MRS Reports/2015

Private lives?

Putting the consumer at the heart of the privacy debate

Lead author – Colin Strong
MRS Delphi Group

MRS Evidence Matters™

Contents

Foreword

Edwina Dunn, co-founder of dunnhumby & CEO of Starcount

The debate surrounding the privacy (and security) implications of harnessing our personal information is by no means a new one.

When I founded dunnhumby with my partner Clive in 1989, one of our key considerations was putting "customers first" – ensuring that the value customers received from relevant offers and benefits was a fair trade for the data revealed about their shopping. Indeed, we needed customer data to be relevant and we made every effort to collect only what we needed to improve the shopping experience. Just because we knew something, we didn't always use it, adhering to an important guideline of "cool", not "creepy".

Today big data insights have extended to driving the fight against disease, strengthening national security and boosting political engagement, to name just a few.

Yet today, as this white paper outlines, the environment in which our data is harnessed is increasingly complex. Personal data is collected as we tweet, shop or even speak, with multiple insights gathered from physical or digital footprints. Data is now a valuable currency, and it is traded in increasingly "big" quantities; consider that just two years ago, 90% of the world's current data didn't exist.

As a consumer, it is increasingly difficult to keep your personal information private. 92% of Apps are free and consumers know that they are free because their data is collected and used. It's a trade that is accepted but not always understood. And so, consumers are increasingly aware of the value of their data and will inevitably become savvier and more selective with whom they share it. What do they get in return? Consumers hold the ultimate sanction, which is to remove permission or, even worse, stop buying the brand if trust or respect is lost.

But in the midst of the privacy debate it is easy to forget the benefits of what this report refers to as the 'datafication of our lives'. Take the retail industry. The Tesco Clubcard provided consumers with both discounts and a more tailored shopping experience through the gathering of their data. Today big data insights have extended to driving the fight against disease, strengthening national security and boosting political engagement, to name just a few.

The success of the Clubcard was built upon the fact it was mutually beneficial to both the consumer and retailer. Today this principal must continue to underpin "data monetisation" as it is currently expressed by many leading global businesses. For consumers to willingly provide their data, they must be shown the value and experience first-hand the benefits of doing so. Otherwise the result is a disengaged consumer base that feels exploited.

Transparency and security is equally essential. If organisations fail to clearly articulate how personal data will be used and with whom it will be shared, the relationship between consumer and brand, and the brand's image, runs the risk of being irreversibly damaged.

"92% of Apps are free and consumers know that they are free because their data is collected and used. It's a trade that is accepted but not always understood."

In the coming years and decades, the data landscape will continue to evolve. There are real challenges and developments around best practice in data architecture and design for all businesses and governments. These include the concept of separating and streaming personal and non-personal data to ensure that the power of insight is practical but that the danger of personal identification is minimised. Such developments are crucial and integral for digital enablement and personalisation – challenging but also empowering when well designed.

This commendable report helps lay out the debate as to how this could be achieved for both consumers and data-gathering organisations alike.

Acknowledgements

This paper has been compiled by the MRS Delphi Group. The Group would particularly like to thank for their contributions: Nick Bonney, Cat Wiles, Edwina Dunn, Rachel Glasser, Tim Britton and Sue Unerman.

About MRS Delphi Group

The MRS Delphi Group is led by a collection of the most respected thinkers in the marketing and research sectors. Drawing on the intellectual capital created by the UK's agencies, the Group delivers valuable insight across a range of important business, social and political issues, including most recently an investigation into the role of the insight function within client organisations. See mrs.org.uk/delphi

The Steering Group includes: Nick Baker, Managing Director, Quadrangle, Chair of the Delphi Group; Clare Fuller, Director, Promise Corporation; Caroline Plumb, CEO, Freshminds Research Ltd; Phil Sutcliffe, Director TNS; Colin Strong; Suzi Williams, Marketing Director BT; Nick Bonney, Head of Insight, Camelot; Tim Britton; Cat Wiles, AMV:BBDO; Jane Frost, CEO of MRS.

About the author

The lead author of this report, Colin Strong, is a UK-based consumer researcher working with a wide range of brands and public sector organisations to help shape their consumer strategies. The focus of his work has always been around 'data' and the way in which it is reshaping our relationships, both between individuals as well as between brands and consumers. He is very engaged in the way the research industry can use ever increasing amounts of data for new consumer insights that, at times, replace but more typically complement, more mainstream forms of consumer research. Colin is also very involved in exploring how the data economy is fundamentally reshaping business models and public policy.

Colin is a regular speaker at conferences and a contributor to a wide range of publications and blogs. His book, 'Humanizing Big Data' is published by Kogan Page. MRS would like to thank Kogan Page for allowing content that first appeared in 'Humanizing Big Data' to appear in this paper.

Twitter: @colinstrong

Blog: colinstrong.net

Executive summary

The increasing datafication of our lives inevitably creates benefits for institutions – brands can sell us more, governments can identify security risks more easily, welfare agencies can spot fraud and so on. And the disclosure of this information certainly provides benefits for individuals – we benefit from institutions knowing something about us individually – creating new services, better customer experience, maintaining our heath and our safety.

But while we have got used to the idea that disclosure of our personal information has bought us benefits, there has perhaps not been enough discussion about the implications of what we are giving up. And linked to this, the terms of the debate have been very limited, with definitions of privacy feeling somewhat constrained in their nature, not properly reflecting the breadth of behaviours that privacy represents.

Putting the consumer at the heart of the debate

The nuanced, context-dependant nature of privacy is such that we need to have that debate across a wide variety of situations in which this issue is relevant.

The market research sector can provide an important new perspective on the privacy debate. Much of the discussion to date has been driven by technologists, lawyers and politicians but there has been relatively little from the perspective of the individual.

This paper pulls together the various strands of work relating to privacy into a single focus – that of the relationship between the individual and the brands, organisations and institutions that he or she interacts with.

Five key points

The issues around privacy that are discussed in this paper lead to five key implications which we believe need further exploration and discussion in the public realm, and within organisations and institutions. They are:

1

Avoid simplistic thinking:
The definition and management of privacy is not something that we can leave to the back-office, to be encapsulated by some terms and conditions. Privacy is a complex issue that requires strategic and considered engagement. The voice of the consumer must be clearly heard; so involve them in the design of privacy mechanisms and messages, rather than leaving it to the technical (or legal) specialists.

2

Understand the long term implications:
Encroaching on our inner, personal lives produces long term effects that can be hard to measure. The trade-off between short term tangible gain (data) and long term intangible downsides (trust) needs to be explored by organisations and institutions, and metrics defined accordingly. More organisations need to measure trust as a key lead indicator of their long term performance.

3

Avoid linear thinking:

It's easy to assume that there is a straightforward, linear relationship between the level of disclosure and derived benefits. Human patterns of behaviour are non-linear, and as such we need to explore the nature of these relationships and perceived benefits. Privacy is passive and active – witness the increasing use of tactics to hide an individual's identity and movements online. Institutions need to understand where the privacy boundaries are and how they vary by context.

4

Understand the value exchange:

People are recognising the value of their personal information and institutions need to be prepared for a more robust justification of what is currently being traded in exchange for disclosure. Value is not just monetary, but social and emotional as well.

5

View privacy as an opportunity rather than a threat:

A more positive approach to privacy can be used to enhance both the quality of life of people, and the success of institutions. To do this, you need to start by building, and then sustaining, trust. For example, by managing customer communications transparently and honestly.

Defining terms

It has become more important than ever to better understand privacy. The increased use of technology has created huge amounts of data about ourselves that is fundamentally changing the privacy environment. The way in which institutions are able to analyse this data to draw inferences about individuals challenges the way in which we manage the distinction between our inner and outer lives. It is the management of the boundaries between the inner and outer that we consider critical to the privacy debate.

The way in which we think about privacy has been shaped by our history; the shift from privacy as a social to an individual construct took many years to form. We are now at a point where we consider that a sense of privacy as a 'personal right' is culturally important in the West. Understanding the historical legacy of privacy is important as it helps us put into context the forces that are now shaping our attitudes.

Changing landscape

Privacy has long been the preserve of the more powerful members of society; we are seeing the very same trends being drawn in current technology behaviours.

The technology landscape has fundamentally changed the way in which organisations gather information about individuals; very granular information can now be collected about some of our most intimate behaviours. This potentially shifts the power balance between individuals and organisations as we may be inadvertently revealing personal information that we may not even know about ourselves. The more affluent and better educated in society can increasingly take steps to manage their privacy; this has potential for a 'two-tier' system where institutions know a great deal about the less advantaged members of society and much less about the better off.

Understanding the historical legacy of privacy is important as it helps us put into context the forces that are now shaping our attitudes.

Changing environment

It has long been argued that surveillance can have a damaging effect on an individual's sense of identity or self. While the effect of government surveillance on society at large has been explored, there has been little research to understand the effect of this on consumer brand relationships.

Privacy and trust are closely related – effective management of privacy will likely engender trust and vice versa. The challenge that institutions have is that privacy is as complicated for them to navigate as it is for consumers – it is likely that any institution will get it wrong at some point. Research suggests that more trusted institutions will be punished more by individuals. In this context it is a serious challenge, given the desire of most organisations to enhance and deepen relationships.

How consumers manage privacy

The trade-off in costs and benefits between privacy and disclosure is often not clear to consumers and citizens. This helps to explain the apparent paradox between stated preferences for privacy and actual disclosure. If individuals feel unable to make decisions concerning privacy then there is potential for mistakes to be made and for trust in institutions to be undermined.

Our evolving, increasingly technology mediated environment means that the way in which our privacy behaviours manifest themselves will develop and change; it does not mean that our desire for privacy has necessarily changed.

Institutions and privacy

It is impossible for people to always read the terms and conditions governing privacy that they need to sign up to in order to use services. Trust frameworks are one way in which a common set of rules, tools and infrastructure can be used to simplify the process; if institutions can work to these then people need only assimilate the T&C's once. The question is whether these are sufficient for the management of privacy.

There is much debate about the degree to which society has a right to privacy, versus the safety and well-being of its citizens brought about by state surveillance. The debate about the trade-off between our privacy and security needs to be broadened out in order to properly recognise the nature of the impact that incursions on our inner lives can have on the health of our citizens and society.

Join the debate

This White Paper is an attempt to broaden the privacy debate and help organisations and institutions properly consider the implications from the perspective of individual consumers and citizens. You may agree with much that is written in this document; you may vehemently disagree. You may believe there are points that need clarification or issues that have been missed or even misunderstood. We welcome the debate, and to this end we include comments from different reviewers at the back of the document. Please feel free to make your contribution.

New research: the individuals' view

Tim Britton presents the key findings from the latest YouGov research, undertaken in February 2015.

So what do we think about our privacy? Does it matter to us? Are we concerned? Is any concern growing or changing? Or is it all a lot of fuss about nothing?

To understand our collective view on privacy in a little more detail we asked a range of questions to a nationally representative group of people taking part in a YouGov omnibus survey. Clearly, anyone willing to be a member of YouGov's (or indeed anyone else's) research panel in the first place has a particular view on privacy, so it is likely that the very privately minded are excluded from our findings. Nonetheless, these findings provide a clear and useful guide to how the nation is thinking.

In short, the research shows that we do care about privacy and we are caring more now than we did in the past.

We recognise a value exchange when we share our data with organisations, but we tend to think that the organisation collecting our data gains more benefit than we do individually. Further to this, a significant number of us do not feel that we have a high degree of control over what of our personal information is kept private.

And finally, levels of trust between individuals and the organisations that collect our personal data vary tremendously across different organisation types.

This all supports this report's contention that this is not a simple area, and that understanding the value exchange in terms of its actual value to individuals, and the equity of the exchange, is of critical importance if public trust is not to be eroded.

We care more and more, yet we're not sure we are getting the benefit

The privacy of personal information is considered more important to us now than it was five to ten years ago, with 70% of us saying it is now more important, and only 5% saying it is less so (the balancing difference either say 'the same' or 'don't know'). This broad view is quite commonly held, but age also matters as there is a clear pattern whereby the older you are the more likely you are to say privacy is of 'much more importance' now: 44% of the 55+ age group give this answer, compared to 35% of the under 35 group.

70%

of people say that the privacy of their personal information is now more important than it was five to ten years ago

58%

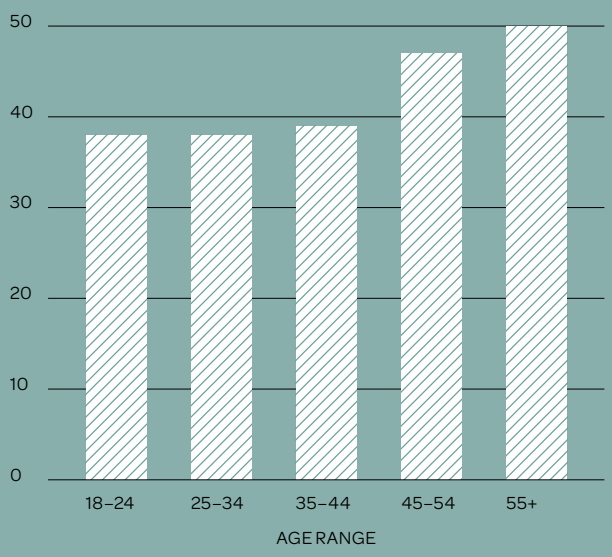
of people believe that we get value from company held data

In terms of a value exchange for the personal information that organisations hold about us, a majority of us do recognise this exists. When asked about the information we share with organisations, only around a quarter of us think that the other party get all of the benefit, giving us nothing back. However, whilst a majority of us think that we do get some form of value (58% believing we get value from company held data and 55% from government held data) we also think that the collecting organisation – rather than the individual – get the best of the deal. 64% of us think that companies get more or all of the benefit, and 60% think the same of government held data. Again there is a difference by age, with the 55+ age group being more likely to think that the organisation rather than the individual benefits most.

We don't all feel in control

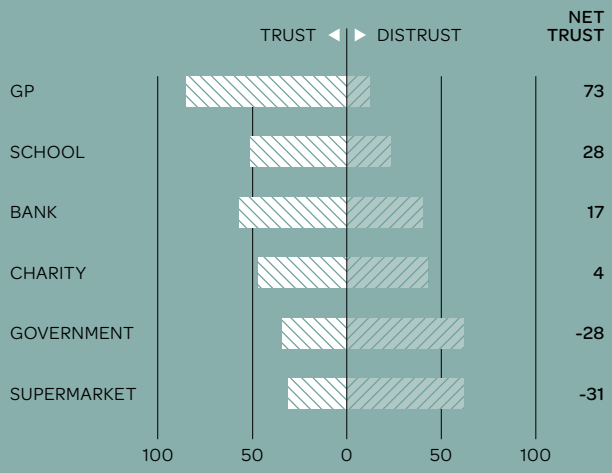
When asked how much control, if any, we feel we have over what of our personal information is kept private, only one in ten of us feel in complete control. But this rises to five in ten when we add in those of us who feel we have a fair amount of control. However, this does leave large swathes of the population feeling we have either not very much (36%) or no (8%) control over what of our personal information is kept private. And again, age plays a significant role: the older we are the more likely we are to feel that we have not very much or no control.

% SAYING THEY HAVE NOT VERY MUCH OR NO CONTROL OVER WHAT PERSONAL INFORMATION IS KEPT PRIVATE



TRUST = 'I TRUST THEM A GREAT DEAL OR A FAIR AMOUNT TO KEEP MY PERSONAL INFORMATION PRIVATE'

DISTRUST = 'I DON'T TRUST THEM VERY MUCH OR AT ALL TO KEEP MY PERSONAL INFORMATION PRIVATE



We don't view all data collectors as equals

As Strong argues, privacy and trust are closely related, and this makes the effective management of privacy a complex challenge for individuals. Our research clearly shows that different institutional types are invested with different degrees of trust, and there are some surprises in how different institutions rank: we trust our GPs, schools and banks significantly more than we do supermarkets and the government. So whilst banks have suffered dramatically in the trust stakes over recent years, we do still have an underlying level of trust that they will look after the (very) personal information which they hold about us; whereas the government has a big brother reputation which makes it hard for us to trust.

Whether we like it or not, sharing our personal information is part-and-parcel of modern day life. Further to this, we may well be getting a greater value from sharing our personal information than we know, as the value of product and service creation which our collective data provides can often be hidden from us as individuals. However, the perceived mis-match in the value exchange, could well have long term trust implications and have an impact on our willingness to share personal information. This is something that data holding organisations, not least the government, need to address.

All figures, unless otherwise stated, are from YouGov Plc. Total sample size was 2,168 adults. Fieldwork was undertaken between 17th–18th February 2015. The survey was carried out online. The figures have been weighted and are representative of all GB adults (aged 18+).

Introduction

It's fair to say that we have a complicated relationship with privacy. We tend to think of it as enormously important, even seeing it as a human right. But we live in an age where, as historian Jill Lepore puts it, "the only thing more cherished than privacy is publicity."[1]

So we feel compelled to place an amazing array of information about ourselves on social networking sites but at the same time worry about the way the same information could be used by prospective employers. Some of us take steps to reduce the personal information that is collected about us online but then expect brands to offer relevant services based on our past histories. We seem to struggle to manage these competing demands.

Of course, privacy has always been a balancing act between our personal and public lives. However, what has changed is the way in which our personal lives have become captured by data. As more of our lives are lived out through technology, ever more intimate aspects of our lives are made available for scrutiny by others. The boundaries between our inner and outer worlds, our private and public spaces seem to be increasingly thin.

As more of our lives are lived out through technology, ever more intimate aspects of our lives are made available for scrutiny by others.

So have these environmental factors changed consumer attitudes and behaviours around privacy? There are certainly differing views on the degree to which our desire for privacy is universal and fixed, or amorphous, and subject to changing social norms. On the one hand, philosopher Alan Westin believed that privacy is a fundamental need that "may well be rooted in his animal origins, and that men and animals share several basic mechanisms for claiming privacy".[2]

On the other hand, we can see cultural differences in attitudes suggesting that privacy (or at least its' manifestations) is subject to the vagaries of social norms. So, for example, we may argue that privacy has historically been less valued in China (at least in the way it is understood in the West – although this is changing) where complete strangers will consider it perfectly acceptable to ask personal information about your weight or your salary, topics that are taboo even among close friends in the West.[3]

Looking at the issue from an historical perspective, Jill Lepore argues that our contemporary sense of the importance of privacy ultimately derives from a time when our institutions based their power on what was often called "mystery". In the case of religion this was the "mysteries of God," and in the case of governments this was the "mysteries of state". As our institutions have become more open, that sense of "mystery" has become secularized and ultimately is now a concept that accrues to the individual rather than institutions. So on this analysis, we consider it imperative to manage our personal privacy more than ever.

And this is perhaps why our concept of privacy is so complex. It is intimately wrapped up with our notion of selfhood, the Western idea that we are independent, cognitively evaluating beings. Privacy is something that needs protecting, something that we need to keep to ourselves, for which we preserve sanctity. Perhaps there is a fear that if our inner lives can be open for all to see then we may not be as individual as we had hoped, and that our secret desires and fears are in fact common and predictable.

Privacy is often approached in a very practical way by governments and brands alike. It has long been the preserve of the 'compliance officer' who has been responsible for determining and then policing the boundaries between the individual and the institution. But the data economy has changed all that. Institutions are now in a position where they may well know more about the individual on particular topics than they know about themselves. For example, pretty good estimates can be made about your life expectancy based on what you have in your shopping basket. Institutions are now asking us to trade off our privacy so they can get access to our data for any number of apparent benefits: for more secure lives by defeating terrorism, for access to services that make our lives more enjoyable and rewarding, for making our cities more efficient. The list of possible benefits that are traded for disclosure is endless.

So much has been written about privacy, it is hard to see what else can be added to the debate. However, one area appears to be lacking. And that is the way in which *we, as consumers or citizens*, think about and behave in relation to privacy. What is our experience of privacy and invasions of it? Just why are we motivated to protect what is, fundamentally, a construct, an idea rather than something necessarily very tangible? It is this that this paper seeks to explore and in doing so contributes to the wider debate of just what do we do about privacy?

Key points:

— The issue of privacy is complex and multi-faceted; we cannot expect easy answers to the complex questions it raises.

— Much of the previous work and thinking around privacy has been either legal or philosophical (with a few notable exceptions); this paper focuses on the consumer experience.

— A useful way to think about privacy is the way in which we manage the distinction between our inner and outer lives.

— The increased use of technology has created new challenges for separation between these lives; this paper is primarily about the way in which increased availability of personal data is changing the privacy environment.

1

Part I

Defining terms

This section aims to:

— Provide an exploration of what we mean by privacy

— Give a historical context of the way in which the concept of privacy has changed over time

What is privacy?

The literature on privacy includes plenty of discussion about the value and function of privacy but less about what it is actually is. And this is where the problem starts. As philosopher Judith Jarvis Thomson noted, "nobody seems to have a very clear idea what it is".[4] A very wide range of activities fall into privacy violations, from a newspaper reporting the name of a victim of an assault through to a company selling its list of customers who have purchased a particular product. The sheer breadth of activities that could be considered privacy violations means that we cannot rely on a single term to properly reflect its meaning.

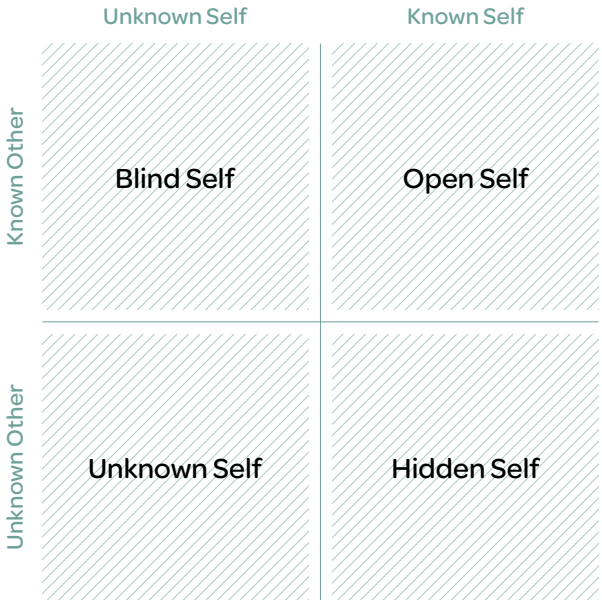
Law professor Daniel Solove considered that privacy is a collection of different issues that is best understood as a 'family resemblance concept'. So the different manifestations of privacy may not share all the same characteristics but are nevertheless still related to each other.[5] He cites the way in which philosopher Wittenstein made the analogy to members of a family who share some features (such as eye colour, height, hair colour and so on) but not others; indeed they may not have one common feature. Instead there is a 'complicated network of similarities overlapping and criss-crossing'.[6]

Solove goes onto create a taxonomy of privacy which identifies different forms of privacy problems relating to information collection, information processing, information dissemination and invasion. It's certainly worth reading the literature on this for a better understanding of the breadth of activity that could be considered relevant to the concept of privacy.

While this reflects the legal profession's deliberation over privacy issues (which is certainly important to our understanding of the terms and definitions), it does not necessarily aid our understanding of the issues from the perspective of the consumer experience. Instead, this falls to the market research profession – understanding the individual experience and articulating the implications of this for organisations.

So this paper examines privacy from quite a different perspective to that which is often found elsewhere – we consider privacy to be about the boundaries between your inner and outer worlds. What you may consider to be outer world and therefore public, and what you consider to be your inner world and therefore private will, of course, vary as a function of context, individual preference, society norms etc.

A useful framework to understand the way in which we think of these boundaries is the Johari Window. It was created in the 1950s by psychologists Joseph Luft and Harry Ingham[7] (the framework is named using a combination of their names). The Window divides all relationships into four areas, determined by whether the information is known to the individual or the world, or for our purposes, to the individual or the organisation.



To elaborate on the four categories:

Open Self
This is where the information is shared by both the individual and the organisation. So my shopping behaviour with my supermarket falls into this category, since we both share the same knowledge about it.

Hidden Self
This is information that I know about myself but my supermarket does not know. This would include my shopping activity at other supermarkets but also major life events, my desires and aspirations. Much (but not necessarily all) of this is what I might reasonably consider to be private.

Blind Self
This is where the supermarket knows things about me that I don't know about myself. This might include my profitability to the organisation, the degree to which I have optimised my shopping activity, where I sit in their segmentation and how the organisation intends to engage with me. Although this is perhaps not private (in the sense that I did not know this information about myself) I might nevertheless have some sensitivity about how this is handled and may feel that others knowledge of this could be an invasion of my privacy.

Unknown Self
This is where information about me sits that neither the supermarket nor I know. I may have unconscious needs and desires that are not yet revealed even to myself, let alone my supermarket. The issue here is that the information contained within the Unknown Self has yet to be formed but when it does so, then it may well quickly be something that I may wish to be kept private.

Using this model is helpful for us to start understanding the way in which we negotiate our privacy with other people but more importantly, with institutions. As organisations collect more information about us from a variety of sources, then the amount about me which is unknown to institutions (such as my supermarket or the Government) starts to shrink. My Hidden Self starts to shrink as my activity with other brands is increasingly available to organisations through sharing or selling consumers' personal data. This may have a negative effect on my relationship with the supermarket as I start to feel uneasy about the way increasingly accurate inferences are made about my social or family life based on my shopping behaviour. But also my Blind Self starts to decline. And perhaps we intuitively sense this but clearly are not in a position to know this.

Privacy is always something that is defined with reference to others – the issue is who those others are, what the information is, what the context is and so on. There are no absolutes, everything is relative. Which makes this such a complex area to navigate and indeed, makes it a topic which goes to the very heart of what it is to be human.

What we therefore need to do is explore the way in which we think about privacy to try and disentangle the motivations of humans, and see if we can draw some broad conclusions about the way in which we would like to manage the distinction between public and private.

Key points:

- Definitions of privacy are hard to arrive at – instead we should consider it a collection of activities.
- This paper explores it fairly simply in terms of the distinction between our inner and outer lives and the challenge we have as individuals of managing this.
- The Johari Window has long been used to explore our relationship with self and others; it is also a useful mechanism for looking at the way in which personal data is starting to change these dynamics.

The balance between our inner and outer lives

As we mentioned in the last section, Jill Lapore traces the history of privacy back to the way in which the mysteries of institutions have become secular. Once the mysteries of the church were considered beyond the wisdom of any person to comprehend but during the Reformation, Protestants rejected many of these mysteries as superstitions. Mystery moved instead to the trappings of the state and their attendant royalty. So by the seventeenth century, the "mysteries of state" referred to "both state secrets and monarchical power and right—not what God knows, and we do not know and must accept, but what the king knows, and we do not".

But of course these notions of the royal prerogative were challenged. Political reformation put knowledge that was once the preserve of royalty into the hands of the politician, and the common person. So we can see the way in which our sense of privacy has moved away from institutions and into the hands of individuals, wishing to guard against encroachment into personal affairs.

This move from the importance of institutions to individuals is not without its critics. Philosophers such as Richard Sennett[8] and Christopher Lasch[9] have bemoaned the preoccupation with the self at the expense of involvement in public affairs. They would consider this to reflect an alienation and seclusion from public life. As Sennett puts it in his book 'The fall of public man':

"Masses of people are concerned with their single life histories and particular emotion as never before; this concern has proved to be a trap rather than a liberation."

Nevertheless, a sense of 'privacy' as an individual act holds to this day and indeed our notions of privacy are accompanied by a sense of entitlement that we can expect it as a right. Much of this can be traced back to an article by two Boston lawyers, Samuel Warren and Louis Brandeis published in 1890 in the Harvard Law Review called "The Right to Privacy."[10] Warren and Brandeis were classmates at Harvard Law School and upon graduation they opened a law firm together. Warren married Mabel Bayard, a senator's daughter, in 1883. This generated, what was then, huge amounts of gossip about the Warren-Bayard family in newspapers—including front-page stories about the funerals of Mrs. Warren's mother and sister. Warren felt that this had violated his family's privacy which, like a letter, had been purloined.

In their article "The Right to Privacy," the lawyers argued that there is a legal right to be left alone—which had never before been defined. They believed that privacy had not always been necessary but the definition of 'publicity' had changed and as such there was a need to protect this 'right'. At the end of the nineteenth century, publicity had meant transparency. As philosopher and reformist Jeremy Bentham put it, "Without publicity, no good is permanent: under the auspices of publicity, no evil can continue".[11]

However, Warren and Brandeis argued that the meaning of publicity had shifted and changed. Publicity now meant (as we often more or less see it now) drawing the attention of the press. So while putting political decision making into the public domain was a good thing, making public the names of those attending at Mrs. Warren's mother's funeral was not.

"If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place"

The principles raised in this case have thus become embedded in law – our desire for privacy is almost sacred in its notion as protector of our individual sanctity. We see it as a right that we go to great lengths to uphold. So what does it mean when Eric Schmdit of Google says "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place"[12] or when Mark Zukerburg claims that privacy is no longer a social norm?[13] Are we seeing a point in history where the tide has turned, when the nature of our interactions are such that we need to rethink the way in which we consider privacy?

Key points:

- The way in which we think about privacy has been shaped by our history; we can see the shift from privacy as a social to an individual construct took many years to form.
- The sense of privacy as a 'personal right' is culturally important in the West.
- We should not ignore our historical roots and accept that in some contexts (and indeed in other cultures) privacy may be more important at an institutional rather than individual level.
- Nevertheless, we should also recognise that attitudes typically take a long time to change, and we should be wary of jumping to the conclusion that they have fundamentally changed, when they may still be evolving.

2

Part 2

The changing landscape for privacy

This section aims to outline the way in which the privacy landscape is being drawn, specifically:

- How personal data is changing the way in which our inner lives are increasingly available for others to view
- How management of our privacy is not always equal in our society

The increasing datafication of our lives

Without doubt, the environment in which we seek to practice our privacy has fundamentally changed.

As Kenneth Cukier and Viktor Mayer-Schonberger write in their book 'Big Data: A Revolution That Will Transform How We Live, Work and Think',[14] the world is increasingly becoming 'datafied'. By this, they mean putting a natural phenomenon in a quantified format so it can be tabulated and analysed. As humans we have always attempted to datafy the world – think mapping, scientific experiments, weather forecasting, and censuses. But what has changed is the degree to which modern IT systems have facilitated this process. IT fundamentally alters our ability to quantify the world, through the way in which phenomenon are now effectively transformed into data, and via our ability to store and then make sense of that information.

There are a multitude of ways in which data is revealing more about consumers, revealing a rich seam for us to draw on for our analysis. Some of the ways in which we are increasingly datafied are outlined below.

Datafication of sentiment/emotions

The explosion of self-reporting on social media has led us to provide very intimate details of ourselves. For example, with billions of people now using Facebook andTwitter, we have an incredible database of how people are feeling. Many market research companies use this by 'scraping' the web to obtain detailed information on the sentiment relating to particular issues, brands, products and services.

Datafication of interactions/relationships

We are now not only able to see the way in which people relate, but with whom they relate. So again, social media has transformed our understanding of relationships by datafying professional and personal connections. Historically, our ability to collect relational data has necessarily been through direct contact. Studies were limited to the social interactions of small bounded groups such as clubs and villages. Social media, or indeed analysis of telephone calling patterns, now allows us to explore relationships on a global scale.

Datafication of speech

It is it not just the written word or connections that have come within the ambit of datafication. Speech analytics is becoming more common, particularly as conversations are increasingly recorded and stored as part of interactions with call/contact centres. As speech recognition improves, the range of voice-based data that can be captured in an intelligible format can only grow.

Call centres are the most obvious beneficiaries of speech analytics, particularly when overlaid with other data. They can be used to identify why people call, improve resolution rates, ensure that those who answer a call follow their script, improve the performance of call centre employees, increase sales and identify problems.

Datafication of what is traditionally seen as offline activity

Within many data intensive industries, such as finance, healthcare and e-commerce, there is a huge amount of data available on individual behaviours and outcomes. But there is also a growing awareness of the potential to utilise big data approaches in traditionally non-digital spheres. For example, retailers have been gathering enormous amounts of data from their online offerings but have struggled to do the same in their bricks- and- mortar stores.

That is changing through innovations such as image-analysis of in-store cameras to monitor traffic patterns, tracking positions of shoppers from mobile phone signals, shopping cart transponders and use of RFID. When overlaid with transactional and lifestyle information it becomes the basis of encouraging loyalty and targeting promotions.

Facial recognition software is also growing more sophisticated. In the UK, supermarket giant Tesco has even been experimenting with installing TV-style screens above the tills in a number of its petrol stations. They scan the eyes of customers to determine age and gender, and then run tailored advertisements. The technology also adjusts messages depending on the time and date, as well as monitoring customer purchases.[15]

So things have changed since Warren and Brandeis published their famous article. We are now at a point where information about each and every one of us is routinely gathered by both government agencies and a wide variety of commercial organisations. However, it is one thing to gather it, but what is actually done with it? In a sense, do we really care what people know about our shopping habits? Some of us may, but on the whole these activities could be viewed as fairly innocuous. Indeed, in the case of retailers, they have long been studying the behaviours of their customers. The Victorian shopkeeper was the original one-to-one relationship manager working hard to understand customers' individual tastes and quirks.

Of course, this has evolved massively through to today's supermarket chains where relevant offers are increasingly based on individual shopping habits. The wealth of data provided by loyalty cards has brought a new depth to personalised offers, and of course even those who don't use them or pay by cash can still be tracked through detailed and segmented demographic data.[16]

It is the online dimension, however, that is transforming data collection. As people do more and more of their daily activity online, cookies can track their every move, while still newer-technology is getting much smarter at identifying even those who actively try to avoid being monitored or who access the web through mobiles, which don't use cookies.

One example is a technique called fingerprinting, which can establish an individual's unique signature by looking at what plug-ins and software have been installed, the size of the screen, the time zone and other features of any particular machines.[17] A wide-ranging investigative project from MIT and Belgium's Louvain University has found that mobile phone records identify users even more accurately than their own fingerprints, even if the phone is turned off.[18] Of course, this ability does raise many concerns, not least the fact that individuals can be identified from what were considered to be anonymised records[19] (so-called re-identification techniques). Nevertheless, to a large extent people are (albeit often unwittingly) allowing themselves to be identified if not by actual name but with a unique ID that allows them to be targeted consistently with relevant marketing materials.

The objective for many institutions, however, is to start to derive particular attitudes and mindsets from the behaviours embedded in our digital footprints. If we can start to understand some of the 'softer' characteristics of people from their hard behavioural data, it opens up a huge set of opportunities for marketers and indeed security personnel, because it tells them much more interesting information about people.

A study by Cambridge University and the Microsoft Research Centre have allowed us to 'look behind the curtain' and start to understand the extent to which inferences from behavioural data can be used to predict a variety of personal attributes including religion, politics, race and sexual orientation.

Their research[20] involved 58,000 Facebook users in the US who completed a psychometric questionnaire through the Facebook app 'myPersonality'. Those taking the test were asked to provide the researchers with access to their Facebook data. This gave the team an immensely rich data source to work with, allowing them to link the results of the personality test and demographic profiles with a person's Facebook Likes.

The team were able to create some highly predictive models using these Likes. For example, they were able to identify male sexuality and sort African-Americans from Caucasian Americans, Christians from Muslims, and Republicans from Democrats. There were also some pretty impressive figures for predicting relationship status and substance abuse. And not all the Likes that were used for modelling necessarily explicitly referenced the outcomes. So, for example, who would have anticipated that liking curly fries correlated with high intelligence, or that people who liked The Dark Knight movie tend to be less sociable? In fact, there were relatively few obvious Likes to work with: fewer than five per cent of gay Facebook users in the study had 'liked' gay marriage, for instance.

So while people may consider that what they are revealing about themselves is anodyne and is not sharing anything of their inner lives (that they may prefer to keep hidden), the reality is far from this. Increasingly we are in a position where we can start to determine an awful lot about people from relatively small amounts of behavioural data.

And to return back to the Johari Window as an explanatory framework, these developments perhaps reflect the extent to which our inner lives are starting to be eroded. Institutions know things about us that we may have hoped to keep to ourselves (our Hidden Self), but are also starting to identify characteristics about us that we may not even have known ourselves (our Blind Self). And surely this fundamentally changes the landscape within which we seek to manage our privacy.

Key points:

— The technology landscape has fundamentally changed the way in which organisations gather information about individuals; very granular information can now be collected about some of our most intimate behaviours.

— Inferences can be made from this data which goes well beyond our behaviours alone. We are increasingly seeing that inferences can be made concerning a wide range of personal attributes and dispositions.

— This potentially shifts the power balance between individuals and organisations as we may be inadvertently revealing personal information that we may not even know about ourselves.

Is all privacy equal?

The previous section identified the way in which our data landscape is significantly changing, making it harder to manage our privacy. But this is not distributed equally throughout the population. We examine what the dynamics are of this and implications for organisations.

Writers June and William Noble focused on the link between privacy and power.[21] They considered that privacy allows or asserts power, and power confers privacy. They write about the circular way in which there is a lack of privacy among the poor which in the workplace leads to stress. The resulting lack of assertiveness means that important boundaries to maintain privacy cannot then be established. And in her book Privacy, Intimacy, and Isolation (1992) the philosopher Julie Inness points out that privacy protection can act as a means of maintaining the dominance of groups or individuals.[22] Noted sociologist Barry Schwartz discusses the way in which privacy maintains social divisions. In the armed forces for example, officers will enjoy their own quarters and private toilets while the lowly ranks will be in dormitories and communal toilets.[23]

We like to think of privacy as a choice, but this choice is not always available to the more marginalised members of society.

And this is what we see in stark reality today as our data trails are able to track individuals like never before. So as reported by Virginia Eubanks[24], Amercian author of 'Digital Dead End: Fighting for Social Justice in the Information Age', welfare recipients are more vulnerable to surveillance because they are members of a group that is seen as an appropriate target for intrusive programs. She argues that immigrant communities are also more likely to be the target of biometric data collection than native-born communities because they have less political power to resist it.

Marginalized groups are in the dubious position of being subject to the cutting edge of surveillance. While some forms of surveillance, like filmed police interrogations, are undoubtedly positive, these same people are subject to some of the most technologically sophisticated and comprehensive forms of scrutiny and observation in law enforcement, the welfare system, and the low-wage workplace.

At the other end of the spectrum, those with money can buy their way out of surveillance.[25] For example, the Blackphone is a $629 Android-based smartphone that has privacy-protecting software installed to allow users to send encrypted texts and make encrypted calls. The handset is apparently enjoying real success.[26] Another device, the OFF Pocket, is an $85 mobile phone case that blocks signals to and from the phone.[27] Both devices are out of reach of the more marginalised, privacy-infringed members of society.

And Reputation.com is just one of many companies that help you to maintain a spotless profile online.[28] For $99 a year you get a basic "reputation starter" package, which monitors when you are mentioned online and provides alerts if anything sensitive comes up, such as "your real age, name, address, mugshots, legal disputes or marital problems". And for $5,000 a year, the firm will "combat misleading or inaccurate links from your top search results".

And some of this is simply having the educational background and or time to implement privacy defences. A recent study found that over one in five visitors to websites now have some form of ad blocking software in place.[29]

Privacy has always been the preserve of the powerful but there is little doubt that with the advent of personal data this age-old issue is becoming ever more polarised. We like to think of privacy as a choice, but this choice is not always available to the more marginalised members of society.

Given that a person's ability to manage their own privacy is not consistent across society, organisations need to consider ways in which different groups need to be engaged and informed about these options. If the collection and usage of personal data is seen to be an activity that is primarily located within more vulnerable groups in society then organisations and brands leave themselves exposed to a number of criticisms. Brands may find that their more valuable customers are not properly represented in their data activities and therefore the return on their investments start to decline. But they may also be in danger of reputational risk by not respecting their customers' privacy in a consistent manner. This is an issue that has no simple answers but it is certainly one that needs greater consideration.

Key points:

- Privacy has long been the preserve of the more powerful members of society; we are seeing the very same trends being drawn in current technology behaviours.
- There is potential for a 'two-tier' system where institutions know a great deal about the less advantaged members of society, and much less about the better off.
- There are moral hazards associated with this, but it also creates a challenge for institutions as they become increasingly reliant on insights from this data.
- This also has the potential to set-up power imbalances that may start to create reputational risk.

3

Part 3

The impact of a changing environment for privacy

This section aims to explore the effects of changes in the way we manage privacy, specifically on:

- Perceptions of self-hood
- Changes to individuals' relationship with both brands and government institutions
- Effect of privacy violations of trust in institutions

The changing data landscape

We seem to have come to a point at which the balance between our inner and outer lives is starting to shift, and we need to understand what the implications are for both individuals and organisations. A key impact that our changing landscape may be having is on our notions of identity and personhood.

As we have seen, much of our modern notion of privacy rests on how it protects the sanctity of the individual. Professor of Philosophy Michael Lynch sees privacy as being "intimately connected to what it is to be an autonomous person". For without privacy "I learn what reactions you will have to stimuli, why you do what you do, you will become like any other object to be manipulated. You would be, as we say, dehumanized." And as he goes on, "when we lose the very capacity to have privileged access to our psychological information — the capacity for self-knowledge, so to speak, we literally lose our selves." So privacy is deeply entwined with the concept of having a 'Self'.[30]

This has been reflected in the way in which other philosophers have considered privacy. Hannah Arendt is often mentioned in this content. Her book, 'The Human Condition' set out some of the basic tenets of privacy: it guarantees psychological and social depth, holding those things that are vulnerable to the constant presence of others; it supports the public by establishing those boundaries which fix identity; and it preserves the sacred and mysterious spaces of life.[31]

Carl D. Schneider related the sense of privacy to the sense of shame in his book, 'Shame, Exposure, and Privacy'. He considered that there were many areas of human activity where privacy is related to dignity. The open display of bodily functions can threaten dignity, leaving an individual vulnerable to being reduced to mere bodily existence. Hence, the function of privacy and shame is to preserve wholeness and integrity. As such, human relationships demand a pattern of mutual and measured self-disclosure and respect for others.[32]

June and William Nobile deplored what they saw as the modern devaluation of privacy. They noted that until the late twentieth century, diaries, letters and biographies were considered as private legacy from the deceased to family, and account how this sanctity has declined through the growth of straight autobiography. They considered that privacy keeps emotions and acts from being trivialized. So, what is important is kept private.[33]

What all these thinkers have in common is the way in which privacy is important to foster a sense of 'personhood'; a reflection of the way in which we as humans respect each other as separate beings. It is instructive, therefore, to examine the effects on individuals of the way in which governments routinely subject their citizens to surveillance. In the former German Democratic Republic (DDR) it is estimated that one in 6.5 members of the population were acting as informers for the Ministerium für Staatssicherheit or Stasi.[34] It is hard to unpack the impact of surveillance itself but author Anna Funder suggests that extreme levels of state surveillance in the DDR reduced the ability of young people to establish their own identity, making them either passive and compliant or angry and subversive.[35] Ian Brown's report on this area is definitely also worth reading.[36]

And related to this, there is plenty of evidence that a reduction in the extent to which people can control their own disclosure (surveillance means you are less able to of course) affects the ability to effectively manage social interactions and position oneself in relation to available social identities.[37] danah boyd coined the term 'context collapse' to reflect the way in which our current digital lives make it much more difficult to navigate between our different identities (husband, colleague, sports team member), as information that we make available in one context is then available in another, which we may of course not welcome. What you communicate to your partner is not something that you would necessarily want to be read by a work colleague, and vice versa.[38]

So surely there is a strong argument that if the part of our lives that is inner and private declines, then it has a strong impact on the way in which we operate in the world. Our relationships are in danger of suffering if we are not able to express ourselves freely and openly without fear that in another context the very same information could be embarrassing or damaging to ourselves. Our sense of freedom to be ourselves is somehow lost.[39]

But what are the implications of this for organisations? There is some evidence that this has the potential for negative consequences for brands, which is what we explore next.

What you communicate to your partner is not something that you would necessarily want to be read by a work colleague, and vice versa.

An uncanny data valley?

As we see above, there is a strong case that the widespread practice of 'dataveillance' (the systematic use of personal data in the monitoring of the actions or communications of individuals) can have a negative effect for the individual but can the same be said for the organisation undertaking this activity?[40] Research undertaken by Colin Strong and fellow researchers Dr Guy Champniss and Dr Kiki Koutmereidou explored this very issue through the use of the concept of the uncanny valley.[41]

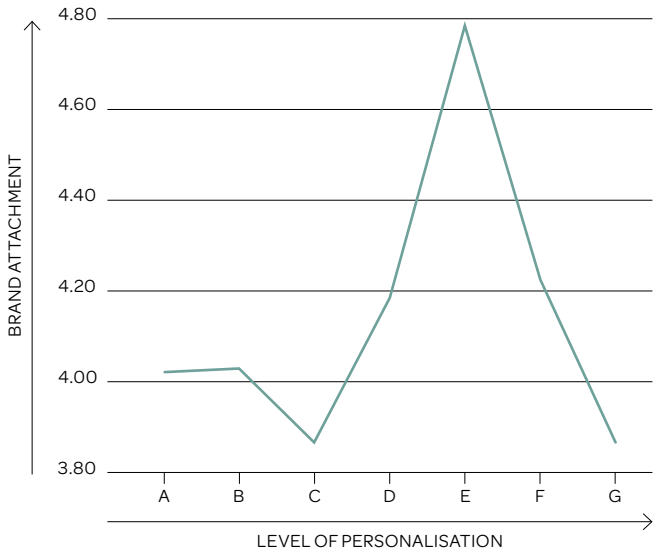
The term uncanny valley was first used in 1970 by Japanese roboticist Masahiro Mori[42] who noted that, although we tend to warm to robots that have some human features, we feel uncomfortable when they start becoming too realistic. And while there has been little empirical evidence to support this claim, it has nevertheless been gaining momentum steadily ever since.

The uncanny valley effect has since been blamed[43] for the failure of a number of films that used CGI to produce very humanlike characters but where the audience is aware that they are, in fact, animations. The film *Polar Express* is often cited as an example where the effects left it with lacklustre box office sales, whereas films such as *Brave* or *The Incredibles* used characters that were clearly not human, and fared much better as a result.

The research undertaken by Strong, Champniss and Koutmereidou was used to identify an uncanny valley phenomenon in relation to marketing communications. Initially, consumers enjoy the personalisation of marketing communications, with steadily improving brand attachment as personalisation increases. However, there then appears to be a line which is crossed when there is too much personalisation for consumers' comfort and brand attachment rapidly declines, falling into an 'uncanny valley'.

The research, as shown in Figure 1, certainly suggests that this is the case – albeit with a little variance early on in the data.

FIGURE 1: IMPACT OF INCREASED PERSONALISATION ON BRAND ATTACHMENT



Of course, *where* brands tip over into an uncanny valley may well depend on a variety of factors. Some categories may be more associated with hyper-personalisation and therefore more accepted. What is considered appropriate for Google may not be right for a consumer goods brand. There were very clear differences in receptiveness to targeted advertising across different population segments – partly, but not wholly, based on demographics such as age, gender and lifestyle.

Marketers need to start asking where the uncanny valley might begin for their organisation, because the brand's marketing activity might just be doing the opposite of what is intended and actually turning consumers off. Similarly, governmental schemes to improve citizens' lives may not be adopted as enthusiastically as hoped due to this phenomenon.

So what this illustrates is that while 'dataveillance' gives organisations a better understanding of individuals' inner lives, which clearly has tangible near term benefits, there appear to be unexpected consequences. Institutions need to be mindful of these effects and weigh up the benefits against our emerging understanding of the downside. Just what kind of society do we want? What kind of customer base do you want for your brand? In terms of the Johari Window, shrinking individuals' Hidden or Blind selves may not always be worth the costs.

Key points:

— It has long been argued that surveillance can have a damaging effect on individuals' sense of identity or self.

— While the effect of government surveillance on society at large has been explored, there has been little research to understand the effect of this on consumer brand relationships.

— Research has suggested an uncanny valley effect where the consumer brand relationship can suffer as a result of the intensive use of personal data.

— Institutions need to better understand the unexpected consequences that may come with intensive use of personal data.

The effect of privacy violation on trust

If consumers find it difficult to navigate privacy and make consistent decisions on what they consider to be right for them, institutions may equally find it hard to predict how consumers will react to the ways in which their data is used. Indeed, institutions are highly vulnerable on this topic, particularly given the received wisdom that the real value of data relates to its potential – and not just its current – usage.

As Cukier and Mayer-Schonberger argue,[44] "Data's true value is like an iceberg floating in the ocean. Only a tiny part of it is visible at first sight, while much of it is hidden beneath the surface. Innovative companies that understand this can extract that hidden value and reap potentially huge benefits. In short, data's value needs to be considered in terms of all the possible ways it can be employed in the future, not simply how it is used in the present."

Cukier and Mayer-Schonberger may set out a very cogent case for this, but as set out in the last section, part of the story is surely missing: how the consumer feels about this and the impact on the relationship between the individual and the institution.

What you communicate to your partner is not something that you would necessarily want to be read by a work colleague, and vice versa.

In the worst case scenario, there is the potential for the careful work on building trust undertaken by governments and brands to start to crumble. Susan Fournier has long espoused the importance of relationships with her ground-breaking paper, *Consumers and their Brands*[45], published in 1998. Her research has established a clear framework for the evaluation of consumer-brand connections and examined the damage that a breakdown in trust can cause. And while this is referenced in the context of brands, it could apply equally well to government institutions.

Together with colleagues Jennifer Aaker and S. Adam Brasel, Fournier explored[46] what happens when things go wrong for brands through a two-month field experiment in which 48 consumers formed a relationship with an online photographic service brand called Captura Photography Services. Two contrasting 'personalities' were created: one was 'sincere', with classic and traditional core values, the other 'exciting', with a more modern, irreverent feel.

Some 48 'customers' interacted with the service one to three times each week over the two-month period. But then they were told that a staff member had accidentally erased their online photos. Two days later they were sent apologies when the online albums were restored.

What is particularly interesting is that the 'sincere' brand, which had developed strong bonds with its customers, suffered more in terms of customer perception than the 'exciting' service. After the apology and recovery, the latter was able to forge a better relationship with customers, allowing it to establish trust, accountability and responsibility in their minds for the first time.

As Aaker warns, when trust, which is central to successful marketing, is violated the effect on the brand can be devastating. This makes the issue of personal data and privacy critical to brand management since brands increasingly use personal data to build long-standing relationships with customers. To quote Aaker, "When trust is violated—as it often is in long-standing relationships—particularly those established with a sincere, warm and honest partner—it can be devastating. So be aware of the type of brand partner you are, the type of relationship you are helping to create, and the expectations that are being set in the consumer's mind." More research is needed to better understand the way this phenomenon may work in relation to privacy violations but it certainly suggests that there are pertinent issues here which merit further exploration.

Nevertheless, brands and governments that use personal data will inevitably find themselves getting it wrong at some point. The impact this will have on a brand will clearly vary. But the message from Fournier's work is clear: sincere brands that are attempting to generate trust will suffer the worst when they transgress.

Key points:

— Privacy and trust are closely related – effective management of privacy will likely engender trust and vice versa.

— The challenge that institutions have is that privacy is as complicated for them to navigate as it is for consumers – it is likely that any institution will get it wrong at some point.

— The work of Susan Fournier would suggest that more trusted institutions will be punished more by individuals – a serious problem given the desire of most organisations to enhance and deepen relationships.

— Understanding individuals' expectations and assumptions around the way in which personal data is used, and their privacy managed, is therefore essential for any organisation.

4

Part 4

How consumers manage privacy

This section examines the activities that consumers undertake to manage privacy and the challenges they encounter while doing so. Specifically:

- How the psychology of privacy helps us to understand the apparent paradox between attitudes to privacy and actual behaviours
- How teenagers, often considered to be more relaxed about privacy, are in reality very concerned about this issue and take steps to properly guard it
- An exploration of what we mean by 'privacy'
- A historical context of the way in which the concept of privacy has changed over time

How we make decisions about privacy

We have seen in previous sections that living in a data mediated world can make it extremely complicated for individuals to manage the balance between their inner and outer lives. Yet, we seem to be in an environment where people want to be able to do just that. We value our privacy – at whatever level it is set. But as privacy researcher Prof Alexander Acquisti notes,[47] it is not always easy for individuals to understand how to manage their privacy.

He considers there are three main reasons for this:

- Consumers can make mistakes as they don't fully understand what might happen if they reveal too much about themselves, due to lack of knowledge about data collection and its uses.
- The life cycle in which personal data operates is now so complex it is impossible for individuals to work out when best to disclose such data and when to keep it to ourselves.
- Even if we were able to access complete information and the cognitive power to process it exhaustively, cognitive biases will typically lead to behaviours that are systematically different from those predicted by rational choice theory.

So consumers are often not in a position to gauge the consequences of disclosing personal information. But further, we don't have stable preferences for privacy given it covers so many different contexts. Is someone getting a glimpse of your naked body on a par with someone knowing what you purchased in the supermarket yesterday? There are so many different elements to calculating the costs of the privacy violation that it's fair to say that our preferences are uncertain. And when our preferences are uncertain, decision making is much more likely to be influenced by factors that are not strictly 'rational', such as the way in which the different options are described, or 'framed'. As such, to better understand our behaviours around privacy and disclosure we need to better understand the psychology of privacy. Some examples of the way in which we can use psychology frameworks to help us understand the mechanisms around privacy are outlined below.

Market versus social norms

As Dan Arialy, a leading behavioural economist puts it, after a meal at your in-laws for Thanksgiving in the US you would not pull your wallet out and ask what payment you could offer for the meal. That's because this is the warm and fuzzy world of *social* relationships where a price is not put on something (unlike in a market relationship). There is a sense of natural trust and no need for immediate reciprocity.

Conversely, when going out to eat at a restaurant, you don't lean back in your chair at the end of the meal, thank the waiter kindly and leave without paying. It is understood that in a market relationship a price has been set which needs to be honoured.

The problem for organisations collecting and handling personal data is that, when leveraging value from it, these social and market norms can collide. For example, people generally understand that there are definite social norms implicit in their relationship with public institutions, which include a shared understanding of civic rights and responsibilities. Most of our public and private institutions rely on the 'good will' of social norms. So not only will the general public feel angry when these are violated but their behaviour may well change in ways which create more trouble and expense in the long run.

One of the challenges facing organisations handling personal data is that when leveraging value from the data that they have collected, these social and market norms can collide. There are certainly social norms implicit in our relationship with our public institutions, with a shared understanding of our civic rights and responsibilities. So, I share all manner of information about myself with my doctor and while I may expect this to be used for the good of others (social norms) I don't necessarily expect it to be sold to insurance companies (market norms). Similarly I may share information about myself that makes it easier for brands to do business with me (social norms) but I may then not expect them to use it for targeted advertising (market norms). So brands need to be mindful of the context in which data will have been shared, as there are implicit assumptions about reasonable use and fairness that underpin the way in which consumers share their data.

Endowment effect

Another lesson from psychology on the effect of data-mediated relationships is the 'endowment effect[48]. This is a phenomenon whereby people tend to place greater value on what they own. Privacy researcher Alessandro Acquisti found just such an effect[49] in relation to personal data. In an experiment he ran, people who started an experiment from positions of greater privacy protection were found to be five times more likely than other people (who did not start with that protection) to forgo money to preserve their privacy. When personal data is discussed in the media or in the government-led public consultation processes around data related issues, it tends to be emphasised that it is 'your data'. Note that the UK government's care.data leaflet emphasises that it is "your health records" and "your information" that is being requested. Emphasising this ownership presses the endowment effect button whereby the public will place greater value on the data and therefore have heightened sensitivity about the way in which it is then used.

Illusion of control

Another study explored the so-called illusion of control. Here, people are likely to disclose much more personal information if they sense that controls are in place. One might of course expect this, but what is less logical is that the presence of controls had a disproportionate impact on the willingness of individuals to disclose data.

Acquisti and colleagues asked in a study[50] whether participants had ever stolen, lied or taken drugs. Then the group was split into three, with each given a different scenario. The first were told that their answers would appear in a research bulletin; the second would be able to give explicit permission about whether to publish those answers, while the third group would be asked for their permission but would also have to give their age, sex and country of birth.

The first group were, not surprisingly, the most reluctant to reveal personal data, while those whose permission was sought were nearly twice as likely to answer all the questions. As for those prompted to give demographic data, every single person volunteered it, even though those details could have allowed a complete stranger a greater chance of identifying the participant. So we seem to overstate the importance of controls in our mind, perversely putting more into the public domain than we would otherwise have done.

So while individuals may well value privacy they struggle to manage the process. And this is a huge dilemma for organisations. If data is collected for one purpose then a strong case can typically be made for using it in a completely different context. But should we be more cautious? We are perhaps in danger of creating an environment where consumers are simply unable to make an informed decision about the way in which their data is collected and managed. And if this is the case then we are in danger of consumers fundamentally losing trust in organisations.

Key points:

— One of the paradoxes of modern life is the way in which we seem to claim we value privacy but then behave as if we don't. A big part of this may be due to the way in which we find it difficult to understand the trade-offs between privacy and disclosure.

— As we struggle to gauge the consequences of disclosing personal information then decision making is much more likely to be influenced by factors that are not strictly 'rational', such as the way in which the different options are described, or 'framed'.

— If individuals feel unable to make decisions concerning privacy then there is potential for trust in institutions becoming undermined.

Teenagers – a sign of things to come?

One of the big questions relating to privacy is whether we are becoming more relaxed about it. Are we more willing for others to have a greater awareness of our inner lives? One of the big discussion areas is that of teenagers. If teens are playing fast and loose with their privacy then, we could argue, surely this indicates more general societal changes? Indeed, Facebook's Mark Zuckerberg has claimed that privacy is no longer a social norm, using it to justify changing the network's privacy settings[51].

Indeed, there is an almost universally-held view that, despite their protestations to the contrary, teenagers simply don't care enough about online privacy. And this apparent attitude can have disastrous consequences[52]. In the UK, for example, Paris Brown famously felt obliged to resign as the country's first Police Youth Crime Commissioner after some ill-advised tweets she had made some years previously. Other cases have tragically involved teens taking their lives after being blackmailed over personal footage posted online. While these are the more extreme examples, many who have contact with teenagers are aware of instances where they have not appeared to have sufficient concern for their privacy .

The reality is that, far from being careless about their privacy, teenagers manage it carefully. They just aren't so obvious about it. Studies among teenagers[53] reveal that the vast majority agree that there are some things they just would not post, and that they would also be wary of putting anything inappropriate online. Of course, self-censorship doesn't always work out and over half of those researched say they sometimes delete things they have posted.

As with previous generations, teens will always make mistakes when experimenting socially. But there are much greater privacy consequences today. The teens surveyed certainly felt the tension between being able to be express themselves spontaneously and freely while simultaneously having to worry about being private (a facet reflected in findings from Pew Research[54] in the US).

Teens also use quite sophisticated means to manage privacy, relying on social coding rather than the more formal means available through, for example, a site's privacy settings. This is often in the form of 'in-jokes', which people will ignore or misunderstand unless they are part of the intended recipient group, or dirtying data, by putting in false personal details.

Another form of coding is 'Vaguebooking', or using an intentionally vague Facebook status such as 'Why would you do this to me?' This is meant to prompt friends to ask what is happening, rather than having to post detailed information upfront. As Danah Boyd, a principal researcher at Microsoft Research, puts it:[55] "The point is to allow access to the content but zero access to the meaning" so that its significance is understood by only a select group of peers.

Another key means that teens use to manage their privacy is to separate their online connections by using different networks. When teens feel they have too many of a particular circle of friends or have family members on some social networks, they divert to other networks to gain some privacy and to feel more able to express themselves freely. So it is an increasingly common route for teenagers, as they get older, to start to find their Facebook presence is over-populated by family and too wide a circle of friends. As a result, they start to migrate to sites which more naturally exclude others such as Twitter or Snapchat.

Boyd has written extensively[56] about how teenagers use 'social stenography' to help manage their privacy online. This is worth reading for those wanting to gain a deeper understanding of the nuances of the issues involved with this demographic group. So privacy does appear to matter to teenagers – it's just that the form of it has changed and the boundaries blurred. Perhaps it gives us a sense of ways in which privacy will manifest itself in future, but certainly does not suggest that privacy is no longer desired.

So we have seen that the idea that privacy is no longer a social norm is not quite the case. Rather, the way in which privacy manifests itself is, necessarily, changing. We often have little choice but to use the online tools available to us. Failure to do so has many downsides – personally, economically and socially. So if we are engaging with our peers by using these online tools, , then we do not necessarily abandon our desire for privacy but simply manage it in different ways.

Key points:

— Teenagers are often held up as an example of changing, more relaxed, attitudes to privacy.

— However, a closer look at their behaviours and attitudes indicates that they are as concerned about privacy ,and will go to some lengths to protect it.

— Our evolving, increasingly technology mediated environment means that the way in which our privacy behaviours manifest will develop and change; it does not mean that our desire for privacy has necessarily changed.

5

Part 5

Institutions and privacy

This section critically examines the way in which institutions can engage with individuals to manage privacy. Three areas are covered:

- Trust frameworks which aim to provide greater simplicity for consumers to navigate privacy terms and conditions
- Transparency which is often considered to be a means of empowering individuals to make better decisions about privacy
- Trading off privacy for enhanced security (by governments)

Trust frameworks

Alan Mitchell, Strategy Director of personal data consultancy Ctrl-Shift, has compared the existing approach to drawing up the terms and conditions that govern the use of personal data to a national rail network that is governed by standards that change every two feet. Brands, Mitchell argues, typically have their own independently drawn-up terms and conditions governing their use of personal data which are unique to their business, but which have no sense of consistency or interconnectedness with those from other brands.

Despite their complexity, consumers are expected to sign up to them before they can make their purchase or use services. Yet very few people actually read them. In fact, a recent poll undertaken among a representative sample of UK consumers found that 40% of consumers agree that they never read any of those they signed up to online. This is despite 85% of those same consumers considering it important to understand what information is held about them.[57]

40%

of consumers agree that they never read any terms and conditions before signing up to online services

This is the conundrum: polls show that consumers want a greater understanding of what they are signing up to. But they don't want to have to become legal experts. One solution might be the emerging concept of 'trust frameworks'. These are sets of commonly agreed rules, tools and infrastructure that enable parties in an ecosystem to do business with each other simply and securely. A standard set of rules and processes will exist for the sharing of information which all parties in the network understand and agree to work to.

The argument is that, if the consumer no longer has to shoulder tasks associated with privacy monitoring, checking, policing and risk taking, they will be more confident when undertaking tasks online that they might not otherwise have engaged in. Similarly, the same benefits accrue to organisations, which can be confident that they can work with each other on the same 'trust framework' basis.

Of course, this will still present challenges. Any organisation can set itself up as a provider of a 'trust framework'. Companies wishing to accelerate growth in new markets will see it as an attractive option, because it quickly establishes a way in which consumers can place faith in brands. However, there is also a credibility issue for a self-appointed 'trust framework' brand appointing themselves as rule makers. Do they, for example, have the resources and effective business model to gain market credibility and sustain this position? Such questions are, however, those that should be asked of any regulatory body.

Ctrl Shift identifies three opportunities for institutions[58] to benefit from 'trust frameworks'. Specifically:

Enhanced efficiency: existing organisational processes can be run more efficiently because there are frameworks in place that govern the way in which information is shared and used.

Rebuilding trust: organisations are encouraged to demonstrate their commitment to responsible data use.

Springboard for innovation: as consumer trust grows, so they might consider sharing other rich data that could complement what brands already hold on them, in exchange for more relevant/enhanced services.

Clearly, benefits exist for consumers who don't need to understand the specifics of each brand's terms and conditions concerning the way in which their data will be used since they will be governed by a set of principles that the company has already agreed to abide by in relation to their personal data. And let's not forget the broader cultural benefits of trust frameworks – embedding a culture of good practice in the industry.

So trust frameworks can be useful – and perhaps they are a necessary condition for any organisation to adhere to. But, the big question is, are they sufficient? And this is the topic of the next section.

Key points:

- It is impossible for people to always read the terms and conditions governing privacy that they need to sign up to in order to use services.
- Trust frameworks are one way in which a common set of rules, tools and infrastructure can be used to simplify the process; if institutions can work to these then people need only assimilate the T&Cs once.
- The question is whether these are sufficient for the management of privacy.

The trend towards transparency

Trust frameworks are, in effect, about providing greater transparency to consumers concerning the way their personal data is managed. Their development has much to do with the broad consensus for 'transparency and control' solutions arrived at by policy makers, industry and privacy advocates. It is manifest, in the US, in both the Federal Trade Commission white paper on consumer privacy[59] and with the White House Consumer Bill of Rights[60]. These promoted transparency and notice being essential to consumer privacy protection.

Digital brands, such as Facebook and Google, have generally backed the approaches by policy makers (although they have also attracted criticism for breaches of privacy). Indeed, Facebook has stated that "...companies should provide a combination of greater transparency and meaningful choice..." for consumers, with Google arguing that making the "collection of personal information transparent" and giving "users meaningful choices to protect their privacy" are two of its guiding privacy principles. Some privacy advocates have also embraced these approaches[61].

Digital brands, such as Facebook and Google, have generally backed the approaches by policy makers (although they have attracted criticism for breaches of privacy).

But does transparency work?

An important paper by psychologists Idris Adjerid, Alessandro Acquisti, Laura Brandimarte and George Loewenstein[62] questioned the value of transparency and the idea that we can effectively place control in the hands of the user. In a series of experiments, they found that the impact of even simple and easily read privacy notices could be manipulated so the consumer unintentionally provides more personal information, rather than less.

The first experiment they conducted looked at the effects of framing the change in privacy protection as increasing or decreasing, even when the absolute risks of disclosure stay the same. Indeed, they found that, if online brands strongly emphasised increases in privacy protection, then consumers would offer more than those in a control condition. Of course, this is common practice in the industry where brands tend to give consumers assurances of constantly improving privacy protection. In addition, the study found that the effect of privacy notices on disclosure reduced over time, so while there may be an initial impact, users quickly settle back into old disclosure habits after a short period.

In their second study, the authors found that the influence of privacy notices on disclosure was reduced by simple 'misdirections'. An example of this is a delay of just 15 seconds between the notice being given and the disclosure decision being required. They argue that the sort of manipulations captured by their experiment mimics the type of obstacles that consumers face when making privacy decisions online in the 'real world'. Examples of this are cited as a time gap between the reading of a notice and the requirement to make a decision. Another common misdirection is when consumers are provided with a detailed notice and the ability to control some dimensions of their privacy preferences (such as the ability for other users to access their personal information), but less detailed and salient notice and ability to control (if any) over the collection and usage of their personal data by the service providers themselves.

The implications of the above research is clear – privacy notices can easily be manipulated so they have little or no effective influence on consumers' disclosure and privacy behaviours. Institutions can clearly (and often do) use this to their favour, often persuading consumers to exhibit ever greater levels of disclosure.

This is not to argue that greater transparency provided by initiatives such as Trust Frameworks are not important. Perhaps we can describe these as necessary – but not sufficient – conditions by which consumers can exercise their judgement.

To this end there surely is a case for communicating more clearly the risks for consumers at the point at which they are called upon to disclosure. But how do we do this? What is the most effective way of raising the awareness of these issues in the minds of individuals and helping them to make the best decision that they can under the circumstances?

Key points:

- It is always tempting to consider that transparency will provide an environment in which individuals are empowered to be able to properly consider information from which they can make an informed decision.
- There is evidence to suggest that even in contexts where a range of information has been presented, individuals can still struggle with decision making.
- Transparency is therefore more of a necessary – rather than sufficient – condition for decision making.
- There is a need for a greater awareness of the way in which data is used, so that individuals can make more considered decisions concerning privacy and disclosure.

Privacy versus security?

Governments have come under strong criticism from privacy campaigners for the way in which they have increasingly allowed ever greater incursions into the private lives of their citizens. The revelations from Edward Snowden concerning the way in which the US NSA and partner agencies in other countries operated, including the UK's GCHQ, has thrown a sharp spotlight onto these practices, creating a huge focus on this activity.

So just what should governments do about privacy? Snowden certainly considers that in the UK government security intrusions into citizens' privacy is 'limitless'; and this is not simply through the activities of institutions such as GCHQ. Other such intrusions include the tracking of people in public places using surveillance technology which is not only CCTV cameras but also body-worn video, drones and number plate recognition systems.

"Everybody is guilty of something or has something to conceal. All one has to do is look hard enough to find what it is."

The justification for privacy intrusion is summed up by a UK government slogan, 'If you've got nothing to hide, you've got nothing to fear.' And this argument is one that is frequently used by politicians, within the media, by members of the public and so on. And in an era where the threat of terrorism certainly feels higher than ever, it seems a very compelling position.

But just how well does this stand up to scrutiny? The leading critic of this argument is Professor Daniel Solove, Professor of Law at the George Washington University Law School. His book, aptly titled 'Nothing to Hide: The False Trade off Between Privacy and Security', presents a critique of this position which is summed up below:[63]

Everybody in fact has something to hide: As Solzhenitsyn pointed out, "Everyone is guilty of something or has something to conceal. All one has to do is look hard enough to find what it is." We all have some regard for our personal privacy as illustrated when Solove invited responses to the 'nothing to hide' argument on his blog. Responses included "So do you have curtains?" and "Can I see your credit card bills for the last year?". He cites Canadian privacy expert David Flaherty who argues "There is no sentient human being in the Western world who has little or no regard for his or her personal privacy; those who attempt such claims cannot withstand even a few minutes questioning about intimate aspects of their lives without capitulating to the intrusiveness of certain subject matters."

Privacy is too complex an issue to reduce to a simple idea. So the notion that we can apply the same principles to such a diverse range of behaviours is not sensible. Solove makes the distinction between surveillance and data processing. Surveillance he considers will involve the collection of information (such as hotels stayed at, cars owned etc) that people wouldn't necessarily be inhibited or embarrassed if others knew that information. The issue, for him, is more to do with the processing of that information – the storage, use and analysis of the data. This, argues Solove, impacts the power relationships between citizens and the state; it creates a sense of powerlessness for the individual and alters the nature of the relationship that people have with the very institutions that make important decisions about their lives.

Privacy is too complex an issue to reduce to a simple idea.

Privacy does not necessarily equate to hiding bad things: Solove points out that a desire for privacy is not always motivated by a desire to hide negative things. We value privacy for a broader range of reasons than simply wanting to keep our negative behaviours hidden (as we saw earlier). There is a danger of confusing this issue when in fact we have very legitimate reasons for valuing privacy.

He outlines a number of the negative aspects that can arise when invasions of privacy occur such as:

- Not having the choice of sharing information – at times you might not mind doing so but you may well feel you should have the choice (e.g. if you had a serious illness or if you were pregnant).
- Government officials having a questionable level of power over citizens – what kind of government do we actually want?
- The lack of accountability in the way in which data is used can mean it is hard for people to assess the dangers of data being in the government's control.
- The data collected can give a distorted picture as they will often fail to reflect the full range of that persons behaviours.

He makes the point that these arguments can struggle to have resonance with the wider public as it can be easy to position the benefits of data collection programmes to outweigh the privacy sacrifice. There is often not sufficient evidence that increased incursions into peoples' privacy is sufficiently harmful for us not to do so. Ann Bartow Professor of Law at the University of South California suggests that privacy's "lack of blood and death, or at least broken bones and buckets of money, distances privacy harms from other [types of harm]."[64] And of course this is particularly pertinent given the nature of the way in which privacy losses incur – they tend to be incremental rather than significant, making it doubly difficult to defend the way in which privacy is lost.

The unpacking of the 'nothing to hide' argument reflects a narrow understanding and set of assumptions of what privacy actually is. The dangers of not properly reflecting on these issues and the way in which they influence peoples' thinking and relationships – both with each other as well as with the institutions of the state – mean that there is a chance that important aspects of peoples' lives are at risk of being eroded without due deliberation.

The balance between our inner and outer lives and the role of the state in determining what is an appropriate balance will always be a contentious issue. However, the debate needs to properly recognise the nature of the impact that incursions on our inner lives can have on the health of our citizens and society.

Key points:

— There is much debate about the degree to which society has a right to privacy versus the safety and well-being of its citizens bought about by state surveillance.

— The rationale for incursion into our privacy is well rehearsed and at times of heightened concern over terrorist activity can be hard to resist.

— However, Danile Solove makes a cogent case for why we should resist the argument that 'If you've got nothing to hide, you've got nothing to fear'.

— The debate about the trade-off between our privacy and security needs to be broadened out, and properly recognise the nature of the impact that incursions on our inner lives can have on the health of our citizens and society.

6

Part 6

Implications and debate

This section aims to:

— Draw together a broad set of implications for brands and government institutions concerning how we can start thinking about privacy in a more nuanced way

— Provide some considerations of the implications of the White paper from a range of practitioners from governments, third sector and brands alike

Implications

Privacy is an issue for individuals as water is to fish. It's hard to see this thing which is all prevalent in our lives, to understand it, to disentangle it from the intricacies of our day-to-day activities. And the concept itself is one that hard to define and evades easily being pinned down. We throw the term around, we ask consumers for the attitudes towards it but as we have seen, it is such a 'catch-all' term and our, often superficial, treatment of it means we are not really doing justice to the debate.

So what should we be doing? There is no doubt that we need to be empowering individuals to have a richer, better informed dialogue about privacy. It is such a complex issue that there are no simple right and wrong answers but there certainly needs to be a stronger counterpoint to the perspective of both government and private sector institutions that benefit from greater disclosure. But further, it is in the interests of those very same institutions that they have a better understanding of privacy and the effects that reductions in privacy can have.

Government institutions have a responsibility to broaden the debate around privacy.

Government institutions have a responsibility to broaden the debate around privacy as the research in this area suggests that reductions in our privacy are not without consequences for the life of our nation. Privacy is integral to the debate over what type of society we want to live in. Commercial organisations should also be part of this debate but also have an imperative that is closer to home. What is the impact of the changing balance between privacy and disclosure on the relationship with the consumer. No-one is suggesting that disclosure is a bad thing but there are signs that more engagement is needed with the issue to determine the longer term commercial implications for brands that don't properly understand where the boundaries of this should be.

There are perhaps a number of points that are relevant for all institutions that have a role in managing privacy.

Avoid simplistic thinking: We like to think that the definition and management of privacy is something that we can leave to the back-office and straightforwardly encapsulate in some terms and conditions. If nothing else, this report has hopefully quashed that assumption. Privacy is an amorphous and complex issue which requires considered thought.

Avoid linear thinking: It's easy to assume that the relationship individuals have with their privacy is a linear one. So for example, the more we reveal about ourselves the better protected we will be or the more relevant services we will be offered and thus we will feel safer or happier. When humans are involved, much of the patterns of behaviour are non-linear and as such we need to explore boundaries. A little disclosure may have welcome benefits in some contexts but then tip over into a negative reaction once past a certain point. Institutions need to understand where these boundaries are and how they vary by context.

Understand the long term implications: The implications of encroaching on privacy and reducing the extent of our inner lives may seem to be theoretical and anodyne. Indeed there are few immediate consequences of doing so that are easily measured; instead, the effects are long term and intangible. But nevertheless we still see these effects – brands suffer from reduced engagement and trust, government can instil a sense of learned helplessness and disengagement amoung their citizens. As ever, the trade-off between short term tangible gain and long term intangible downsides is a hard one to navigate for any institution, but a greater awareness of the issues should help facilitate this.

Understand the value exchange: People are increasingly recognising the value of their personal information and as such are demanding a more open debate about what they will get in return for disclosure of this data. As such institutions need to be prepared for a more robust justification of what is currently on offer, whether this be better services or greater safety.

View privacy as an opportunity rather than a threat: There has arguably been a history of institutions seeing how far they can go to encourage people to disclosure information about themselves – either through active volunteering of that information or through passive data collection. But we are starting to see some organisations making a virtue from respecting your privacy; there is a booming market for products that manage your privacy for you or that set the bar higher in terms of care being taken over information collected about you. Similarly, we are seeing cases where companies face significant commercial set-backs if they do not appear to have taken due care with their customer privacy. Should we be looking more carefully at the way in which a more positive approach to privacy can be used to enhance our quality of life and the success of institutions, rather than seeing it as a threat?

As we highlighted at the outset, this document is not designed to be a comprehensive 'guide' to the issue of privacy or indeed a 'how-to' manual on managing privacy. Instead it is designed to highlight the issues and raise the debate. You may be in full agreement with the issues raised or violently disagree. There may be other nuances you would flag, other areas you would take into consideration. We welcome the debate and ask that you contribute to do it. On the following pages we have some perspectives by those we have already consulted, prompted by reading this document. We encourage you to consider what your perspectives are on this challenging, but hugely important issue. Thank you for being part of this.

Nick Bonney, Head of Insight, Camelot

These changing attitudes and behaviours towards data and privacy are impacting the way that consumers are choosing to interact with brands and accordingly brands need to adapt to survive in this increasingly data-centric world.

The concept of a trust in a brand becomes more important than ever in an environment where consumers are handing over swathes of their personal information – sometimes knowingly - but often simply as a footprint of their previous transactions.

All too often, robust data can end up being the part of the project that's de-scoped in the interests of expediency or budget controls, but brands across all sectors will need to treat data as a fundamental part of the marketing mix moving forward. This isn't just about processes and procedures to capture accurate data, but also about ensuring the consumer sees a fair exchange in revealing data at the heart of the proposition, and that the end to end process is underpinned by a focus on security and architecture. As many brands look to outsource to cloud-based solutions, this landscape becomes even more challenging. Recent high profile breaches (icloud etc) have resulted in a drop in trust here. This creates an interesting paradox – a recent BT survey showed that 76% IT decision makers are anxious about security when using cloud based services but at the same time 79% are adopting cloud based solutions within their business...

We have talked about the concept of the 'uncanny valley' in this report and it's fair to say that many instances of consumer concern around personalisation are where machines are perceived to know too much. There is an undoubted need for the consumer to remain in charge of what data is disclosed and how this is used. Offering consumers the choice of what transactions are identifiable, and offering them suitable incentives to disclose preferences, seem like sensible principles that allow brands to interact directly with those consumers who want to do so on a one-to-one basis. This may result in marketing databases becoming smaller but, if those who remain are more engaged, the commercial metrics (click through, revenue generated etc) may well actually increase in the longer term.

Longer term, we could well see regulatory intervention in this space – while the midata initiative has remained voluntary for now, we may see a push for increased transparency and portability of consumer data in the near future.

Finally, amongst the hype of big data and the promises of data becoming the new oil, the companies who thrive will be those who have a realistic grasp on what data they actually have at their disposal. Either through deliberately trying to cheat the system (through systems such as Tor or Ad Nauseum) or inadvertent behaviours, consumers are often only revealing partial views of their transactional history to brands. Knowing the limitations as well as the power of the data you hold as a brand will become critical to driving insight. We see a fusion of consumer research and behavioural analytics in the future, rather than the battle so many commentators seem keen to predict.

Sue Unerman, Chief Strategy Officer, MediaCom

The MRS paper on privacy is very interesting and gives us planners lots of food for thought.

As I stated in my first book "Tell the Truth, Honesty your most powerful marketing tool" all the metrics of advertising image and recall are irrelevant when the thing that a brand is remembered for most of all is the experience of invading privacy.

Every aspect of a brand needs to be aligned in order for a communications strategy to succeed, and a brand's impact is built up over time. A good brand image is hard to build, and yet it is easily trashed if a misstep in respect for the customer by an over-intrusive exploitation of data occurs.

Equally though, not using data properly might mean that customer expectations aren't met. And for one individual what they want from one brand or category is not the same as it is from another.

Take me, for instance. I'd love my online shopping brand to be able to tell what I have run out of. For my shopping list to automatically update online. At the moment in the Unerman household we have a glut of toilet rolls (yes you can have too many) and no cheese. This is because I can rarely be bothered to properly amend the list and it just rolls on from week to week. So I'd love a bit of invasion of privacy of my kitchen cupboards and fridge.

On the other hand, my bank is too intrusive. My eldest daughter is at uni in Durham, which means that for the last year I've been spending time (and money) in the North East. My bank can't stand it, they stop my payments every time they go through until I have had a conversation with their fraud team. Who don't work weekends. Which is when I am there. Too much use of data – or it's just not intelligent enough, but it makes me feel like they're monitoring my life a bit too closely.

Which brings us to one of the points of privacy really. We'd all quite like a butler – someone or something that makes our lives simpler and easier. That anticipates our needs and can offer us a solution. We don't want a stalker or a brand to behave like a headmaster or an over-intrusive parent – intruding into our lives and making us feel our every move is getting the third degree interrogation treatment. I honestly feel like saying to my bank: "thanks for your concern, but a) you're not my dad and b) who's money is this anyway? And "c) can I refer you back to the last time this happened?"

There's all kinds of ways in which a brand's use of data can help it become closer to the consumer, and to find ways to be helpful. Any changes need to be signposted and people need to accept them and indeed understand them. We're volunteering so much information now all the time it is important for any brand to be sensitive to making use of it in a positive and authentic way, and not to exploit our openness.

Cat Wiles, Board Account Planner, AMV BBDO

‘Private Lives?’ is a thought-provoking white paper that I would urge everyone in the communications industry to read.

We are in the era of big data where competitive advantage is gained from knowing our consumers better than anyone else. We know more about our audience than ever before and we are hungry to learn more. However, in our quest for more knowledge, how often do we stop to pause, take a step back and think about how this could impact on an individual’s sense of privacy?

This is more fundamental than just making sure the data is secure – it’s about respecting the consumer and what they want would want us to do with their data.

As ‘Private Lives?’ asserts, consumers have a complicated relationship with privacy – on one hand consumers expect us to mine their data with analytics to provide them with relevant offers and products to improve and enhance their shopping experience, yet on the other hand they want to keep some things private and away from prying eyes.

It is imperative that we strike the right balance between privacy and personalisation. Get it right and trust in the brand is built. Get it wrong and the bond of trust will be broken.

There is not a one-sized-fits-all approach to privacy, as the relationship someone wants with a brand will differ dependent on the category, the moment and any pre-existing level of trust with the brand concerned.

For example, consumers will have different attitudes towards their privacy relationship with brands like FitBit that they have opted to invite into their lives to help them live a more active, healthy life. They are open to suggestions from the brand because there is a clear and transparent value exchange and that builds trust. Consider this in contrast to the relationship consumers have with their bank who they expect to be secure but would not expect or indeed want to receive feedback on their spending.

As an industry we need to ensure that we continue to respect our consumers and build trust by acting in their best interests. We must use data to create tangible consumer benefits which make their lives better. If we do this we can hold our heads high.

Rachel Glasser, Partner, Director of Digital Privacy, GroupM North America

Consumers need to know what data privacy means in the context of online marketing, what type of data are collected and the value exchange for sharing data with marketers. Communication must be clear and transparent about what data is collected and how it will be used. Furthermore, Marketers need to provide consumers with the choice of whether they want to share their data. And if consumers entrust their data to marketers, they must have the assurances that the data will be stored securely and used responsibly.

Data collected for behavioral marketing is anonymous and in the main, benign. It is not personally identifiable. In fact online marketers shy away from collecting personal data, because it is perceived to be intrusive by consumers. The aim of behavioral targeting is to find people who may be interested in a product and serving a relevant ad to them at the right time – and at scale. There is no need to identify an individual – marketers need to find thousands of people who are interested in their product.

There is a clear value exchange: The idea is that by a consumer sharing their data they are, in exchange, afforded many benefits. Amongst these benefits is the access to millions of pieces of content – essentially a free Internet which is supported by advertising. Advertising provides funding for smaller independent sites to function and deliver unique content to a vast user base. It funds community based websites where users can share information with one another, and even contribute to group discussions or find support groups. Advertising based on data collected and shared online supports free resources available on the web that help foster education and learning.

Benign data or not, consumers should be offered a choice of whether they want to share their data with marketers. Self-regulatory programs such as the United States' AdChoices program include serving a globally recognizable symbol, which informs users that data is being collected and gives them the choice to opt out of data collection. In other regions of the world there are directives, which require user choice prior to cookie placement for collection of data. Initiatives like these that offer transparency and choice help foster trust.

But the greatest opportunity Brands and marketers have to build trust with their consumer is through a simply worded privacy statement, where users should be educated and informed about data collection, why it is necessary, how it is used and with the full assurance that it will be stored safely.

It is only then that Marketers will begin to earn consumer's trust and then consumers will be more willing to share data with marketers contributing to efficient practices and the free web.

Respect privacy. And the consumer.

Jane Frost CBE, Chief Executive, Market Research Society

There was no debate when the MRS Delphi Group decided to cover the topic of privacy; the issue has engulfed not just this industry, but every institution and organisation regardless of sector. Formulating a response to privacy is a matter of urgency that no company, large or small, can resist, in order to continue to operate successfully, or to operate at all.

But as we have seen in this report, 'privacy' is a convenient catch all for a wide spectrum of personal anxieties, cultural values, commercial considerations and national priorities.

In a relatively short period of time – just a few years – operational issues such as security and consent that used to slink around the back office domains of the IT or legal department have fused together with people's deeper ethical concerns, to form a newly minted currency. The coin has two sides: on one is privacy, introspective and protective; on the other is trust, that emotional connection that compounds our relationships with people and things. This currency encapsulates the new power of the consumer, and as such is the stuff of both dreams and nightmares for CMOs and CEOs.

Today's market research industry was born from the earliest explorations of social research – amplifying the voices of the powerless, holding governments to account, helping us all to live fuller and richer lives. The social, philosophical and ethical issues explored in this report demonstrate that this sector isn't just about helping governments and businesses to better understand their relationship with citizens and customers. At its core, our industry is about better understanding what it is to be human, our external and internal lives.

The work of our sector helps forge trust between professionals and people, marketers and consumers, CEOs and stakeholders, political parties and voters. We also have our own domestic privacy concern – that of preserving trust between us and our respondents. And yet, by ignoring to formulate a response to the issues explored in this report we all put this relationship at risk every day.

The MRS Fair Data initiative was launched two years ago, and to date has 60 partners. Take-up is accelerating as this new sense of urgency permeates the organisation from the back office through to the boardroom.

It's no longer just the cost of security breaches, but the consumer backlash that is driving organisations to take privacy seriously. The smart ones are also seeing privacy as an opportunity to differentiate themselves, rather than simply as a threat to be handled by particular department. With many economies only just showing growth after years of recession, this new privacy/trust currency looks set to gain in value exponentially over the coming years.

Data standards and trust marks

There is a multiplicity of data standards which function well as B2B quality standards. These include BS ISO 20252 and BS ISO 26362, as well as the US-EU Safe Harbour agreement.

MRS, DMA and several other associations all have Codes to which their members should be adhering.

However, none of these are in a format which the consumer can readily understand. The complexity and detail of these quality frameworks resemble Ts&Cs in opacity and length.

The research sector launched Fair Data as an answer to this challenge – designed as it is to help the public easily identify companies and organisations that can be trusted with personal data.

As a recognisable trust mark, Fair Data also provides an external reminder to all parts of the organisation that has signed up to it that handling personal data demands an ethical, responsible approach from everyone involved, at all levels within the supply chain.

MRS Code of Conduct
mrs.org.uk/code

Fair Data
fairdata.org.uk

Fair Data™

About Market Research Society (MRS)

MRS is the world's leading authority for the research, insight, marketing science and data analytics sectors. With over 5,000 members and 500 company partners in 60 countries, MRS serves all those with professional equity in provision or use of market, social and opinion research, and in business intelligence, market analysis, customer insight and consultancy.

Market Research Society
The Old Trading House,
15 Northburgh Street,
London EC1V 0JR
Tel: +44 (0)20 7490 4911
mrs.org.uk

References

References

1 Lepore, Jill (2013) The Prism: Privacy in an age of publicity, *New Yorker*, June 24 [online] http://www.newyorker.com/magazine/2013/06/24/the-prism

2 Westin, Alan (1984) The origin of modern claims to privacy. Appears in *Philosophical Dimensions of Privacy: An Anthology*, edited by Schoeman, Ferdinand. Cambridge University Press

3 The long march to privacy, *The Economist*, Jan 12th 2006 [online] http://www.economist.com/node/5389362

4 Thomson, Judith Jarvis (1975) The right to privacy, *Philosophy and Public Affairs*, Vol. 4, No. 4. (Summer, 1975), pp. 295-314

5 Solove, Daniel (2002) Conceptualising privacy *California Law Review*, Vol. 90, p. 1087

6 Wittenstein, Ludovic (1999) Philosophical Investigations. Prentice Hall

7 Luft, J.; Ingham, H.,The Johari window, a graphic model of interpersonal awareness, *Proceedings of the western training laboratory in group development* , UCLA, 1955.

8 Sennett, Richard (1977) *The fall of Public Man*. New York: Knopf

9 Lasch, Christoper (1991) *The True and Only Heaven: Progress and Its Critics*. W. W. Norton & Company

10 Warren, Samuel and Brandeis, Louis (1890) The right to privacy *Harvard law Review* Vol. IV December 15, No. 5

11 Bentham, Jeremy (1843) Of Publicity, Appears in *The Works of Jeremy Bentham*, published under the Superintendence of his Executor, John Bowring

12 Inside the Mind of Google, 2009, *CNBC documentary* December 3

13 Privacy no longer a social norm, says Facebook founder, *The Guardian* (2010) [online] http://www.theguardian.com/technology/2010/jan/11/facebook-privacy

14 Cukier, Kenneth; Mayer-Schonberger, Viktor (2013). *Big Data: A Revolution That Will Transform How We Live, Work and Think*. John Murray.

15 Tesco petrol stations use face-scan tech to target ads (2013) [online] http://www.bbc.co.uk/news/technology-24803378

16 Ferguson, Donna (2013) "How supermarkets get your data—and what they do with it", The Guardian June 8 [online] http://www.theguardian.com/money/2013/jun/08/supermarkets-get-your-data

17 Tanner, Adam (2013) The web cookie is dying. Here's the creepier technology that comes next, *Forbes*, June 17 [online] http://www.forbes.com/fdc/welcome_mjx.shtml

18 Ungerleider, Neal (2013) Mobile phones have fingerprints, too, *Fast Company*, 2 March 29 [online] http://www.fastcompany.com/3007645/location-location-location/mobile-phones-have-fingerprints-too

19 de Montjoye, Yves-Alexandre, Hidalgo César A., Verleysen, Michel & Blondel Vincent D. (2012) Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports* 3, Article number: 1376 [online] http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html

20 Digital records could expose intimate details and personality traits of millions university of Cambridge 11 March 2013[online] http://www.cam.ac.uk/research/news/digital-records-could-expose-intimate-details-and-personality-traits-of-millions

21 Noble, June, and William Noble (1980) The Private Me. New York: Delacorte Press

Read more: Privacy – The Psychological Functions And Philosophical Values Of Privacy – Press, University, York, and Cambridge – JRank Articles http://science.jrank.org/pages/10854/Privacy-Psychological-Functions-Philosophical-Values-Privacy.html#ixzz3OcMbtb8n

22 Inness, Julie C. (1992) Privacy, Intimacy, and Isolation. New York: Oxford University Press

Read more: Privacy – The Psychological Functions And Philosophical Values Of Privacy – Press, University, York, and Cambridge – JRank Articles http://science.jrank.org/pages/10854/Privacy-Psychological-Functions-Philosophical-Values-Privacy.html#ixzz3OcMm5cwK

23 Schwartz, Barry (1968) The social psychology of privacy American Journal of Sociology Vol. 73, No 6, pp. 741-752

24 Eubanks, Virginia (2014) Want to Predict the Future of Surveillance? Ask Poor Communities Forbes, January 15 [online] http://prospect.org/article/want-predict-future-surveillance-ask-poor-communities

25 Has Privacy Become a Luxury Good? (2014) Julia Angwin *The New York Times* March 3 [online] http://www.nytimes.com/2014/03/04/opinion/has-privacy-become-a-luxury-good.html?_r=1

26 Blackphone offers a mostly secure Android-based smartphone for $629 *Engadget* February 24th 2014 [online] http://www.engadget.com/2014/02/24/blackphone-privacy-phone/

27 An $85 hack that could hide your smartphone from prying eyes *Fast Company* August 7, 2013 [online] http://www.fastcompany.com/3015354/an-85-hack-that-could-hide-your-smartphone-from-prying-eyes

28 The price of reputation, *The Economist* Feb 21st 2013 [online] http://www.economist.com/news/business/21572240-market-protected-personal-information-about-take-price-reputation?fsrc=rss%7Cbus

29 Strong, Colin, "What is the Future for online advertising" *Huffington Post*. November 2013. http://www.huffingtonpost.co.uk/colin-strong/online-advertising_b_4269606.html

30 Lynch, Michael (2013) Privacy and the threat to the self, *The New York Times* June 22 [online] http://opinionator.blogs.nytimes.com/2013/06/22/privacy-and-the-threat-to-the-self/?_r=0

31 Arendt, Hannah (1958) *The Human Condition*. Chicago: University of Chicago Press

Read more: Privacy – The Psychological Functions And Philosophical Values Of Privacy – Press, University, York, and Cambridge - JRank Articles http://science.jrank.org/pages/10854/Privacy-Psychological-Functions-Philosophical-Values-Privacy.html#ixzz3OcPZgVJW

32 Schneider, Carl D. (1977) *Shame, Exposure, and Privacy*. Boston: Beacon

Read more: Privacy – The Psychological Functions And Philosophical Values Of Privacy – Press, University, York, and Cambridge - JRank Articles http://science.jrank.org/pages/10854/Privacy-Psychological-Functions-Philosophical-Values-Privacy.html#ixzz3OcQ22gsh

33 Noble, June, and William Noble (1980) *The Private Me*. New York: Delacorte Press

Read more: Privacy – The Psychological Functions And Philosophical Values Of Privacy - Press, University, York, and Cambridge - JRank Articles http://science.jrank.org/pages/10854/Privacy-Psychological-Functions-Philosophical-Values-Privacy.html#ixzz3OcQB2U6M

34 Pfaff, S. (1996) *Collective Identity and Informal Groups in Revolutionary Mobilization: East Germany in 1989*. Social Forces, 75(1), 91–117

35 Funder, A. (2003) *Stasiland*. Granta Books: London

36 Brown, Ian (2013) *Future Identities: Changing identities in the UK – the next 10 years*. Oxford Internet Institute [online] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/275755/13-507-surveillance-and-privacy-technologies-impact-on-identity.pdf

37 Joinson, A.N. and Paine, C.B. (2007) *Self-disclosure, privacy and the Internet*. In Joinson, A., McKenna, K, Postmes, T and Reips, U.-D. (eds.) The Oxford Handbook of Applied Psychology, Oxford University Press: Oxford, 237–252

38 boyd, danah (2013) how "context collapse" was coined: my recollection December 8 [online] http://www.zephoria.org/thoughts/archives/2013/12/08/coining-context-collapse.html

39 Much of the material for this section was sourced from McDougall, Bonnie, Privacy – The Psychological Functions And Philosophical Values Of Privacy [online] http://science.jrank.org/pages/10854/Privacy-Psychological-Functions-Philosophical-Values-Privacy.html

40 For more on 'dataveillance' see Roger Clarke's Dataveillance and Information Privacy Home-Page [online] http://www.rogerclarke.com/DV/

41 Strong, Colin (2014) *The Human Side of Big Data: Exploring the way Data Shapes Consumer-Brand Relationships* Appears in Digital Enlightenment Yearbook 2014, IOS Press

42 For more about the uncanncy valleu see here [online] http://www.movingimages.info/digitalmedia/wp-content/uploads/2010/06/MorUnc.pdf

43 Did The "Uncanny Valley" Kill Disney's CGI Company? *Fast Company* March 31, 2011 [online] http://www.fastcodesign.com/1663530/did-the-uncanny-valley-kill-disneys-cgi-company

44 Cukier, Kenneth; Mayer-Schonberger, Viktor, *Big Data: A Revolution That Will Transform How We Live, Work and Think*, John Murray, 2013.

45 Fournier, Susan, 'Consumers and Their Brands: Developing Relationship Theory in Consumer Research', *Journal of Consumer Research*, Vol. 24, No. 4, pp. 343–353, March 1998.

46 Aaker, J., Fournier, S., Brasel, A., 'When Good Brands Do Bad', *Journal of Consumer Research*, 1–16, 31 June 2004.

47 Acquisti, Alessandro and Grossklags, Jens, *'What can Behavioural Economics teach us about privacy?'*, draft preliminary version, presented as Keynote Paper at ETRICS 2006, http://www.heinz.cmu.edu/~acquisti/papers/Acquisti-Grossklags-Chapter-Etrics.pdf

48 For more information on the endowment effect see Kahneman, Daniel (2012) Thinking fast and slow, Penguin

49 Sengupta, Somini, "Letting our guard down over web privacy" *New York Times*, 31 March 2013 http://www.nytimes.com/2013/03/31/technology/web-privacy-and-how-consumers-let-down-their-guard.html?pagewanted=all&_r=0

50 Brandimarte, Laura, Acquisti, Alessandro and Lowenstein, George, 'Misplaced Confidences, Privacy and the Control Paradox', *Social Psychological and Personality Science*, vol. 4 no. 3, 340–347, May 2013.

51 Zuckerberg, Mark, 'Facebook's Zuckerberg Says Privacy No Longer A 'Social Norm'', *Huffington Post*, 18 March 2010. http://www.huffingtonpost.com/2010/01/11/facebooks-zuckerberg-the_n_417969.html

52 Strong, Colin, 'Five things you may not know about teenagers and privacy', *Huffington Post*, 21st August 2013. http://www.huffingtonpost.co.uk/colin-strong/five-things-you-may-not-know-about-teenagers-and-privacy_b_3785248.html

53 Strong, Colin (2013) Five Things You May Not Know About Teenagers and Privacy *Huffington Post* August 21 [online] http://www.huffingtonpost.co.uk/colin-strong/five-things-you-may-not-know-about-teenagers-and-privacy_b_3785248.html

54 Madden, Mary; Lenhart, Amanda; Cortesi, Sandra; Gasser, Urs; Duggan, Mary; Smith, Aaron and Beaton, Meredith, *'Teens, Social Media and Privacy'*, Pew Research Centre, 2013. http://www.pewinternet.org/Reports/2013/Teens-Social-Media-And-Privacy.aspx

55 Henley, Jon, Are teenagers really careless about online privacy? *The Guardian*, 21 October 2013, http://www.theguardian.com/technology/2013/oct/21/teenagers-careless-about-online-privacy

56 Boyd, Dana and Marwick, Alice, *'Social Steganography: Privacy in 'Networked' Publics'*. Paper presented at ICA on May 28, 2011 in Boston, MA.

57 Strong, Colin (2013) Are consumers finally getting interested in terms and Conditions? *Huffington Post* 10 May [online] http://www.huffingtonpost.co.uk/colin-strong/are-consumers-interested-terms-and-conditions_b_3242411.html

58 Ctrl Shift, (2014) Trust Frameworks: Driving privacy and growth, Published by Ctrl Shift, 31 January. https://www.ctrl-shift.co.uk/research/product/86

59 Federal Trade Commission, 'Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for businesses and policy makers', March 2012. http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

60 The White House, 'Consumer Data Privacy in Networked World', 2012. http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

61 Reitman, R., 'FTC Final Privacy Report Draws a Map to Meaningful Privacy Protection in the Online World', 2012. https://www.eff.org/deeplinks/2012/03/ftc-final-privacy-report-draws-map-meaningful-privacy-protection-online-world

62 Idris Adjerid, Alessandro Acquisti, Laura Brandimarte, George Loewenstein (2013) *Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency*. Published in SOUPS '13 Proceedings of the Ninth Symposium on Usable Privacy and Security Article No. 9

63 Solove, Daniel (2013) *Nothing to Hide: The False Tradeoff Between Privacy and Security*. Yale University Press

64 Bartow. Anne (2006) *A Feeling of Unease About Privacy Law* University of Pennsylvania Law Review 154