too unrealistic and would be constraining, and that merely avoiding abuse and personal attacks should be seen as positive behaviour.

In terms of **penalties for negative behaviour**, participants felt that if abusive messages were posted on a website, that website itself, rather than the government or other users, should monitor this and should step in, possibly blocking the person's account for a period of time; for example, one week for the first offence, two weeks for the second, and then to be eventually banned completely. It was also noted that merely banning someone's account is not effective, as another one can easily be created, and so banning someone's IP address was advocated.

It is notable that participants were generally not sure what procedures were currently in place to enable offensive comments to be reported, or whose responsibility it was to report them. Generally, they thought that matters to do with moderation should be down to the owners of the website, although they also understood that a voluntary force, as in the scenario, could support this function.

There were concerns about the impartiality of moderators, and some mentioned that they would have to follow clear, well-publicised guidelines, and that people should even be able to 'appeal' a moderation decision. Others were anti-moderation, and felt that if people were posting abuse online, then it was for the community as a whole to show their disapproval to them, both online and offline, rather than have an individual and authoritative moderator.

6) Account suspended

"MAN HAS INTERNET ACCOUNT SUSPENDED OVER INACCURATE CONTENT ROW"

A student from Cheshire has his internet account suspended by his internet service provider over an ongoing row with Wikipedia and a top tourist attraction in the area over his modifications of their Wikipedia page. The man is accused of repeatedly modifying the page to show inaccurate opening times over the course of several weeks, leading to loss of business.

Generally, participants felt that although Wikipedia is an open source site, there to be edited, it was still **morally wrong to deliberately mislead people and there should**

be consequences for doing so. What the consequences should be, however, was a matter for debate. Generally it was felt that only Wikipedia should address the problem, and that for the internet service provider to get involved was a step too far. Conversely, a few agreed that his internet access should be suspended altogether until he stopped 'misbehaving'.

One participant actually knew someone who had faced a similar situation and who had found that such issues could be difficult to resolve.

'I had a friend who was in a band. He knew someone in a rival band who kept changing his band's Wiki page, writing really malicious stuff about him being arrested for stuff. He tried to stop him but it took ages to resolve. I'm not sure if wiki shut him down or he just decided to stop.'

Male, Grimsby

Broadly, however, participants' reaction to this scenario tended to vary according to the status they gave to Wikipedia. Those who felt that it had attained the status of an official, authoritative and legitimate source of information were more inclined to feel that tampering with entries should receive punishment, just as graffiti-ing a street sign would do. Others were more sceptical about the reliability of Wikipedia, specifically because it can be edited by anyone, so they did not think it could be trusted; consequently, they felt that the student, although probably acting in an immature way, should not receive any punishment.

'This is stupid, who would believe Wiki? It's edited by people no one thinks it's the truth. It would be different if he sabotaged an official website; that would be hacking and he should be punished.'

Male, Cardiff

Participants also tended to feel that Wikipedia was sufficiently well-referenced, so that people could verify information if they needed to.

6. Future trends

6. Future trends

Key findings

Participants foresaw a **future increasingly dominated by the internet**. They expressed a sense of **inevitability** about this, as an increasing number of daily activities were being moved online. This move was not generally perceived to be problematic, as long as the changes were of some **personal benefit** to people. Participants imagined that the functions of the internet would become more **x tailored to the individual**, and this could have a positive outcome for them: they were drawn to imagining a world in which they received **personalised services** from companies, which in turn would be rewarded with **consumer loyalty**, and personal information which individuals could sell to the highest bidder.

A further positive prediction was one of **greater harmony between humans and technology**. Participants imagined the devices we use becoming more **integrated** with our lives, and even with our bodies, and expected that such a **symbiotic** state would become a reality in the relatively near future. Even participants with the lowest digital literacy recognised that they would need to **move with the flow** of technology, or risk being left behind or alienated.

Finally, participants envisaged a future in which the trend towards having an online presence becomes irresistible, and in which **almost all of our personal information is stored online**. Without controls, this world would descend into chaos, so total security of information was seen as the next stage, in which cybercrime would be totally eliminated. However, not all were optimistic about such a prospect.

Participants were asked to provide spontaneous suggestions on what the future of the internet might hold, and were encouraged to think 'outside the box'. They predicted greater **human-technology integration**, perhaps through brain implants or voice recognition. They felt that the form of computers would change, perhaps becoming holograms, and that there would be total access to all information, for free, which everyone would constantly interact with, without ever disconnecting. The **always-on**, almost touchable nature of the internet was predicted to become an even greater reality. Conversely, some predicted that the internet would be affected by **increasing regulation and censorship** to 'bring it into line', and because online crime would be so much more prevalent, more rules and regulations would have to be put in place.

6.1 Participants could imagine the benefits of a more symbiotic relationship between humans and technology

Participants were asked about '**machine-to-machine communication**', such as their fridge being able to communicate with the supermarket to order food which is running low. Participants were largely accepting of such developments, and felt that they would

happen in the near future. While some felt privacy concerns, the idea was in general seen as no more an invasion of privacy than loyalty cards or online shopping, both which have already been taken up.

'Tesco already knows what you want when you shop online.'

Female, Glasgow

Participants were also asked about smart meters, already provided by British Gas, which record detailed information about what appliances are being used and when. Again, they were willing to **trade in this information if they felt that it would provide them with a better, or more personalised, service**, although they remained resistant to their details being sold on to a third party.

'I would only want my provider to have my details.'

Female, Glasgow

6.2 People predicted that personal information would be increasingly commoditised, but also that they would have greater control over their data

Given the previous focus on security and data, discussions about the future of the internet often drew upon these themes. Participants envisaged a combination of increased security and increased openness online in the future. They thought that **'increased security will ensure that no-one can access your details or impersonate you'**, removing the threat of identity theft. Participants predicted that fingerprint or iris identification would become standard, and viruses would be permanently defeated. They also saw themselves having **closer relationships with companies**, in which the consumer allows companies to understand more about them and they in return receive not just free products and services, but also more **personalised marketing and services**: a perceived win/win scenario. Thus the relationship is 'closer' in terms of information, but still remains impersonal. In this way, personal information becomes increasingly commoditised; with people increasingly seeing it explicitly as a resource that they are able to sell or exchange, but at no real loss to themselves.

'What do I care if they know what milk I buy and when? ... In the grand scheme of things who cares whether somebody buys Heinz or Branston, except Heinz or Branston?'

Female, Glasgow, Medium

They predicted that in the future, people will have more control over who has their personal data, unlike now, where some feel that data is often being freely shared between companies without their permission. The **company's responsibilities regarding data would therefore have to be explained in much more user-friendly terms**, possibly standardised, so that everyone knows how to read them and what they mean. Companies would receive punishment for 'burying' important information in long, old-fashioned 'terms and conditions' documents.

Participants envisaged that with increased sharing they will become increasingly affiliated, or attached, to certain companies, just as we are now to utilities providers. We will have 'our' supermarket, or 'our' bookstore, 'our' online marketplace. Participants also imagined enhanced e-commerce procedures, including greater automation of routine purchases, such as fridges being able to order food supplies. Similar trends of increased automation and increased personalisation were envisaged regarding interactions with government services, thereby reducing interaction to a minimum.

Some participants, especially those who were mistrustful of corporations, thought that the trend towards exposing hitherto private information should be resisted,. Some were concerned that an **increasing reliance on online technologies would expose us to a systemic failure or attack**. Likewise, if we 'design out' people and employee discretion from systems, people may find themselves unable to interact at a human level. This was felt most acutely with regard to government services which, although they are increasingly automated, do sometimes still allow for sympathetic, or 'human', exceptions to the rules to be made, exceptions which an automated system would be incapable of making.

All, however, predicted that the internet would play an **increasingly ubiquitous role** in our lives and that we will all be swept along by these trends. As opting out will involve ever-increasing effort, inconvenience, and ultimately disadvantage, we had all better try to keep up, and enjoy the advantages that increased integration brings.

'I don't [feel in control of my privacy online], but this is the way the world is going. This is a life thing; as you go through life, you start to realise whether you think you have control, you realise you don't, you may get a family, have children: you lose control of your life. But you just don't worry. You just learn as you go on, and you hope you don't get your fingers burned.'

Male, Cardiff, Medium

Appendix

7. Appendix

Discussion group details

Workshop	Location	Date	Digital literacy level
Pilot	Ipsos offices, London	Tuesday 22nd January	Low digital literacy
			Medium digital literacy
A	St Albans	Monday 28th January	Low digital literacy
			Medium digital literacy
B	Leamington Spa	Tuesday 29th January	Low digital literacy
			Medium digital literacy
C	Grimsby	Wednesday 30th January	Medium digital literacy
			High digital literacy
D	Glasgow	Monday 4th February	High digital literacy
			Medium digital literacy
E	Cardiff	Monday 4th February	High digital literacy
			Medium digital literacy