CORSHAM INSTITUTE

Trust and ethics

Building a more informed digital society

A consultation in partnership with the Corsham Institute Thought Leadership Programme 2016

Report June 2016

WINDSOR CASTLE
HONI SOIT QUI MAL Y PENSE
COLLEGE OF ST GEORGE

This report was produced following a consultation at St George's House, as part of a programme of events in the Corsham Institute 2016 Thought Leadership Programme.

The report should be viewed in conjunction with reports from the series.

The consultations in the 2016 programme were:

- Digital health: Digital's role in health and care – March 2016
- Cyber and resilience: Digital's role in regaining resilience – April 2016
- Digital living: Getting the most out of digital society – May 2016
- Trust and ethics: Building a more informed digital society – June 2016

This programme hosted at St George's House was developed in partnership by Corsham Institute, RAND Europe and the Smart Societies Institute.

St George's House is a place where people of influence and responsibility in every area of society can come together to explore and communicate their views and analysis of contemporary issues. The aim is to effect change for the better in society by nurturing wisdom through dialogue.

Corsham Institute (Ci) was formed in 2013 to explore the opportunities and benefits of the digital society, both social and economic, with particular focus on shaping a future where individuals can realise their potential in a highly connected world.

RAND Europe is a not-for-profit research institute whose mission is to help improve policy and decisionmaking through research and analysis. Lying on the spectrum between that of universities and consultancies, RAND Europe's work combines academic rigour with a professional, impact-oriented approach.

The Smart Societies Institute is an independent, non-profit think tank aimed at improving society through the use of science and technology. The Institute envisions a future where science and technology augments and enhances our day-to-day lives to improve the quality of life for everyone in our society.

The report should be cited as: Corsham Institute (2016). Trust and ethics: Building a more informed digital society. Windsor: St George's House.

Published October 2016.

Key findings

Context

The majority of citizens are now purchasing goods and services online, while also providing information about themselves in order to access online services. Data is now becoming a significant economic resource for many organisations. However, it appears that the public remains unclear about the data they are giving away every time they make a transaction (financial or social) and how this data is subsequently used. In all online transactions, an acceptance of terms and conditions, which describe how your data will be used, is required, but most users typically accept such terms and conditions without fully understanding what they are actually consenting to. In spite of these problems, there are many advantages to sharing personal data. Benefits range from allowing purchase preferences and product recommendations to be efficiently remembered when dealing regularly with a retail website, through to more strategic benefits such as using data to deliver better health outcomes and support policy development. This subject of trust and ethics in online transactions formed the basis of the discussion during the fourth session of the 2016 Thought Leadership programme.

Key discussion points

Is the public aware that it's giving away personal data?

The term 'privacy paradox' emerged from the discussion. It refers to the public's habit of sharing more personal data, while simultaneously expressing concerns about the consequences of doing so. Most people instinctively want to keep their data as private and protected as possible, but when presented with opportunities to share data, many do so without thinking through the implications and potential risks. Overall, the lack of transparency and understanding about how personal data is collected and used emerged as a key theme. This has profound implications, as the public's trust in the digital world could be significantly eroded as a result.

How is consent granted?

Consent to use personal data is an ambiguous issue. Organisations are increasingly reliant on using assumed consent during online transactions, which allows them to use personal data for commercial purposes. Again, the lack of transparency emerges as a key theme, with the public not being aware that this is happening when they provide assumed consent during transactions.

Are there any other considerations?

The group reflected on how the increasing use of digital technologies is changing ways of interaction and transaction within society. New behaviours are emerging through the increased use of digital technologies, and these are having an impact on the wider society. There needs to be consideration of what actions are acceptable or unacceptable in today's modern digital age – a new digital norm. The different perspectives across different generations also require further consideration. The situation appears to be more nuanced than a simple division between a younger generation that does not mind its data being shared and an older generation that does. Therefore, this area requires further research.

Next steps

It is important to create a more enlightened and ethical digital society. To deliver this, there needs to be a public-led framework, written in accessible language, which helps the public understand the rights and responsibilities of different parties, such as individuals, corporations and governments, when using personal data. At the same time, social media, online retailers and other organisations need to be held to account to ensure that they are not misusing personal data and that there are clear and transparent terms and conditions. In addition, acceptable online behaviours need to be defined, so the public is aware of what acceptable online behaviour is and how they can be a good digital citizen. All of the above points could be addressed through a social contract to which all people, organisations and governments pledge, to ensure a common ethical purpose across all society.

Introduction

The Corsham Institute (Ci) Thought Leadership programme, which was designed and delivered in conjunction with RAND Europe, was established to explore the opportunities and challenges that digital technologies are creating within society. The programme seeks to bring together senior leaders from across academia, industry, government and non-government sectors in order to enable the emergence – through a combination of robust debate, knowledge sharing and personal reflection – of new thinking and ideas on how everyone in society can benefit from the use advantages that digital technologies can offer.

This report represents the main findings from the consultative event that was held on 14 and 15 June 2016 at St George's House. The topic was trust and ethics, and how we can build a more informed digital society.

The overarching question which this consultation sought to consider was:

'How do we better equip society to understand the benefits and consequences of transacting in a digital world?'

Recognising that the digital world has already demonstrated clear economic and social benefits, and that more aspects of our day-to-day lives are moving towards digitally enabled modes of delivery, the participants to the consultation felt that there is a need to explore how confident citizens feel when they participate and, in the broadest sense, transact digitally. Greater confidence will require citizens to have a better understanding of what personal data is being provided to third parties and how this is collected, stored, used and shared with others as part of an individual's digital footprint. As digital transactions become a more important feature of every aspect of our daily lives, we need to consider how informed and prepared our society is to handle this new mode of interaction.

We have approached this consultation with an understanding that 'transacting digitally' needs to be considered in the broadest sense and needs to cover a wide range of different digital interactions. Some of these transactions may not involve a financial payment being made but are nonetheless defined legally as a transaction by virtue of the legal agreement that governs the interaction between the individual user and the provider of a digital service or product. For instance, sharing information directly with other individuals through social media services, accessing public services (e.g. health, Local Authority or democratic services), as well as more conventional commercial transactions, can all be defined as 'transacting' for the purposes of our discussions.

As with all Ci Thought Leadership reports, we have aimed to capture the main ideas and views put forward during our discussions, with the understanding that not everybody involved in the consultation will necessarily have endorsed all of the proposals and viewpoints reported.

This report has been structured to reflect the main findings and conclusions, under the following headings:

1. Background and context: Transacting in a digital world
2. Benefits and risks of a digital footprint
3. Strategic Issues
4. Towards a new ethical framework
5. Conclusions and next steps

As with all St George's House consultations, this report has been prepared under the 'Chatham House Rule'. Any phrases that are italicised and in double quotation marks are direct, but unattributed, quotes from the discussions during the event.

Ci and RAND Europe would both like to extend their warm thanks to the participants who introduced each of our sessions, and to all participants for stimulating and contributing to the high level of discussion that took place. A list of all participants is provided at the end of this report.

1. Background and context: Transacting in a digital world

The concept of a digital footprint

As a society, we spend a great deal of the time interacting digitally with family, friends, commercial and public sector organisations, as well as service providers. All of these interactions can be considered to involve transactions of some sort, although they may not involve commercial or financial payments. We all recognise that there are significant social and economic benefits to be realised from the ability to transact digitally in this manner; however, many citizens are unaware that every time they do 'transact', they leave behind a digital footprint – a lasting record of the data that has been transferred in the process of undertaking each and every digital transaction that we make.

During this consultation, we heard how part of a person's digital footprint may be created deliberately and consciously – for instance, through the choice of products or services, by accepting 'cookies' from websites that are visited, or by agreeing to sign up for a service or by using a social media service. There is, however, another element to a person's digital footprint that is created less consciously or that is created by third parties (often using data analytics, data enhancing through combining with other data sets and increasingly artificial intelligence) without the consent and/or explicit knowledge of the individual concerned. Sometimes described as a 'digital shadow', this represents an aspect of a person's digital footprint that has not been created or shaped by the person it represents. This shadow can affect the individual's personal reputation, the type of services or products offered, newsfeeds received or ability to access services. Yet this information has been neither created nor managed with any personal knowledge or consent.

Recognising that it is impossible to undertake any kind of digital interaction without creating some form of digital footprint, the participants were in general agreement that even those who believe they tread lightly in the digital world can leave a significant digital footprint. Fleeting interactions in the digital world can still leave permanent records, as one participant explained: *"I was contacted by an organisation about the ongoing use of my contact data, having attended an event organised around five years earlier and with no further interaction since that date!"* In this instance, the organisation was contacting the person to seek consent to continue using their personal data, but how many other organisations hold our data without regularly seeking such consent? As another participant noted: *"I could be the most private person in the world…and yet I'll have a digital footprint because of what other people put online which relates to me."*

A digital footprint can also be shaped by the method of data collection that has been consented to, often without the individual realising the full implications of the consent that is provided. For instance, we heard of the case of a fitness device manufacturer who pinpointed the epicentre of a recent minor earthquake *"using data gathered from the devices about users' waking and movement patterns on the day the earthquake struck!"*

Registering for any digital service requires the individual's acceptance of terms and conditions of use. Many participants felt these are often very difficult to understand, legally worded and therefore hardly ever reviewed by anyone before giving their consent in order to have access to a service or website. Perhaps a less visible and more frequent issue of consent relates to website cookies, which collect personal data and preferences on our web browsing behaviour, but which are rarely visible to the individual, who is offered very little choice over the data that is being collected and the cookies that are being placed in their web browser. It could be argued that individuals are made aware of cookies through notifications when they first visit a website, and that this offers an opportunity to review the terms and conditions of cookie use. However the whole process of placing cookies in one's web browser is based on assumed or informed consent, because the individual is not offered the option to use the website without such a process taking place. The balance of power is strongly in favour of the website operators, because refusal to accept cookies is only possible by not using a website, or by having the technical knowledge of how to remove any cookies placed in your web browser at a later stage.

Others were concerned that we are witnessing the downgrading the importance of privacy and transparency in some organisations in terms of information held and an individual's digital footprint. This was highlighted by a participant who explained that he had agreed to take part in a recent market research survey into the perceptions and practices of a social media company. When asked what should be the company's priority, he replied that it should be data protection. However, this response was not part of the pre-determined list of options. *"It was clear…that none of the individuals who were involved in designing this survey had thought that privacy issues were particularly important."*

And, finally, participants noted that few individuals recognise the longevity of the data that is being shared when they transact digitally. This was best summed up by the following comment: *"when you're actively posting your photos and information and putting your data out there, you are probably not planning for it to be up there and available for the next 80–100 years!"* but that is the reality of what many people are agreeing to when they transact digitally, sharing personal data and creating a digital footprint. Another participant went further in describing the naïve manner in which people are sharing data in the digital world, by referring to something they had read recently which described how in digital terms many people are "*pole dancing in public*", without realising how much of themselves they are exposing to public scrutiny.

The commercialisation of data

Despite these concerns, there was general agreement about the need to recognise the significant social and economic advantages that can be realised from sharing your digital footprint and associated personal data. Such benefits range from allowing purchase preferences and product recommendations to be offered efficiently when dealing with a regular retail website, through to much more strategic policy benefits that can be realised from health data or transport data, which can support better policy development, planning and research.

The value and potential gain that are possible from the commercial exploitation of our digital footprints is so great but we heard that many organisations collect and use this data without gaining informed consent to do so. One participant mentioned that some of the latest statistics on the effectiveness of email personalisation demonstrate the commercial value of holding personal preference data, with email personalisation increasing the likelihood of opening a marketing email four-fold. If this personalisation is combined with personal behavioural triggers, the response rate can be many hundreds of times stronger than without any personalisation at all. Participants suggested that such commercial opportunity could be driving organisational behaviour in a less than transparent and ethical manner in gathering personal data and exploiting our digital footprints.

Many citizens are unaware of the data analytics industry that has grown out of the benefits that can be realised from the analysis of our digital footprints. And many are unaware that, once they have shared personal data with an organisation, this data is often combined, analysed, re-used and sold to third parties for completely different purposes to those for which it was originally collected. Most of us know very little about how this is done, or by whom, but as one participant commented, *“there is a kind of shadowy, third-party data-brokering industry, which has absolutely no retail presence or reputation to protect”*. Nonetheless, this industry is using personal data provided by the user through transactions to determine, through the use of algorithms, what products you are offered, what news feeds you are recommended and what personalised services might be of interest to you. The lack of visibility, brand presence or reputation for these organisations allows these organisations to handle and exploit personal data in ways that some participants considered less than ethical, without fear of reputation or brand damage. As this is a relatively new capability, we have not, as a society, developed a *“reasonable expectation”* of how such data might be used, and to what end. As one participant noted, we need more people to ask: *“What analysis and what technology is being used to find out about you?”*

The participants also raised concerns about the equality and inclusiveness of the increased digitisation of society. They stressed the need to ensure that the opportunities and protections are available to all. This means ensuring that the needs of groups excluded by virtue of geographical location, age, income, educational attainment and physical as well as mental health are considered when developing any new privacy and data sharing standards.

We also heard – most notably from individuals who work in, or are connected with, the data analytics industry – that there seems to be a form of “*paranoid fear*” emerging about the negative consequences of providing third parties with access to your personal data and digital footprint. These participants felt that this paranoia is misplaced, because it focuses solely on the negative potential consequences, many of which are highly unlikely to occur, and ignores the many significant benefits which such data analysis can create. As one participant noted, there are in fact very few organisations with the capability and reach to influence what type of information and news a person might receive in order to influence personal opinion. Another participant noted: *“I wonder to what extent we are seeing concerns about our digital footprints arising as a result of middle-class, middle-aged concerns.”* Such exploitation of personal information is not a new phenomenon; digital just enables a different way of exploiting personal information, as noted in the following statement: *“the criminal use of personal data is not a new phenomenon, and a lot of* *criminality would have occurred without digital; digital just enables new ways of exploiting some of our vulnerabilities and means we need to educate individuals about how to stay safe."*

This led us to conclude that, as a society, we seem to be more concerned about third parties collecting and holding data on us than we are about the reality of how such data can, and is, being exploited to both the benefit and the disadvantage of society. Others, however, felt strongly that we should be concerned about the trade-offs between providing data and thereby gaining access services, and the invasion of privacy that this allows that are being undertaken, not simply because the conundrum represents the collection and exploitation of our personal data, but because it represents a profound invasion of our privacy and because, as one participant explained, a digital footprint and the collection of personal information *"can support sexual predators, incite violence or is an unacceptable invasion of our privacy."*

Equally important and ambiguous is the issue of consent, and the increasing reliance of organisations on 'assumed consent' in order to commercialise personal data for purposes other than what it was originally collected for. In effect, this means that third parties are deciding that, because someone consents to the collection and use of their data for one purpose, it is reasonable to assume they have given consent for their data to be shared or analysed for another purpose. One participant shared the example of a social media company using data about its users to test out ways of interacting with different user groups. This amounted to *"experimenting"* on its users, for which their consent had not been sought. Participants felt that this is both a less understood and an under-regulated aspect of data usage within the digital economy, and that because of the lack of transparency about shared expectations to guide how this activity is undertaken, there is a need to consider how the process of giving consent can become more informed. As one participant summarised: *"Consent of a different type is needed, but recognising that it wasn't even sought, never mind given, means that the question is really what is consent, and what do people actually consent to"* when they provide such authority?

Building on the issue of informed consent, the consultation heard about the lack of accessible explanation by many organisations as to why access to personal data is being requested. Often explanations are set out in the detailed terms and conditions statements, which cover every aspect of how our data will be collected, stored and shared. Because these long, complicated statements are densely legalistic in language and tone, most users agree to such terms and conditions without fully understanding what they are actually consenting to. Equally, we need to recognise that the balance of power is currently strongly weighted towards the provider of a service or product, giving the individual (consumer) very little option but to agree to the terms and conditions being offered. As one participant noted: *"every time you install a piece of software or sign up to a service, there are some insane legal documents which include reams and reams of terms and conditions, which are legally binding, but how many of us actually read them?"*

The exploitation of personal data is by no means restricted to private and third sector organisations. We heard how *"The government's sharing and surveillance policies make it* *as much a part of the problem as the corporate sector."* At the same time, some felt that the government has lagged the private sector in terms of capability and understanding of the risks associated with data collection and sharing. This lack of understanding of the risks and unintended consequences means that *"many policymakers don't really understand digital."*

In concluding this discussion on the commercialisation of data, we note that participants felt that as long as the commercial opportunity exists to exploit personal data and make significant commercial returns through access, sharing and analysis of personal data, a resource which has previously been described as *"the oil of the new economy",* there will always be tension between protecting customers' privacy and the desire by third parties to access and share personal data without giving a transparent explanation for the purpose and outcome of such a process. This is well summarised by the following comment, made by a participant in relation to a social media companies: *"The business model is basically the only way that they can make any money – by swapping personal information. It's a huge conflict of interest which they're in total denial about."*

The impact on trust

A key consequence of the confusion and tensions described above is that trust in the digital world is being eroded by a lack of transparency about and understanding of how our personal data is being collected and exploited, often for commercial return.

Interestingly, we heard how there is an emerging *"privacy paradox"*; citizens are sharing more and more personal data, while simultaneously expressing concerns about the consequences of doing so. Most people instinctively want to keep their data as private and protected as possible, and yet when presented with opportunities to share data, many do so without thinking through the implications and potential risks of doing so.

This paradox is perhaps explained by the fact that in spite of all of the concerns and potential issues of informed consent and trust, the potential benefits of the digital revolution are massive. As one participant noted: *"The benefits are huge, and the same way as the industrial revolution introduced a pace of change, in a dimension that people didn't understand, to the extent that regulation failed to keep up, now in exactly the same way the challenge is not what should we regulate, but how on earth can we regulate?"*

At the same time, however, we must recognise that, while digital society can offer many potential benefits, a minority of people actively use digital services to undermine trust, through, for instance, online bullying, trolling and other forms of pernicious and threatening behaviour.

Participants had differing views about whether the current lack of social norms and rules for transacting in a digital world is resulting in an erosion of trust, or whether this lack reflects the relative newness of the Internet, and that the situation will settle down into established codes of conduct over time. Alternatively, some felt that society could be seeing a situation where the fundamental openness of the Internet means that it will always be very difficult to establish standardised practices and norms.

Whichever scenario is followed, one issue remains consistent throughout, namely, that the rate of change is enormous and that policymakers and legislators have not been able to react with the speed and flexibility that is required. As one participant noted: *"what has struck me most is the very limited ability of national governments and nation states to control this issue",* meaning the issue of data collection and privacy. There is perhaps a need for greater collaboration at a supra-national level. New legislation and technology is now appearing at such a level, for instance, new data portability legislation adopted by the European Parliament. However, the adoption of new technology, such as Blockchain, is again set to disrupt the way in which we can access and share personal data. Policymakers need to recognise the speed of change and the need for greater social understanding of the implications, so they can decide how best to respond in a more agile and trans-national way. As one participant noted, we need to consider *"How do you reconcile tech moving very quickly with…centuries-old institutions like Parliament?"* And as another participant pointed out: *"The legal structures and the law are not keeping up to date, society is changing but not changing quickly enough, technology is rapidly changing, and in the shadows there are these people buying and selling all this stuff about us."*

Finally, perhaps one of the most important issues raised with regard to the erosion of citizen trust is the lack of understanding about society's expectations about data privacy and sharing. As one participant noted: *"Society is not saying what it wants, and what the red lines are."* If these expectations and requirements were better articulated and published, it would provide stronger guidance about what the citizen expects and requires to the organisations and third parties that are collecting and exploiting our personal data. Such a set of societal requirements could then help to facilitate change through the competitive nature of market forces. As one participant noted*: "Maybe the WhatsApp new offering in terms of encrypted messages is the beginning of a change in the market towards such a change."*

2. The benefits and risks of a digital footprint

When considering how a more informed digital society can be created, it is important to understand the motivations and concerns of different stakeholder groups. To this end, the consultation looked at the perspectives of citizens from three different generational groups (pre–generation X, mid-career and millennials) as well as the commercial and public sectors to identify what might motivate each group to move towards greater use of digital technology, and what risks and downsides might exist for each group. It should be noted that this is an initial brainstorm by the limited number of participants at the consultation and that these ideas should be further explored going forwards to validate and refine them. For example, it would be interesting to look at benefits and challenges in general and the extent to which these, and other specifics, affect different generations.

Pre–Generation X

For people who are categorised as pre–generation X (i.e. individuals born before the early 1960s), the benefits of having a lasting digital footprint were identified as:

- **Communication benefits:** new and easier ways of keeping in touch with family and friends
- **Day-to-day efficiency:** the ability to live more efficiently by, for example, spending less time in shops through the use of online retail
- **Efficiency of information sources:** the ability to access more information more efficiently; this may be both functional information (e.g. service information) or hobby information (such as family ancestry research)

The biggest risk and downside of digital for this group was considered to be the risk of scams and the way in which a digital footprint might create a 'digital shadow'. Given the relatively recent growth in digital services, this generation is considered to have lower awareness of how their data is collected and used, and may therefore share data more freely, without realising how it will be used.

Mid-career

For people who are mid-career (i.e. those in their early thirties to mid-forties), the advantages of the digital footprint include:

- **Convenience:** the ability to transact efficiently and conveniently in different aspects of daily life
- **Personalisation:** the growing ability to personalise services based on expressed and/or remembered preferences (an example would be LinkedIn and the ability to access career information, networks and personal references); the growth of digital-first services offers the potential for improved and tailored public services

It was recognised that people in this population segment grew up without many digital services. They lead busy lives, and so they are keen to take advantage of the benefits that can be obtained.

The potential risks and downsides of digital for this group focus around the loss of privacy, the potential abuse of personal data, as well as the threat of online abuse (targeting both children as well as the individuals themselves), and the seeming ubiquity of spam and junk communication. We concluded that, while the ability to obtain better services in return for sharing personal data is viewed as a good deal by individuals in this group, there is a high level of cynicism regarding such promises, with many companies being viewed as only being interested in collating more personal data for their own commercial gain. There is also a high risk of discrimination and potential for social exclusion within this group based on the ability and skills needed to participate in digital society.

Millennials

For millennials (i.e. individuals who reached young adulthood around the year 2000), there are many potential benefits to consider that accrue from having a digital footprint. Members of this group have grown up during the emergence of many digital services that are available today, and they view such technology as part of everyday life. The main benefits identified for this group are in the following areas:

- **Communication:** the ability to connect globally with others and manage one's communication and engagement on a truly global basis

- **Education:** the potential to access knowledge and learning opportunities more effectively, the scope for creating new job opportunities through innovation, and the creation of new ideas and thinking

- **Leisure activities:** the creation of huge leisure opportunities by digital technology, from online gaming to watching videos

- **Reputation:** the ability to build a trusted online presence over time; the ability to build a 'digital reputation' across different platforms by virtue of the longitudinal nature of one's digital footprint is considered a significant benefit

While such exchanges are not an explicit benefit, the group felt that this age group are more likely than others to offer personal data in exchange for free access to digital services and products. This group recognise the value of their personal data and are willing to trade off access to it for the benefit of free-to-use digital services.

A major risk of digital technology for this group was identified to be that decisions made when they were younger could have negative (and often significant) consequences later in life. Whereas previous (non-digital) generations grew up with clear and well-defined social norms and standards, this generation adopted digital technology with little explanation of what behaviours are consider acceptable and what the consequences might be of not adopting similar, expected social norms. As one participant noted: *"As a child you [could* *have said] something that could be misinterpreted or you could have just not have meant to say it [in that way], and now it affects your job prospects."*

To some extent, this risk has arisen as a consequence from the lack of "*digital parenting*", although, as discussed earlier (under Pre-Generation X), many parents of Millennials do not have any significant experience or understanding of the digital world and therefore are not well placed to offer parental guidance and support. In such a vacuum, it is important to find a new mechanism to educate and guide young people with regard to social norms and the consequences of having a digital footprint with longevity. Without such support and guidance, this generation has no mechanism to learn what behaviours are expected and how to avoid sharing personal views and information in a manner that may affect their life chances in later life. As one participant mentioned: "*[The digital world] is like a schoolyard with no teachers."*

Others expressed concern about another risk for this generation, namely, the lack of tools and support to help manage and prevent abuse and cyber bullying. There have been a number of high-profile cases of such cyber bullying, trolling, abuse and grooming in which digital technologies were the mechanism to enable such contact. The example was given of the case of a 14-year-old boy[1] who was groomed and murdered by a sexual predator who had used social media to make contact. Despite his parents' attempts to gain support from Surrey Police, he was not offered any support or protection.

Government and the public sector

Government and the public sector have embraced the use of digital technologies because they see this as a more efficient and less costly mechanism for transacting with citizens. There are a range of benefits, including:

- **Policy development and planning:** access to data sets and the ability to combine different data sets in support of more effective policymaking and planning decisions
- **Personalisation of services:** the ability to tailor services to better meet the needs of individual citizens
- **Communication:** a more efficient channel for the dissemination of information
- **Cross-agency sharing of data:** the potential to share data between different departments and agencies for more effective tracking of individual compliance with policy and legislation
- **Cost savings:** a more efficient (and in many cases automated) process for decision making and transacting with citizens

The final two benefits raised a number of interesting comments from participants with regard to informed consent and the increasing reliance on the use of algorithms and

[1] 'Breck Bednar Stabbing: Lewis Daynes Admits Boy's Murder.' BBC News, November 25. As of 7 October 2016: http://www.bbc.co.uk/news/uk-england-essex-30193056

automated decision making processes in transactions involving government and the wider public sector (for example, the NHS). The key issue or risk here is accountability.

In a more decision-automated digital world, how do you maintain a degree of personal accountability for ensuring that appropriate and accurate decisions are being made? Some went as far as to say there should be a new code of conduct for coders and individuals associated with the development of such automated processes and algorithms in order to set minimum standards, while others argued that algorithms should be increasingly open-source in nature – although on its own, this may not result in the degree of transparency that is needed to create accountability.

A further risk for government and the public sector is that, if norms and rules are not established and negative experience erodes individuals' confidence in digital technologies, then we may start to see the withdrawal of citizens from the notion of having a digital footprint, which will make it difficult for government and the public sector to exploit the opportunities which digital can provide.

Some argued that, in response to this risk, government should proactively establish a mechanism for delivering what was described as "*digital parenting*" within society, that is, helping society to create and establish the rules of the game. There was, however, general agreement that government is not well placed to deliver the role of digital parent in a constantly and rapidly changing environment, and that the optimal way forward is for government to ensure that a framework is in place that demonstrates the required behaviours and practices, but does not attempt to play that role itself. As one participant noted: *"Maybe it's that the government aren't the right people to do the parenting role, but they do have a responsibility to put in place the infrastructure that would then protect the vulnerable."*

A final interesting point which arose from our discussions regarding the role of government in creating trust within a digital society is that trust needs to be earned and governments need to focus on how this can be achieved. This will require government to segment the different types of data that are managed and to consider each type separately (e.g. health, location, income). It is not often that the use of silos is recommended in relation to public services, but in this case, if citizen trust if to be earned, silos will be important in the management of different data sets and data types.

Business and commerce

The private sector has embraced the use of digital for many of the same reasons as government and the public sector:

- **Understanding customers:** the ability to better understand customer needs and requirements and to tailor offerings more effectively
- **Innovation:** the ability to create new products and services, using stronger data sets, based on real-time understanding of customer needs
- **More efficient transactions:** more automated and efficient transactions, which reduce costs and enhance potential return on investment

The risks facing business and commerce are essentially similar to those facing government and the public sector, with trust being the underlying common theme. While the ability to access, aggregate and analyse personal data has huge commercial benefits, there is a risk that, without greater transparency and a clearer framework of rules and behaviours on how this will be undertaken, people may start to decline to share their personal data. This situation is likely to be exacerbated by the increasing number of bad-news stories in the press about how personal data is being misused or insufficiently protected. As one participant noted: *"Fundamentally, my belief is that the ones that built the greatest trust with their consumers, and their customer base, will sustain."*

The concept of a new 'trust covenant' was suggested as one mechanism through which greater transparency, consumer understanding and, ultimately, trust might be created. This covenant would outline, in accessible language, the roles and responsibilities of the different parties involved with respect to data handling and privacy, and it would set minimum standards. These standards could form the basis for a kite-mark mechanism through which organisations could become accredited as a means of demonstrating their public commitment to handle data in a responsible manner.

Others went further, suggesting that, if trust is key to survival in increasingly competitive markets, there is a need for commercial organisations to earn consumer trust by creating a new, more transparent relationship around data. "*There is a need to put the user in control*" of what happens to their data. The concept of user-managed access (UMA)[2] was outlined as a new mechanism for enabling individuals to control who has access to their personal data and for what purpose.

[2] UKAuthority. 2016. 'Putting Privacy and Consent in the Hands of Citizens.' April 20. As of 7 October 2016: http://www.ukauthority.com/news/6123/putting-privacy-and-consent-in-the-hands-of-citizens

3. Strategic Issues

Ten strategic issues around creating a more informed digital society emerged from this consultation. These are issues which will need to be considered and addressed if citizen understanding and trust with regard to data sharing and the benefits and consequences of such processes are to be achieved within society. In summary, these strategic issues are as follows:

(i) **Map existing protections:** Any future solution needs to be based on a clear understanding of what structures and frameworks already exist, and it needs to offer protection for individuals in terms of personal data and privacy. It will be important to resist the temptation to create new structures and legislation without considering what already exists.

(ii) **Define rules and protocols on data ownership**: There is an urgent need to define rules and protocols around data ownership. The picture at the moment is confused, with current legislation being seen as inadequate and based on 'implied consent' (that is, use without the individual's explicit knowledge). There is a need for more specificity in terms of how different types of data should be handled. And there is a need to define more clearly who ultimately 'owns' personal data, so that a new basis for sharing such data can be established.

(iii) **Protect personal privacy**: There is a need to place the commitment to protect every individual's right to privacy at the heart of any new rules about personal data. There is a need to give more power back to individuals, both as consumers and as citizens, so they can govern how their data is used and shared and so they have the opportunity to rescind their consent to its use when they wish to do so.

(iv) **Improve transparency**: One of the reasons why there is such confusion over personal privacy is a lack of transparency with regard to how third parties (including government) handle personal data. There is a need to define a new, accessible framework with regard to how personal data is collected and used, who can access it, and how one's digital footprint is being shaped by such activities. Such openness and transparency will support the development of citizens' confidence with regard to their personal data and the use of digital technologies.

(v) **Define the role of regulation**: There is a need to consider how we can encourage the adoption of new behaviours in relation to data provision and management, and what roles regulation and legislation should play within this process. A balance needs to be struck between encouraging change through informing consumers and allowing market forces to generate change, on the one hand, and the need for direct legislation and regulation, on the other. Because business will generally respond to market forces, there is a need to educate and encourage consumers so that they are more explicit in terms of what they require and what they consider to be 'red lines' in terms of data handling behaviour. This might encourage certain organisations to adopt new approaches as a means of differentiating themselves in a competitive market. At the same time, there is a need to recognise that regulation may be the only solution in certain aspects of data collection and management (e.g. to be able to penalise the sharing data with third parties without explicit and informed consent having been sought).

(vi) **Consider sanctions**: Linked to the issue of regulation is the need to consider what, if any, sanctions could be applied to encourage changes in behaviour and to encourage new social norms to flourish. Rights have little value if they cannot be enforced, and there is a need to consider what consequences should be developed for people and organisations that deny others their rights to access digital technology in a safe and secure manner. There is a need to have a debate about what sanctions might be appropriate and proportionate and how they could be implemented.

(vii) **Develop the concept of good 'digital citizenship'**: There is a need to consider how the concept of good digital citizenship might be developed and embedded across society. For many individuals, the key motivator for driving positive behaviour online will be to learn from experience and demonstration. This aims to enable more secure, enjoyable and productive digital experiences, while also being clear about how individuals wish to be treated by others. There is a need to consider who should lead the development of such a concept. Should it be led by government in collaboration with wider stakeholders, or should a new global structure be established?

(viii) **Create awareness and educate**: Developing the concept of good digital citizenship and appropriate standards of corporate behaviour will not be effective at creating societal change unless we consider how to communicate such concepts to citizens around the world and ensure that everyone in society is better informed and educated. Who, in effect, is to be responsible for delivering such training and 'digital parenting'?

(ix) **Use accountable algorithms**: The increased use of automated algorithms to support automated decision making in every aspect of product and service delivery means that there is a need to define who remains personally accountable for the accuracy and appropriateness of such decision making. If trust in digital technology is to be enhanced, there is a need to assure citizens, who are often not aware that such decisions are being made using an algorithm, how the decisions have been made and how they can be challenged. There is a need to define how algorithms can be more accountable to the individual consumer.

(x) **Maintain an international focus**: While this consultation has considered many of the issues from a UK perspective, there is a need to recognise that the challenge of greater transparency and awareness of how our personal data and our digital footprints should be managed is, in fact, a global challenge. Legislation, regulation and the concept of good digital citizenship will all require collaboration and coordination at a global, supra-national level if the changes are to be effective in a digital economy, which, by its very nature, does not recognise national boundaries.

4. Towards a new ethical framework

Throughout this consultation, we heard about a society that, as a whole, is struggling with the lack of rules and social norms to guide acceptable behaviour at the individual as well as the organisational level in this new, more digitally enabled world.

A common theme to emerge throughout our discussions, and from previous consultations held as part of the 2016 Thought Leadership series, was the need for a new ethical construct, or framework, that is able to address this gap. Such a construct would need to build on existing work, rather than starting from a blank page. As one participant put it, *"this shouldn't be about reinventing the wheel, but rather about pulling together and consolidating what is already there, and then if there are gaps, we can look to try and address those."*

As a starting point, the participants suggested five potential sources of existing legislation, knowledge and standards which should be reviewed as part of the development of this new ethical construct:

(i) **Article 8 of the European Convention on Human Rights:** This article covers the right to respect for private and family life. More specifically, it states that 'Everyone has the right to respect for his private and family life, his home and his correspondence' and that the state should not interfere with this right unless there is a clear national interest justification for doing so. That justification has to address questions of necessity, proportionality and accountability.

(ii) **The Tunis process:** Globally, the UN facilitates the Tunis process, which seeks to create a forum for government and civil society to debate the future of the Internet.

(iii) **New data portability legislation:**[3] Adopted by the European Parliament in April 2016, this legislation will create a new right for people to 'transfer their personal data in a commonly-used electronic format from one data controller to another without hindrance from the original controller.' In other words, it will make it harder for organisations to put barriers in the way of people who want to take back their data, having previously shared it with a third party.

(iv) **Professional standard-setting bodies:** For example, the bodies responsible for standards in market research (the Market Research Society of Great Britain) and standards in statistical analysis (the Royal Statistical Society) set out how professionals in their relevant sector or field should conduct themselves with regard to the data held on research participants and service users, including with

[3] European Commission. 2016. 'Joint Statement on the Final Adoption of the New EU rules for Personal Data Protection.' As of 7 October 2016: http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm

respect to confidentiality, attribution and secure storage. It was felt by participants that such protocols could be adapted for use in a new digital construct.

(v) **Recent work undertaken by the cross-party think tank Demos[4] on 'digital citizenship':** This work is focused on developing a framework covering the norms, manners, responsibilities and basic values of online citizens.

Principles

Having considered current sources of learning and legislation, we identified the key principles that should underpin any new ethical framework of rules and social norms in a digital world. Seven core principles were identified, as follows:

(i) **Welfare and wellbeing:** We heard a strong message that the overall focus of this new framework should be on making life better by improving welfare and wellbeing for citizens. There are many potential benefits from having a clearer set of rules and social norms for digital society, such as enhanced productivity and greater efficiency, but at its heart the new construct should be seeking to improve the lives of all citizens.

(vi) **Accessibility:** The framework needs to be written in an accessible language, so that it will be understood and therefore accepted by all, and not by just a select minority of people within society. The use of 'plain English' as a drafting standard was recommended by many participants.

(vii) **Practicality:** Linked to the issue of accessibility is the suggestion that the new framework needs to give practical, non-technical examples of what represents good behaviour in a digital context. To be effective, it must not describe a set of high-level generalities but, instead, provide real-life practical examples to people of what is and is not acceptable behaviour.

(viii) **Good manners:** The framework needs to set out explicitly what represents good 'digital manners' in different contexts and be clear about what represents bad digital manners. It is important that the focus be on manners, defined as the inbuilt way you conduct yourself - which can be applied to everyone, as opposed to etiquette, which is the expression of rules - which can be used to exclude people.

(ix) **Rights and responsibilities:** The framework should include clear rights and responsibilities for different parties operating within digital society, recognising that everyone (both individually and organisationally) has a responsibility to adopt certain core behaviours and responsibilities towards each other in terms of how data is shared, stored and used. These rights and responsibilities should empower people to make choices about their own digital footprint, about when it is shared and on what basis, and about how to rescind authority to share.

(x) **Cultural sensitivity:** Recognising that any new framework will need to have global appeal if we are to encourage change across digital society, participants noted that there is a need to consider and be sensitive to cultural differences in terms of the

[4] http://www.demos.co.uk/research-area/centre-for-analysis-of-social-media/

sharing and use of data. For example, members of a persecuted group or their descendants, or inhabitants of countries with a history of political repression, may feel far less comfortable about sharing data than people in countries where there have been stronger controls on privacy.

(xi) **Citizen-centric:** There is a need to create a mechanism which allows citizens to demonstrate more efficiently the kinds of trust building and ethically sound behaviours they want to see in a digitally enabled society. This mechanism could take the form of markets and other interactive spaces, but ultimately it will enable individuals to provide practical examples of the behaviours they wish to see if we are to create a more trusted and ethically sound digital world.

This discussion concluded with the idea that a new framework based on the principles listed above could be used to encourage and embed the shared notion of digital citizenship across society.

5. Conclusions and next steps

This consultation closed with the identification of five main conclusions about the most effective ways in which society might be better equipped to understand the benefits and consequences of transacting in a more digital world.

(i) **Create a new narrative for digital rights and responsibilities*:*** Recognising that the past two decades have seen an unprecedented rise in new digital technologies and systems, with a rate of change that has never been seen before in human history, we concluded there is a need to create a new narrative for a global civil society, which is human by default but digitally enabled.

Based on the principle of the Gettysburg Address[5], which was delivered succinctly in around 2 minutes, the consultation attempted to draft an initial narrative to describe the rights and responsibilities of everyone in a more digitally enabled society. This initial narrative has been reproduced below.

Building the World's First Global Civil Society: Human by Default

- *The past two decades have seen the rise of new, digitally based technologies and systems as never before in human history. The pace and scale of change is unprecedented.*
- *A totally new narrative for human society is emerging, with new challenges and opportunities, both physical, virtual and emotional.*
- *Emergence of a digital identity for all individuals is creating a new narrative for human social interaction. One side effect is intentional and unintentional harm caused by the exploitation of digital identities.*
- *After 20 years of playful and imaginative creativity, there is now a pressing need for a new maturity to address these issues if we are to harness the benefits of the digital opportunity and avoid the harms; in effect, we need to usher in a new renaissance.*
- *We need to generate a set of digital rights and responsibilities to protect human dignity and capture societal benefit.*
- *In response to these challenges and opportunities, we should develop ethical models of justice and equity to ensure that they are human by default, not digital by design, in our globally connected age.*

The narrative suggests that we need to generate a new set of digital rights and responsibilities to protect human dignity and capture social benefit. Such rights and responsibilities should be designed from the core principle of *"human by default, not digital by design"*. Such factors as social justice and individual wellbeing should

[5] https://www.ourdocuments.gov/doc.php?flash=true&doc=36&page=transcript

be the priorities, rather than efficiency or technological progress for the sake of progress.

On a more practical level, there remains the question of how such a set of new rights and responsibilities would be embedded on a global scale. However, there may be opportunities for promoting many of these rights and responsibilities into digital citizenship courses and workshops, including through educational institutions and workplaces. For example, such courses and workshops could take into account lessons already learned and described in the literature to develop and roll out a programme of digital citizenship.

(ii) **Map what already exists in terms of digital ethics:** There is a need to map what legislation, research and insight are currently available. Recognising that much work has already been undertaken globally around the issues associated with data access and sharing and around how to create a more informed digital society, participants noted that there is a need to identify in a systematic way what already exists, so that proposals arising from this consultation can be mapped on to relevant activity.

There is a significant body of existing material to review, and we concluded that any mapping should start at the trans-national level, reviewing the work of UN, European Union, as well as UK-based policy developments around digital strategy, intellectual property and data protection, before broadening the remit to include the work of leading academic institutions, think tanks, professional standards bodies and NGOs (including the work of the 'Web We Want' campaign), and faith groups.

(iii) **Encourage greater dialogue and public engagement:** Linked to the development of a new narrative regarding ethical conduct and rights and responsibilities within a digital society is the need to start a more informed conversation across society with regard to trust and digital citizenship. If we are to embed behaviour change across society, any changes will require the buy-in and commitment of different stakeholder groups and will need to ensure that the interests of different stakeholder groups are represented, both in the dialogue and in the final outcomes. While such a process will take longer than current systems to reach a final outcome, it was felt by many participants that it would be the most appropriate way in which to design a new set of ethical rights and responsibilities for a digital world.

Initial thinking suggested that such a dialogue could be undertaken using an informal coalition that includes government (at all levels), industry, academia and civil society. There is a need to engage each of these groups from the start, so that they all have a chance to shape the debate, instead of being left to respond to ideas and decisions that have already been taken by others. It was suggested that, to prevent any dialogue becoming a permanent 'talking shop' with limited action or outcome; there should be a clear focus from the start on the intended outcomes – that is, on establishing a new framework of digital rights and responsibilities.

Further work is required on who might 'host' such a discussion and how such an initiative might be funded. A number of neutral suggestions were made, such as the Confederation of British Industry (known as CBI) and the Institute of Business Ethics. Others suggested that such an initiative should have a well-respected and visible figurehead to chair the group – for example, Baroness Lane Fox or the Government Chief Scientific Adviser (who is independent of government). We envisage that this host would be supported with representation from across government, business and civil society. Further work is now required to define the terms of reference for this group and to consider funding options.

(iv) **Encourage stronger parliamentary engagement:** There is a need for stronger parliamentary engagement in the issue of digital ethics to influence future policy development and to raise public awareness. Parliament holds a unique set of powers, and it has an important role to play in terms of reviewing evidence – in a non-partisan, non-political manner – so that any gaps may be identified and suggestions may be made on how our legislation could be strengthened to better support the development of a more ethical and more informed digital society.

Although we heard throughout the consultation that government should not be responsible for implementing many of changes that are required, participants felt that government does have an important role to play in terms of facilitating change across society and encouraging greater partnership working. The possibility of establishing a parliamentary committee or a 'speaker's conference' should therefore be investigated. Establishing such a committee would also represent an opportunity to take evidence from a range of different sources, including citizens, and to better understand the attitudes of the public as well as organisations and other interested parties around ethics in a digitally enabled world. Such independent research and evidence would be valuable for influencing future policymaking and also any legislative changes which might be required.

To facilitate this parliamentary engagement, there may be scope for establishing a parliamentary inquiry to consider the issue of digital citizenship and the role of trust in encouraging growth in a digital society.

(v) **Conduct public awareness campaigns:** We concluded that there is a need for two types of public awareness campaigns to be considered as part of the creation of a more informed digital society.

The first campaign would focus on the objective of digital inclusion, encouraging individuals who do not currently use digital technologies to consider adopting a more digital approach to transacting, by giving them a clearer understanding of the benefits and the risks of transacting in this manner.

The second campaign would target those individuals who are already transacting digitally with a 'Know your footprint' campaign, aimed at creating greater awareness of what one's digital footprint is, and focusing on five specific aspects of one's footprint in particular:

- Good and bad behaviour around sharing data
- Information that can be more dangerous to share (such as physical addresses)
- Protocols around sharing the data of others
- The data market – how people's data is collected and used, and the role of cookies in this process
- Identity fraud – how it is committed and how to avoid it

Market segmentation will play an important role in how this campaign is delivered. While the key messages should be the same, the method of delivery is likely to change by target audience. Therefore a segmentation model needs to be developed based around age, current level of digital experience, usage of digital technologies, and other relevant factors, so that more relevant channels can be identified for each segment of the population. Several participants also felt that an online game format would be a useful way to raise awareness and engage interest among younger age groups. At the same time, a series of public information articles in the national press would be helpful to draw attention to the campaign at an early stage.

Next steps

This consultation was one of four topics covered in the Corsham Institute 2016 Thought Leadership Programme investigating the opportunities and challenges created by digital technologies in society.

The other topics were:

- Digital health: Digital's role in health and care
- Cyber and resilience: Digital's role in regaining resilience
- Digital living: Getting the most out of digital society

A key findings report[6] highlighting the overarching themes to emerge from across this year's programme, as well as the key findings from each of the four consultative events, is now available for download on the Corsham Institute website.

[6] Corsham Institute and RAND Europe. 2016. Thought Leadership 2016 Programme: Key Findings. RR-1771-CI Santa Monica, Calif.: RAND Corporation.

Ci and RAND Europe look forward to building on the findings from the 2016 Thought Leadership programme with a series of further Thought Leadership consultative events to be held during 2017 that will focus on:

- Education
- Open science
- Currency
- Civic engagement

Participants

Name	Position	Organisation
Claire Alexander	Chief Operating Officer	Corsham Institute
William Barker	Deputy Technology Leader (Strategy, Resilience & Futures)	Department for Communities and Local Government
Isobel Brown	Director/Chair of Grants & Commissioning Committee	Forces in Mind Trust
Janina Cross	Chief Digital Transformation Officer	West of England Academic Health Science Network
Phil Dawson	Chief Executive	Assured Digital Group
Talitha Dubow	Research Assistant	RAND Europe
Katie Ghose	Chief Executive	Electoral Reform Society
William Heath	Partner	Kelston Tump LLP
Trevor E Hilder	Management & ICT Consultant	Cavendish Software Ltd Nailsoup Ltd
John Houghton	Principal Consultant	Shared Intelligence
Till Lembke	Consultant	GoodCorporation Ltd
Sakara Malcolm	Creative and Digital Media Apprentice	Corsham Institute
Dr Catriona Manville	Research Leader	RAND Europe
Dr Lucy Mason	CONTEST Review Lead	Home Office
Carl Miller	Research Director, Centre for the Analysis of Social Media	Demos
Alisha Miranda	Managing Director	I.G.Advisors
Helen Olsen Bedford	Publisher	UKAuthority
Dr Marcus Alexander Ong	Commercial Director	Smart Societies Institute

Name	Position	Organisation
Brian Parry	Director, Strategy and Thought Leadership	Corsham Institute
Dr Sunil Patil	Senior Analyst	RAND Europe
Hans Pung	President	RAND Europe
Dr Tristram Riley -Smith	PaCCS External Champion	PaCCS, Centre for Science & Policy, University of Cambridge
Daniel Sprague	Technical Director	Smart Societies Institute
Mark Svenson	Head of Analytical Services (OIC Central)	NHSE
Marianne Talbot	Director of Studies in Philosophy	University of Oxford
Dr Gareth Thomas	Shareholder, Adviser	GoodCorporation Ltd

Thought Leadership 2016 programme delivered by:

Corsham Institute

http://corshaminstitute.org

Corsham Institute (Ci) is a not-for-profit organisation whose mission is to accelerate an inclusive digital society that is citizen centric and trusted. We do this by creating a physical and intellectual space to convene, connect, educate and innovate across sectors.

Ci was formed in 2013 to explore the opportunities and benefits of digital society, both social and economic, with particular focus on shaping a future where individuals can realise their potential in a highly connected world.

Our four key areas of work are promoting digital skills and education, driving research and thought leadership, powering enterprise and realising digital communities.

Our values are to work openly and collaboratively and to make a sustainable contribution to the economy for both national and commonwealth public good. We do this by imagineering, co-developing and sponsoring services for citizens and government where trust, ethics and informed consent come first.

RAND Europe

http://www.randeurope.org

RAND Europe is a not-for-profit organisation, whose mission is to help improve policy and decision-making through research and analysis.

Part of The RAND Corporation, we were founded in 1992 to provide quality impartial research and rigorous fact-based analysis, and to serve the policy needs of EU institutions, governments, charities, foundations, universities and the private sector. Our work lies between that of universities and consultancies, combining academic rigour with a professional, impact-oriented approach. In other words, we operate as a research-focused business, using a professional services model within the context of a public good mission.

We combine deep subject knowledge across many policy areas – including health, science, innovation, defence and security, transport, infrastructure, criminal justice, education, employment and social policy – with proven methodological expertise in evaluation, impact measurement and choice modelling.

St George's House

http://www.stgeorgeshouse.org

St George's House was founded in 1966 by HRH The Duke of Edinburgh and the then Dean of Windsor, Robin Woods, as a place where people of influence and responsibility can gather to grapple with significant issues facing contemporary society.

The House offers a safe physical and intellectual space, rooted in history but focused firmly on the future. The emphasis throughout our carefully-crafted consultations is on dialogue and discussion to encourage creative thinking, informed debate and sustained engagement. This is a place where participants can make a real contribution to society, where personal enrichment and social progress are mutually compatible, and where Wisdom is nurtured.