COMMUNICATIONS
CONSUMER
PANEL

Digital Footprints: a question of trust

November 2016

Contents

1. Foreword

These days, data is big business. But perhaps few of us realise fully the extent to which our personal information is collected, stored and used. Fewer still may feel that we have control over our personal data – and many of us are uneasy about the situation.

More and more of our personal data is being collected – both as people knowingly disclose information on platforms such as social media and as they unknowingly share details about themselves whilst going about their everyday business online. This gives rise to two fundamental questions:

1. What are the implications for our individual privacy?

2. How can we control and manage the use of our personal data more effectively?

The vast range of opportunities created by the internet, mobile apps and micropayments offers consumers and citizens a host of potential benefits; but this means that it is ever more important that people understand the implications of the consent they are giving organisations for the use of their data, and the precautions they can take to safeguard their personal information.

The Internet of Things (IoT) offers many exciting possibilities for UK consumers and citizens, but brings with it greater concerns about privacy, data protection, the control of data and security. This is particularly relevant to the growth of big data – especially that of machine to machine data. What sets this apart from our current situation is the new development of aggregated data and inferred data. So while there are great opportunities for innovation, there are risks too. We commissioned new research to build on our earlier report, Online Personal Data – the Consumer Perspective. Much has changed since 2011, but people's concerns about the security and privacy of their online data have increased, not decreased.

This report is intended to inform policymakers and the wider public about consumer perceptions of online security. But not least, we urge companies to take heed of the evidence and better take account of consumers' interests – for example, through clarity and consistency about consent for use of personal data, through clearer privacy policies and through giving consumers more control.

Consumers are to an extent aware of their own responsibilities - but too often they are not helped by the companies who seek their data and who must do more to earn public trust. This includes companies being transparent and educating consumers about what happens to their personal information.

In this report we make a series of recommendations which we believe are fundamental if consumers are to benefit from this fast-moving area of technological development, rather than suffer detriment as a result of it. We will engage with governments, regulators, industry and consumer stakeholders to follow up these recommendations.

2. Recommendations

Based on our research, we believe that there is a clear set of recommendations that needs to be implemented by Governments, regulators, enforcement agencies and companies to ensure that consumers thrive in this new data-rich environment and are not subject to detriment:

Companies:

- Proactively provide clear and consistent information about the consumer implications of people consenting to supply their personal data;
- All consent decisions to be “opt in” as the default position;
- To facilitate greater consumer control in terms of use of data – through clear information, options and choices;
- To always keep to a minimum the amount of data that they collect and store;
- To store data securely; use it only for the purpose intended; retain it for no longer than is necessary; and check with consumers periodically whether permission is still given to retain the data;
- To follow all relevant legislation and regulation[1];
- Privacy policies and terms and conditions should be informed by the ICO’s ‘privacy policy checklist’; contain an easily accessible ‘key facts section’ and be short, clearly written and avoid jargon;
- Must be transparent about what information they collect about their consumers and how they will use this information – including whether they will pass it to any third party;
- Should clearly highlight on their websites how consumers can request that their personal information be amended or deleted from the company’s records;
- Explore how best to serve and support low-confidence consumers in vulnerable situations in respect of privacy and security: tangible steps might be ensuring essential information is provided about available resources; with ISPs providing for free a basic level of internet security (antivirus/spyware) by default for all customers and taking a role in highlighting on-line scams to consumers;
- Staff should be trained and/or have access to information so that they can accurately help consumers with enquires about use of personal data.

Governments, regulators and enforcement agencies:

- Act decisively in cases of non-compliance; and
- Consider producing a Code of Practice and/or good practice guidance.

[1] Including compliance with the UK implementation of the General Data Protection Regulation

3. Executive Summary Digital Footprints 2016

What do we know about how our personal data is collected, stored, used and protected? Do we feel in control of our personal data? How much of a concern are these issues to consumers?

The Panel's 2011 research into consumer attitudes towards online privacy explored these issues and revealed a number of concerns. Given the pace of change since then and the importance of this issue, the Panel commissioned Ipsos MORI to conduct new quantitative and qualitative research to update our understanding in this area.

By 2016, almost nine in ten (86%) of UK adults have internet access at home[2]. The average internet user estimates they spend 25 hours online each week and total UK expenditure on internet advertising grew by 17.3% from 2011 to £8.6bn in 2015. Internet advertising continues to be the largest type of ad spend in the UK, and accounted for 41.1% of the total estimated UK advertising spend in 2015[3]. This is a highly lucrative – and rapidly expanding – market. Ofcom's 2016 Media Use and Attitudes[4] study reported that more than four in five adult internet users (82%) say they have ever bought things online.

Our 2016 research found that most people understand that personal information is collected, stored, and used by public and private sector organisations. However fewer are aware of how such technologies work or how their personal data is used. We found that privacy and security are major concerns for consumers – financial transactions are particularly sensitive areas. From our sample[5], people with a higher degree of internet confidence (eight out of ten) tend to be more aware of when their personal data is being used and why companies may want this information. They also have a clearer sense of what steps they need to take to protect themselves. This group tends to be younger and use the internet more frequently to perform multiple tasks.

Less confident users still recognise that companies use their personal information. However they are less aware as to when it is collected and they have fewer skills to protect themselves while online - often either relying on friends or family to help them or limiting their internet use altogether. This group tends to be older, less frequent internet users who tend to have a slightly higher degree of anxiety about online privacy. Many however are satisfied within the limits of their internet use and do not feel the effort of learning more is worth the time.

[2] Ofcom: The Communications Market 2016
http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr16/uk/UK_Internet.pdf

[3] ibid

[4] http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/adults-literacy-2016/2016-Adults-media-use-and-attitudes.pdf

[5] A representative survey of 1,423 adults aged 15 and over across the United Kingdom was conducted face-to-face on Ipsos MORI's Capibus survey between 19 February 2016 and 23 March 2016. In addition to the quantitative survey, 21 qualitative in-depth interviews were conducted.

Within our sample we found that the majority of internet users are concerned about how their personal information is used online. Most would prefer companies not to use their personal information if given the choice; but many feel that they can live with companies using their data if done responsibly and while being transparent about how the data is being used – even if this is for marketing purposes.

Nearly all consumers feel a sense of suspicion if companies sell their personal information to other companies. The research finds that 'trust' is a cornerstone in respect of how we use the internet, with consumers also using pre-existing views and opinions as a proxy to decide whether to trust a website or not. We found that this trust depends on companies adhering to three things:

- Being fully open about what data they collect/use and what they will do with it;
- Giving consumers the opportunity to opt-out of any use of their data;
- And, keeping consumers' information safe and secure.

Key Findings

Confidence and Trust

- Privacy and security of personal information are major concerns for high confidence and low confidence internet users alike - financial transactions are a particularly sensitive area;
- Consumers are more concerned about privacy than they were five years ago; but are taking less action to protect themselves;
- Whilst there are high levels of confidence when using the internet, a significant minority of people are not confident;
- There is a digital divide between high/low confidence: one in five people lack confidence online; and one in three are not confident about protecting themselves by adjusting privacy settings;
- Young people are generally more confident internet users - approximately half of people aged 65-74 are not confident online and this rises to seven in ten in the 75+ age group;
- Younger people are generally less concerned about privacy than older people;
- The digital confidence divide is not just age-related - there are also lower levels of confidence among disabled people, compared to non-disabled people;
- Trust is a key consumer issue - three tenets are essential in building trust: transparency, personal control and security;
- Many people confine their purchasing to brands they already trust in the offline world;
- People have higher levels of concern about using public Wi-Fi – they have less confidence and are more concerned about hacking and identity theft;
- There are lower levels of confidence when it comes to using security settings on mobiles/tablets.

Awareness and Control

- Consumers do not feel completely in control of their personal information - they want more control and to decide for themselves what is shared or not;
- Lack of control leads to a sense of disempowerment;
- 14% of people are not using security software, or are unaware of it;
- Security measures and the choice to opt out of receiving marketing information are not generally well known;
- People have a greater sense of security when using home broadband.

Data Use and Sharing

- There is a perceived lack of transparency about data use - people may understand that data is collected but not how it is used, how long it is kept for and why;
- Terms and Conditions and privacy policies are not widely read or fully understood and need to be clearer;
- People want more information about how their personal information will be used; third party sharing is an area of particular concern;
- There is confusion and inconsistency, and conflicting emotions, regarding sharing data online; on balance, consumers feel that collection of personal data is most beneficial to the companies collecting it;
- Consumers do not fully recognise the link between providing personal information and the benefits of doing so;
- There are concerns about privacy and control of personal data in regard to Smart products.

Recommendations

Based on our research, we believe that there is a clear set of recommendations that needs to be implemented by Governments, regulators, enforcement agencies and companies to ensure that consumers thrive in this new data-rich environment and are not subject to detriment:

Companies:

- Proactively provide clear and consistent information about the consumer implications of people consenting to supply their personal data;
- All consent decisions to be "opt in" as the default position;
- To facilitate greater consumer control in terms of use of data – through clear information, options and choices;
- To always keep to a minimum the amount of data that they collect and store;

- To store data securely; use it only for the purpose intended; retain it for no longer than is necessary; and check with consumers periodically whether permission is still given to retain the data;
- To follow all relevant legislation and regulation[6];
- Privacy policies and terms and conditions should be informed by the ICO's 'privacy policy checklist'; contain an easily accessible 'key facts section' and be short, clearly written and avoid jargon;
- Must be transparent about what information they collect about their consumers and how they will use this information – including whether they will pass it to any third party;
- Should clearly highlight on their websites how consumers can request that their personal information be deleted from the company's records;
- Explore how best to serve and support low-confidence consumers in vulnerable situations in respect of privacy and security: tangible steps might be ensuring essential information is provided about available resources; with ISPs providing for free a basic level of internet security (antivirus/spyware) by default for all customers and taking a role in highlighting on-line scams to consumers;
- Staff should be trained and/or have access to information so that they can accurately help consumers with enquires about use of personal data.

Governments, regulators and enforcement agencies:

- Act decisively in cases of non-compliance; and
- Consider producing a Code of Practice and/or good practice guidance.

[6] Including compliance with the UK implementation of the General Data Protection Regulation

4. Literature Review

In this review we discuss some of the existing research surrounding online data protection and privacy. Key themes from the relevant literature include the disparity between technological literacy and awareness of how personal data is used, contradictory behaviour in terms of how people safeguard their personal data; and a brief contextual overview of the changing market environment surrounding internet use.

Awareness and use of personal data

Most people understand that personal information is collected, stored, and used by public and private sector organisations. However a lower proportion are aware of how such technologies work or how their personal data is used. Catapult Digital found that 80% believe that it is being used for the company's own economic gain. This also holds true for the public sector where 45% think it is using people's personal data in a beneficial way for the organisation. Regardless of the extent to which regulations covering personal data and privacy are clear cut from a legal perspective, this same clarity does not exist within the minds of consumers (WIK-Consult 2015). On the whole, consumers are largely unaware of how organisations are using personal data and for the most part do not understand privacy policies (Catapult Digital 2015) (Office of Fair Trading 2013).

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

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

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

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

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

Contradictory behaviour

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

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

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

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

5. Main Themes

Confidence and concern

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

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

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

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

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

Issues of Trust

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

Three factors are key to building trust:

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

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

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

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

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

Consumer control over personal information

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

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

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

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

The benefit exchange and behaviours

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

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

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

6. Contrast between 2011 and 2016 research

In 2011, three-quarters of the UK population had broadband at home, using the internet to share their thoughts, ideas and information. The Panel recognised that for consumers, providing personal data could have significant benefits in the form of services and applications that are more tailored to their needs, or that they might otherwise have to pay for. But the Panel was also concerned about the risks – that consumers disclosed personal information without understanding how it is used or by whom, that data are misused, and that the law did not keep pace with industry developments or consumers' expectations. Against that backdrop, the Panel decided to carry out quantitative and qualitative research with consumers and a summary of our 2011 research report can found here.

There are methodological differences between the two surveys (telephone compared with face-to-face); and relatively recent headline news about data breaches and hacking could have raised awareness and heightened concerns since 2011. But although the two surveys are not directly comparable, there are some interesting points of contrast between our 2011 and 2016 reports.

Concerns about using the internet, and specifically in relation to privacy and safety of personal details/ID theft appear to have become much more central to people's thinking. In 2011, 52% of respondents said that they had no top-of-mind concerns when using the internet; by 2016 this dropped significantly to only 15% having no such concerns.

We asked respondents what their top-of-mind concerns were. In 2011, 14% said privacy. By 2016, this had risen to 42%. Similarly, in 2011 26% said that they were most concerned about the safety of their personal details/ID theft. By 2016, this had risen to 38%.

However when looking at people's awareness and action related to addressing their concerns, we see an obverse trend. In 2011, 83% of people were aware of being able to opt out of marketing and information; however, by 2016 this had dropped to 66%. In an apparently related development, 85% of respondents said that they had opted out of receiving marketing or information in 2011. By 2016, this had dropped to 74%. In terms of awareness of the Terms and Conditions that they were agreeing to when purchasing online, 64% of respondents in 2011 said that they read such statements. By 2016, this had dropped to 50%.

7. Conclusions

Over time, consumers have become more concerned about privacy and personal information but less engaged in terms of protecting themselves and taking control of their data.

This is not a happy situation, placing as it does the consumer at risk of harm and with most control residing with the companies who seek, hold and use the data – inter alia through unclear opt in or out alternatives, unhelpful privacy policies and confusing and unwieldy Terms and Conditions that often give consumers little choice.

Given the size of the online market in all its shapes and forms, now is the time for change.

Ofcom's 2016 Media Use and Attitudes[7] study reported that more than four in five adult internet users (82%) say they have ever bought things online. Thirty per cent of these say they buy things online at least weekly. Around half the number who say they have ever bought things online have sold things online (41%) with less than one in ten saying they do this 'at least weekly' (8%). Two in three internet users (67%) say they have ever gone online to bank or pay bills, with 40% saying they do this at least weekly.

These figures will only grow, so based on the evidence from our research we urge all stakeholders to collaborate in a way that enables markets to innovate in the interests of consumers, whilst making it easier for those same consumers to have confidence and trust in companies not to misuse their personal data.

As the market for personal data becomes ever more complex and monetised, it is increasingly important that people understand the implications of the consent they are giving organisations for the use of their data and, with regard to security, the precautions they can take. The IoT will potentially involve a vast increase in the collection and transmission of data – and particularly sensitive personal data. The protection of this data is paramount. However, there is an opportunity to learn from the experiences of the use of data online and how it has been utilised along the value chain by some commercial organisations, sometimes to detrimental effect for the consumer - e.g. as a partial cause of nuisance calls.

Consumers can only make truly informed decisions about the provision of their information and take responsibility if they know how their data is being collected and processed and have the tools to manage its use. This should not mean making privacy policies longer and more complicated – in fact there is a good case for simplifying such information. Consumers should also be able to easily reverse decisions that they have made to share personal data. Companies need to ensure that they have a compliance culture (which could involve a Code of Conduct for example) - to supplement any existing regulatory framework - and adhere to it. Companies need to use their expertise in content presentation to provide privacy information and tools in user-friendly ways. We are

[7] http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/adults-literacy-2016/2016-Adults-media-use-and-attitudes.pdf

therefore calling for consumer-centric policies - clear and layered privacy notices and flexible regulations that allow innovation but hold companies responsible if they misuse data.

Communications Consumer
Panel and ACOD
Riverside House
2a Southwark Bridge Rd London
SE1 9HA

contact@communicationsconsumerpanel.org.uk

Published by the Communications Consumer Panel

This publication is available in electronic form on the Panel's website in English and Welsh. We can also provide alternative formats on request.

www.communicationsconsumerpanel.org.uk