TRUST IN THE DIGITAL AGE

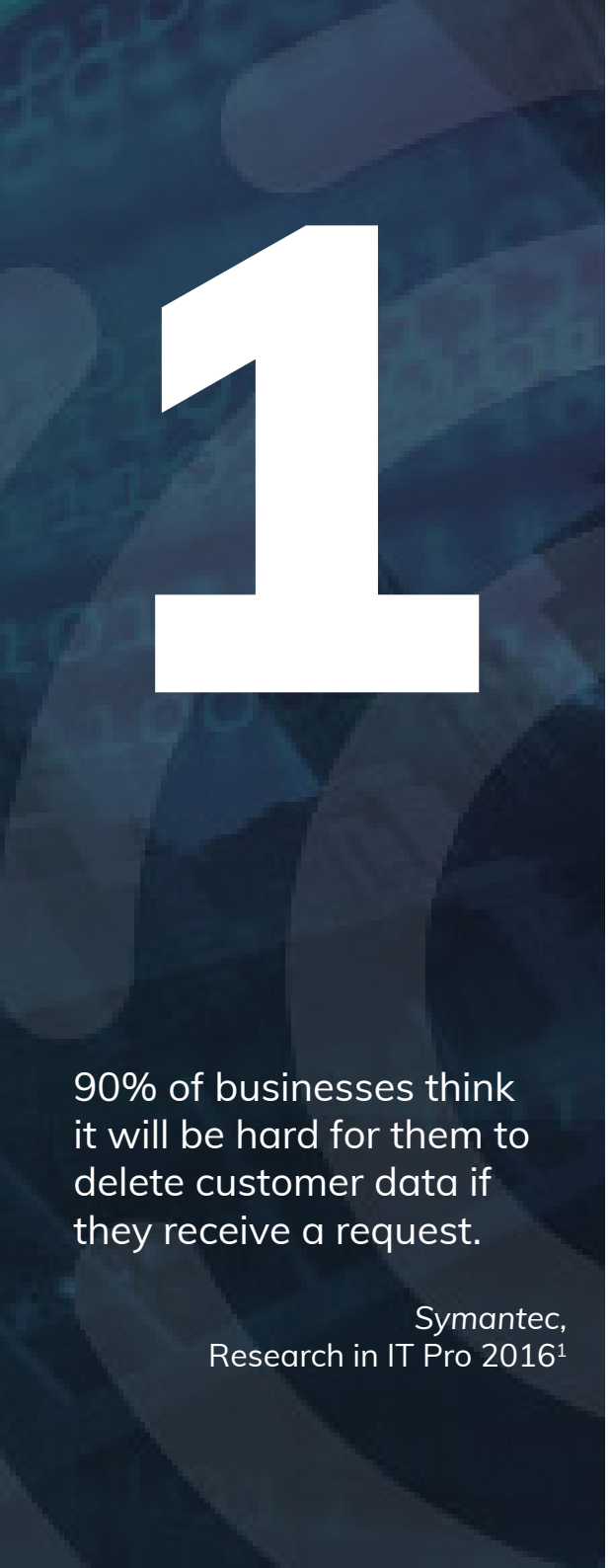
Rethinking personal data to deliver change

A MyLife Digital white paper

 www.mylifedigital.co.uk | www.consentric.io

mylife digital

CONTENTS



90% of businesses think it will be hard for them to delete customer data if they receive a request.

Symantec,
Research in IT Pro 2016[1]

INTRODUCTION AND EXECUTIVE SUMMARY

In this increasingly digital world, do individuals understand the amount and worth of the data they generate? Are organisations transparent about how they use and store this personal data? Have the disreputable practices of some organisations damaged consumer trust beyond repair?

Data has significant value to any organisation. Hidden within data are important insights leading to competitive advantages. The amount of personal data organisations collect and store is increasing. Machine learning capabilities enable huge quantities of data to be processed in seconds. Leading to insightful strategy and planning opportunities.

In the midst of this desire for insight, organisations have overlooked the most important aspect. This data belongs to the individual. Their personal data is being analysed - preferences, purchases, donation history, sports performance and in some cases, even sensitive matters such as their health.

It's time organisations took a new approach. They need to combat the growing sense of resistance and mistrust. They need to protect personal data against misappropriation and misuse. Individuals are, quite rightly, frustrated that their relationship with organisations has been one way. That they have given their information, but had no control over it.

The imbalance has been recognised. New legislation is coming into effect. The General Data Protection Regulation (GDPR) stipulates that clear, unambiguous indication of consent will largely need to be given for the collection, storage and use of personal data.

This is also reflected in the UK Data Protection Bill 2017, which is based on GDPR. The individual will have the right to know exactly what data is stored, who has access to it and what is being done with it. They can remove their permissions and will have the right to erasure.

Companies must take the lead in bringing business and society back together. The recognition is there among sophisticated business and thought leaders, and promising elements of a new model are emerging.

How to Fix Capitalism Harvard Business Review,
Michael Porter & Mark Kramer 2011[2]

Quite rightly, technology is evolving to meet society's demand for greater transparency. Privacy and security need to be kept at the forefront of system design to ensure the protection of personal data. This will lead to the strengthening of trust through a new value exchange between organisations and individuals. Building new empowered relationships to increase loyalty and deliver benefits to both parties and society as a whole.

This white paper discusses four key points organisations must address to ensure they maintain their market share and strengthen engagement with the individuals whose data they hold:

TRUST **TRANSPARENCY** **PRIVACY** **SECURITY**

We have brought together some principal research in these areas. Research that led to the development of MyLife Digital's Consentric Platform, which places the citizen's trust at the heart of your data protection and GDPR strategy.

John Hall
Chief Executive Officer, MyLife Digital

2

Perceived violation of privacy: 67% of organisations, companies and agencies ask for too much personal information online.

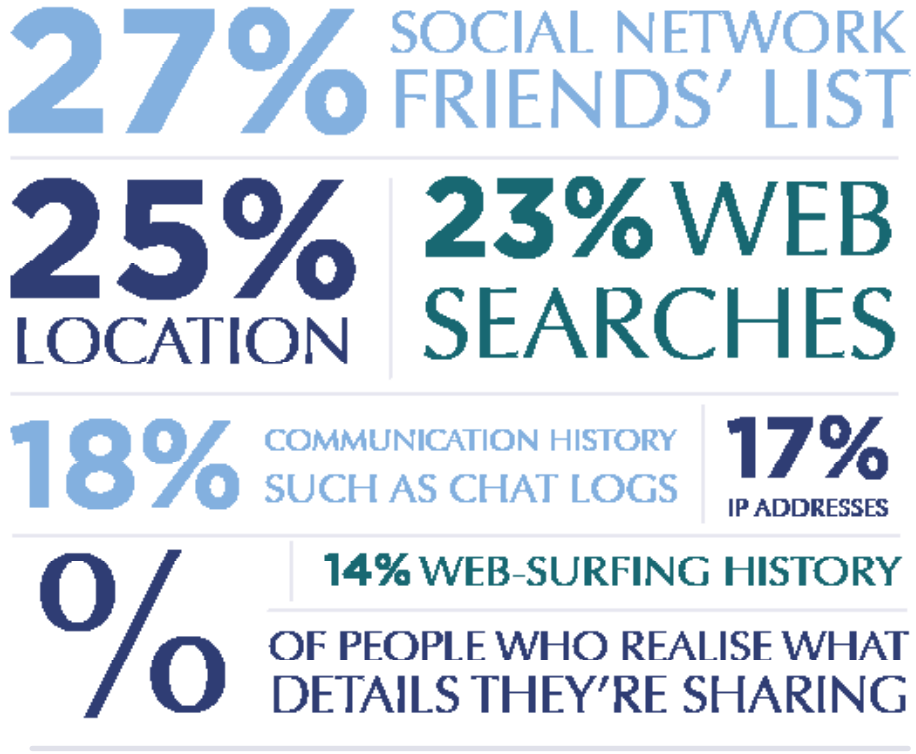
Rethinking Personal Data: A New Lens for Strengthening Trust, WEF[3]

TRUST — EARN IT

It is easy to understand why individuals find it hard to trust organisations with their personal data. They are inundated with nuisance cold calls. They are constantly approached by unknown and unrequited organisations. Plus, they are asked for excessive information when they subscribe, donate or purchase online, and more frequently in person. Each engagement presents confusing opt-in or opt-out choices along with lengthy terms and conditions – which usually go unread. Which lead to this well reported decline in trust.

Contradicting this entirely, when people post on social media platforms they freely share vast quantities of information daily. They exchange this readily, often without realising that their online activities are tracked along with more covert monitoring such as location and contact lists.

The introduction of new, smart connected products and services and the IoT means that more detailed information about individuals, and their lives, is collected constantly.



Customer Data: Designing for Transparency and Trust
Timothy Morey, Theodore Forbath, Allison Schoop, May 2015[4]

“I had concerns that consumers weren’t being properly protected, and it’s fair to say the enquiries my team have made haven’t changed that view. I don’t think users have been given enough information about what Facebook plans to do with their information, and I don’t think WhatsApp has got valid consent from users to share the information. I also believe users should be given ongoing control over how their information is used, not just a 30 day window.”

Elizabeth Denham
UK Information Commissioner

Recognising that the treatment and relationship with employees and customers alike is integral to building trust, business should adopt an “inside out” approach, which begins with listening.

Edelman Trust Barometer 2017[5]

So, what caused this decline in trust and how does it impact organisations? Lack of transparency is one of the main causes. News headlines frequently contains examples of organisations that have used, shared or exchanged personal data contravening existing regulations. These practices have led to significant fines from the ICO[6].

The sharing of information between WhatsApp and Facebook[7] caused an enormous public outcry with the regulator having to step in to prevent data sharing between the two organisations.

2.1 WHY REBUILDING TRUST IS IMPORTANT

Imagine if every individual refused to let an organisation use their personal data. If they decided that they didn't want to engage with any charities, organisations, public bodies or other organisations, and withdrew all permissions for this purpose.

While it is unlikely that the above scenario would happen now, individuals are demonstrating an increased scepticism about the use, and sometimes misuse, of their data. They recognise that their personal information is valuable, and are becoming more selective about where they share it and for what purpose.

For an organisation, this could prove to be their downfall. An organisation without a database of prospects and existing customers – or at least a legitimate reason to contact them, would soon lose marketing advantage to their competitors and, ultimately, the bottom line would suffer.

In the UK, trust is now the second most important reason for choosing a retailer, after price. As the world gets more unsettled, trust and familiarity become more important. It takes years to build, and yet one bad day on social media can obliterate it altogether.

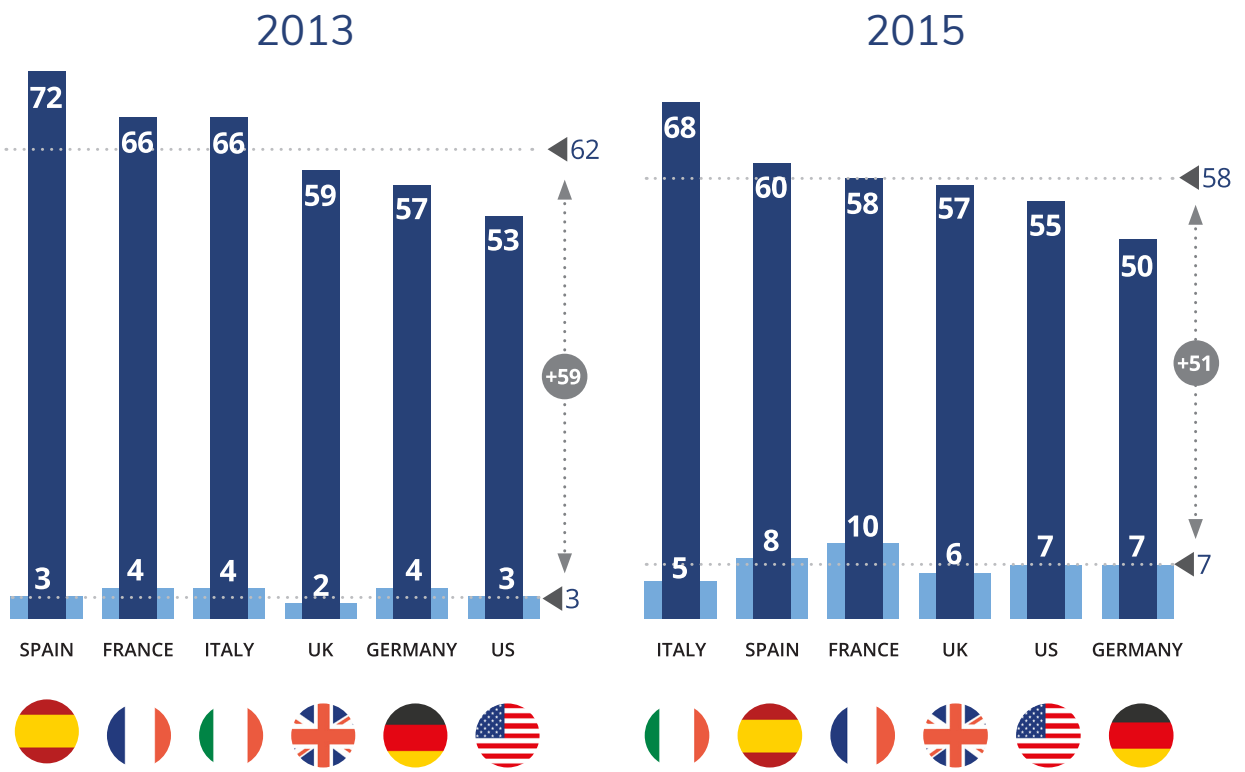
PwC: Total Retail 2017[8]

A firm that is considered untrustworthy will find it difficult or impossible to collect certain types of data, regardless of the value offered in exchange. Highly trusted firms, on the other hand, may be able to collect it simply by asking, because customers are satisfied with past benefits received and confident the company will guard their data.

Customer Data: Designing for Transparency and Trust.
Harvard Business Review, May 2015[9]

Trust can unlock data disclosure. Organisations must take the lead in bringing business and society back together.

Generating trust increases access to data by at least five times.



Percentage of consumers who would be willing to allow companies to use data about them.

Companies with consumer trust

Companies without consumer trust

BCG Global Consumer Sentiment Survey 2013 and Big Data and Trust Consumer Survey 2015[10]

2.2 DRIVERS FOR CHANGE

People are more aware of their digital rights. Organisations need to remember that people are their lifeblood. Addressing their scepticism and realigning relationships to strengthen trust should be a primary driver.

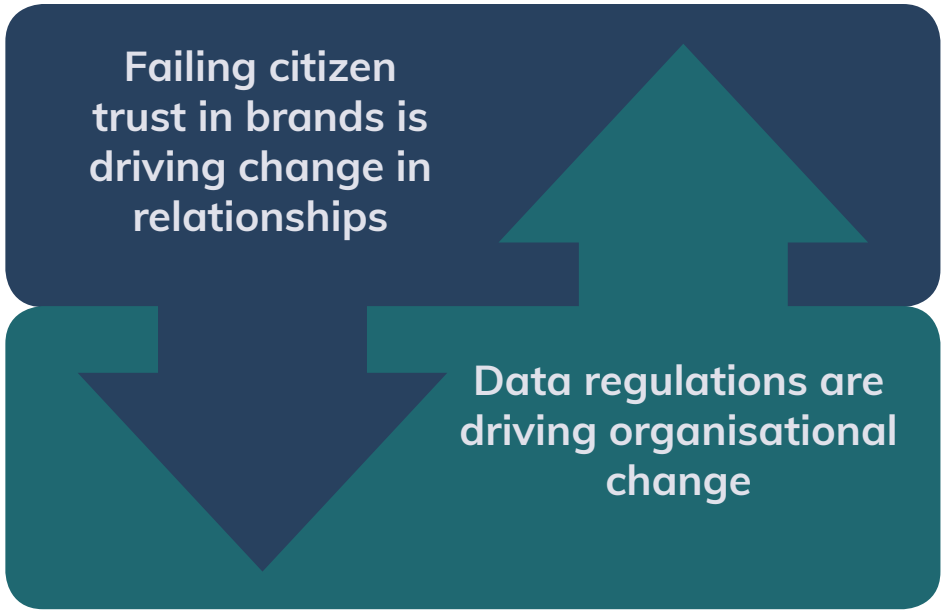
There are many documented reports supporting the individuals' rights to privacy, trust and protection.

The preferred outcome should be that individuals have a true digital understanding of how organisations process their personal data.

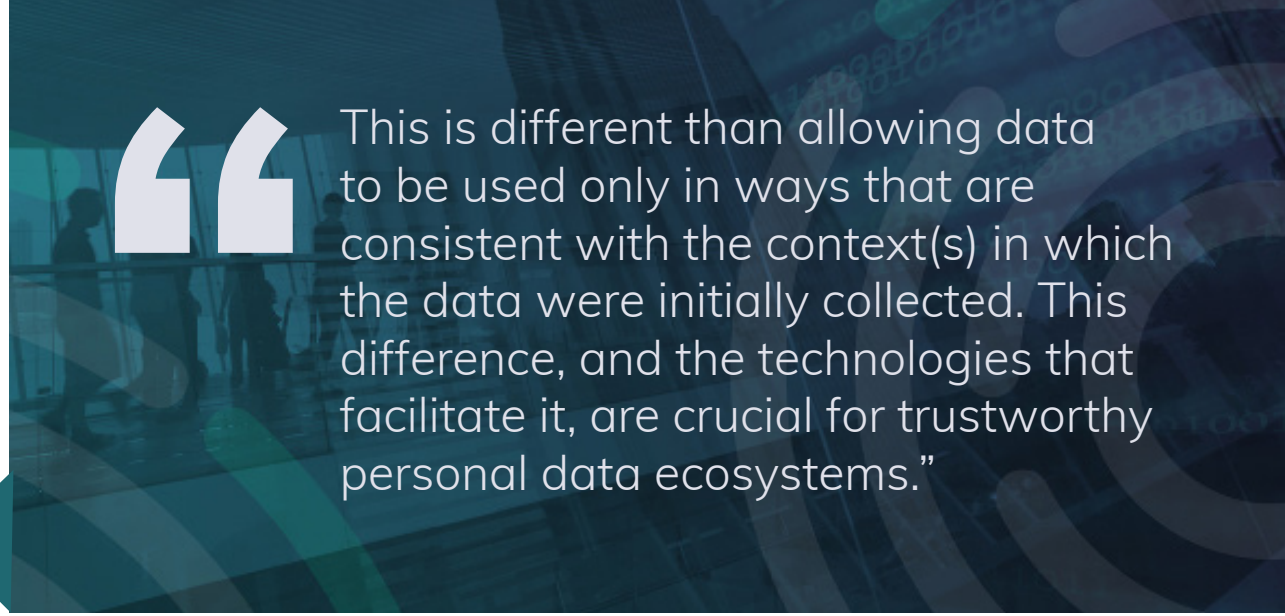
An information differential exists between institutions and individuals, creating a crisis of trust that results from uses of data being inconsistent with user expectations and preferences.

The Caldicott Report in the health sector[11]
to the World Economic Forum[12]

Two forces are coalescing to drive change:



The WEF Rethinking Personal Data report also states:



Another seminal paper, from The Boston Consulting Group (BCG) entitled The Value of Our Digital Identity[13], advises that "in an increasingly digital society, personal data has become a new form of currency. The biggest challenge for political and business leaders is to establish the trust that enables that currency to keep flowing." They describe the Digital Identity as the sum of all available information about an individual which is held digitally.

This Digital Identity is more complete and traceable than ever before. The exponential growth in available data and big data capabilities to process and analyse it drives organisations to better understand the needs and wants of their market. Individuals are worried about losing both their privacy and control over their personal data. Organisations, on the other hand, fear compromising their position as trusted provider.

Alongside any commercial drivers, there are also regulatory factors and compliance to consider. Currently organisations have industry regulators, ombudsmen and the Data Protection Act (DPA) to conform to. But, from 25th May 2018, the new EU General Data Protection Regulation (GDPR) will become enforceable, overriding the DPA and adding levels of complexity to the everyday gathering of individuals' personal data. The UK will also have the Data Protection Bill 2017 to adhere to.

There is increased scrutiny from regulatory bodies, such as the Information Commissioners Office (ICO). In December 2016 the RSPCA and British Heart Foundation were fined for not following best practice and eleven other charities had notice of intent to fine imposed against them in January 2017.

The ICO cited that the charities were not transparent enough with their supporters regarding the use of additional profiling and data sharing.

Now is the time for organisations to ensure they're ready for GDPR compliance before May 2018.

Start as they mean to go on and trust will be regained.

2.3 GDPR AND WHAT IT MEANS

As part of the GDPR, organisations need to answer these questions from individuals concerning the transparency of their personal data:

- What data has been collected?
- Who is using my data? *(Recipients of all personal data)*
- How safe is my data?
- Why has my data been collected? *(The lawful reason for processing their data)*
- When and where was permission granted?
- Where is my data? *(Intention to transfer personal data to other country or organisation)*

90% of businesses think it will be hard for them to delete customer data if they receive a request.

Symantec Research in IT Pro, 2016[14]

The "right to be forgotten" has a small but consistently positive impact on the willingness to share, increasing it by 10% to 18%.

The Value of Our Digital Identity, *Boston Consulting Group*[13]

Additional information also includes:

- Identity and contact details of the Data Controller
- Contact details of the Data Protection Officer (DPO) where applicable
- How long will personal data be stored?
- The right to request rectification, erasure or restriction of processing personal data

In terms of the last point, it is worthwhile to note that some data might need to be kept, for example transactional data. In addition, an organisation should keep details of who has been erased so they are not inadvertently contacted again in the future. While the regulation recognises that this may be complex and involved for organisations, if systems and processes are in place to fulfil this right, there are positive impacts on the individuals' reaction to the organisation.

2.4 PRIVACY BY DESIGN

With all the current news about data breaches, ‘Privacy by Design’ is a hot topic.

This basically means having an approach that promotes privacy, security and data protection in system design.

“Unfortunately, these issues are often bolted on as an after-thought or ignored altogether,” says the ICO[15].

The ICO encourages this approach in the early stages of any project.

For example when:

- building new IT systems for storing or accessing personal data
- developing legislation, policy or strategies that have privacy implications
- embarking on a data sharing initiative
- using data for new purposes

3

TRANSPARENCY — SEE IT

Organisations have been realising the benefit from insights into personal data for many years. Now individuals are demanding equal visibility into organisations. And that visibility includes transparency about what information the organisation holds on them, how it's used and where it's shared.

Until now, organisations have built their systems to suit their own internal infrastructure and processes - not to address the needs of the individual.

Today's dissent is that organisations need to process data but individuals demand transparency and a way to control, view and edit their personal data, update their permissions or erase their record completely.

The current approach to transparency has been focused on disclosure of information, which is often a difficult process and overwhelms the individual with details.

The new perspective is for organisations to focus on generating ongoing engagement. It's about providing individuals with insight and empowering them to manage their personal data.

The future relationship between organisations and individuals starts with transparency and results in trust.

There are three key things organisations need to deliver to achieve transparency:

- Alignment of systems and processes around the individual and their data rights
- Integration of front and back office processes
- Make data available on an open access but secure platform

Key factors shaping transparency

World Economic Forum

It is nearly impossible to track how data flows and is used

The growth of passive data collection from billions of sensors will make disclosure effectively impossible

Effective transparency is contextual and relevant only on specific data usages... not general purposes

Full transparency threatens the economics of secondary usage

Transparency without choice and control creates tension. Individuals have limited control over their data

Too much transparency overwhelms and creates opacity

Organisations need to simplify the ways in which they communicate their data practices to reduce the complexity of transparency for individuals. Also needed are policies and tools for understanding how data flows "out the back door" of institutions. The forward transfer of data throughout the ecosystem is complex, opaque and drives uncertainty and suspicion.

Rethinking Personal Data: A New Lens for Strengthening Trust

WEF[16]

3.1 RELINQUISHING CONTROL

The question organisations need to ask is whether they are ready to change their thinking – to realise that personal data belongs to the individual, not the company.

The management of this data resides with the individuals who provide their permission to the organisation to use it. It's time to give back control, which will improve loyalty.

Rather than owning and controlling their own personal data, people very often find that they have lost control of it.

The Data Deluge, The Economist 2010

The Economist article states, "The best way to deal with these drawbacks of the data deluge is, paradoxically, to make more data available in the right way, by requiring greater transparency in several areas."

Give individuals control over their own data, make the individual the point of integration of data about themselves, help manage relationships with many suppliers (rather than helping organisations manage relationships with their many customers); help individuals specify their wants and needs, and make this available to suppliers in the marketplace.

Personal Information Management Services: An analysis of an emerging market

Ctrl-Shift[17]

4

PRIVACY— PROTECT IT

Trust is only rebuilt when organisations turn words into action. When they demonstrate that they hold the best interests of the individual at the heart of their operations. Where they hand over control of personal data to the individual, who is empowered to grant or rescind access to their information.

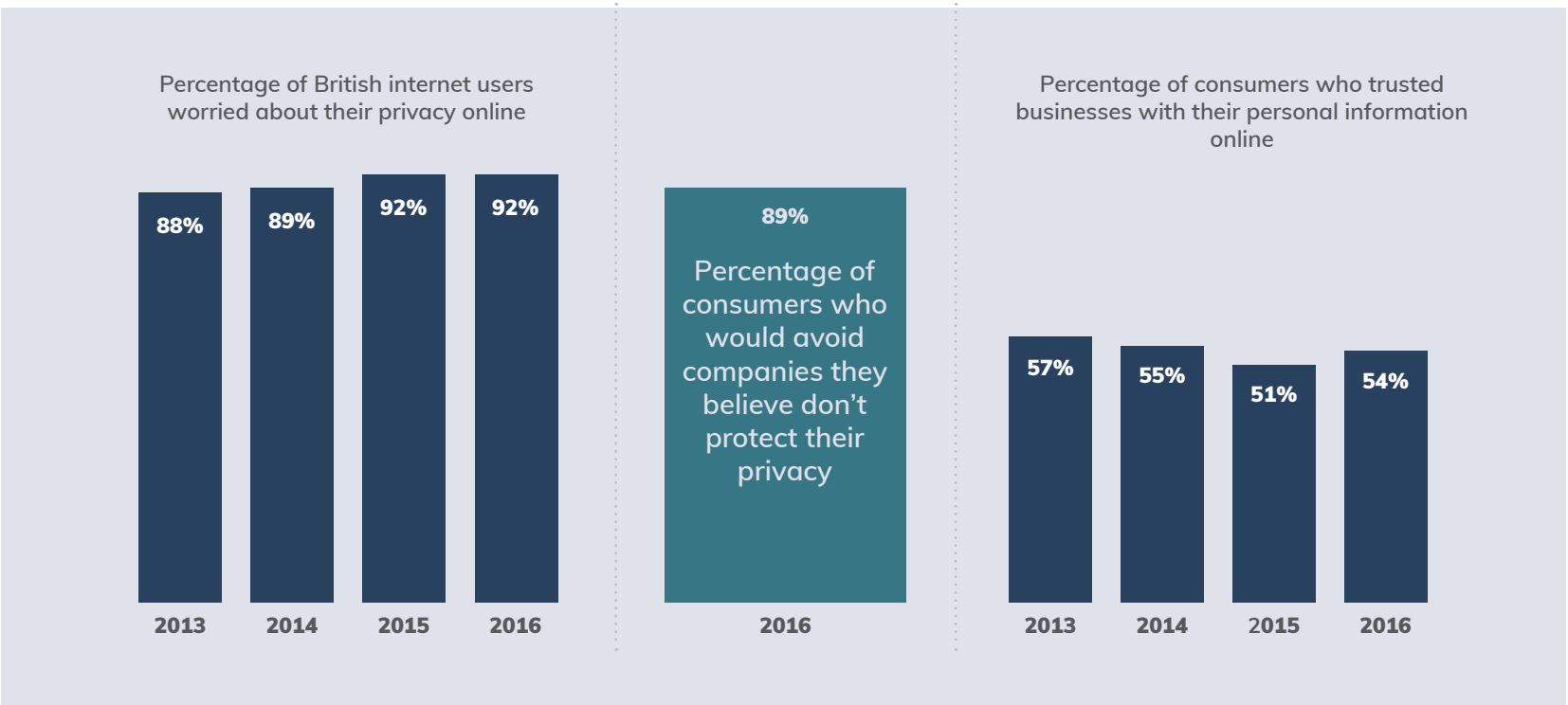
Privacy is one of the biggest problems in this new electronic age. At the heart of the internet culture is a force that wants to find out everything about you. And once it has found out everything about you and 3.4 billion others, that's a very valuable asset, and people will be tempted to trade and do commerce with that asset. This wasn't the information that people were thinking of when they called this the information age.

Andy Grove
Co-founder and former CEO of Intel Corporation

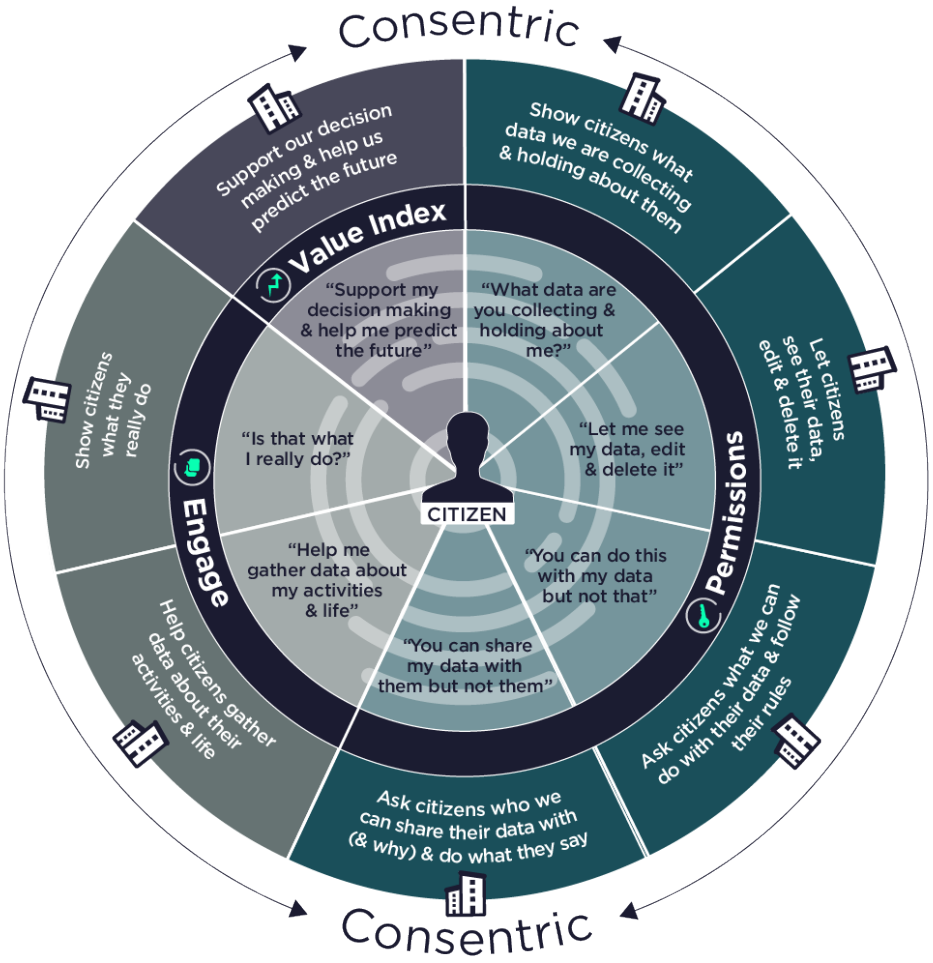
The Privacy Engineer's Manifesto[18]

4.1 PRIVACY CONCERNS

The TRUSTe/NCSA GB Consumer Privacy Index 2016[19] reveals the extent of individuals' concerns regarding data privacy and how this impacts their relationships and exchanges with organisations. (TrustArc - the new TRUSTe)



4.2 ADDRESSING CONCERNS

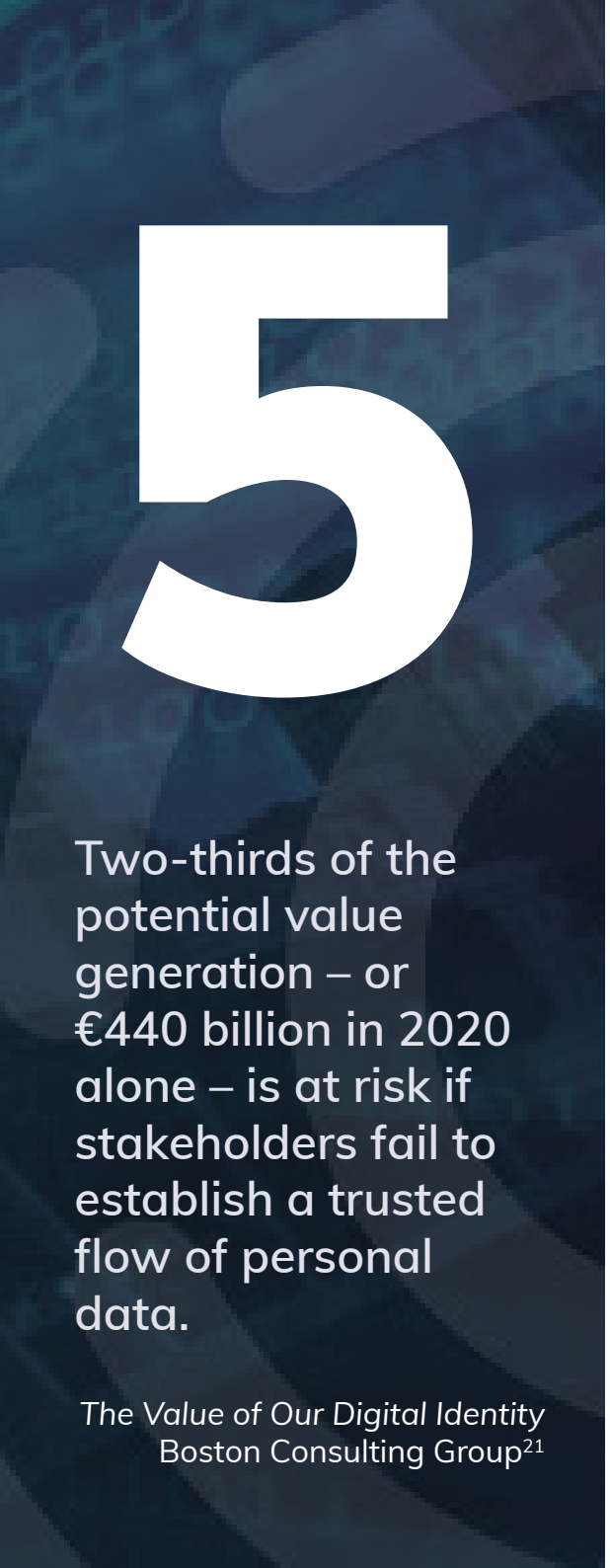


In this diagram we look at how organisations can reduce individuals' concerns and increase the levels of trust.

The inner wheel reflects statements individuals may say or ask, the outer wheel addresses the same from the organisations point of view - as deliverables.

Permissions, Engage and Value Index are solutions that may help organisations deliver these outcomes. Practical steps that can be put in place immediately with the MyLife Digital Consentric Platform.

With the Consentric Platform consented data, real-time data capture, and machine learning are brought together. It's one place for all personal information management, that's secure and convenient and that grows with you.



5

Two-thirds of the potential value generation – or €440 billion in 2020 alone – is at risk if stakeholders fail to establish a trusted flow of personal data.

The Value of Our Digital Identity
Boston Consulting Group[21]

SECURITY — TRUST IT

Security of data is of tremendous concern for individuals and could prove to be a killer blow for organisational or brand trust. Whether it's in the form of security breaches, with credit card details being stolen or incidents of lost records, organisations are under fire for not keeping data secure. Issues around information security have also raised awareness of the value of data.

Breaches have been more prevalent is recent years - see figures below from the ICO Data Security Incident Trends by Sector and Type 2017/18 Report.

January to March 2016	448
April to June 2016	545
July to September 2016	598
October to December 2016	577
2016 Total	**2168**
January to March 2017	678
April to June 2017	697

An increase of 38.4% for the first six months of 2017.

These range from loss of paperwork, data sent in error, information uploaded to the web to verbal disclosures.

Cyber attack decreased by 17% during Q1 2017, but still remain a key risk. Ransomware accounted for 14% of reports to the ICO for the same quarter.

These numbers speak for themselves. Action needs to be taken and security and privacy need to be embedded from the start - not as an afterthought.

71% of people said that they were concerned about their information being protected from loss or theft.

Royal Mail[20]

5.1 DATA BREACHES AND FINES

One of the most onerous areas of the GDPR is how organisations respond if data is breached.

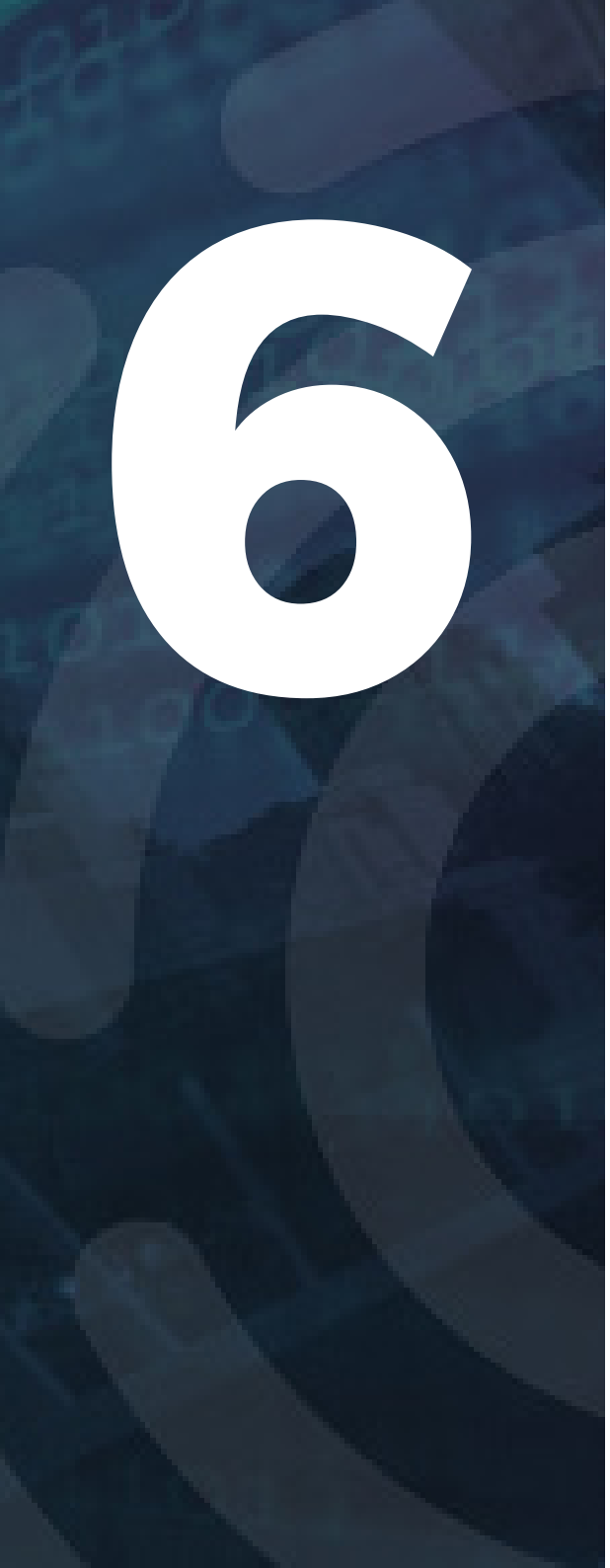
This is also of critical concern to individuals, especially as large scale data breaches regularly make headlines in the news. The most recent organisations hitting the headlines for this are Equifax and Uber. Uber now face government scrutiny around the globe for the data breach affecting 57 million drivers and passengers, which it tried to conceal.

Organisations need to be accountable - to their customers and the regulator. Being prepared for next May should be a priority, and it starts in the boardroom and disseminates through the entire organisation, not just the marketing, sales and IT departments.

A breach can happen anywhere - documents or devices lost, verbal disclosures, ransomware attack or incorrect email distribution.

The regulations now give only 72 hours for organisations to report any breaches to the supervisory authorities. Not only is this a tight time-frame but if processes aren't in place, it will stretch any organisation to the limit.

Equally, depending on the severity of the data breach, you might also need to inform individuals. You will need to look at how much information was held and whether anonymisation of data was in place. If you have stringent privacy protections and anonymisation of data, you might not have to report the breach to individuals.



6

THE VALUE EXCHANGE

The increasing amount of personal data available to organisations plus the ability to analyse and extract insights from it, means data is an extremely valuable commodity. And reports say that data is set to grow 10-fold by 2020 as the internet of things takes off.

It's changing the shape of business. Such data is altering how decisions are made within the organisation and by the individual.

Both parties should benefit from the value exchange and if possible so should the wider community in which the organisations operate - or better still society as a whole.

6.1 THE VALUE OF DATA

In the digital market, data is currency. Highly valuable, it's what organisations trade. Through analysing data and finding patterns and trends, strategies are formed and competitive advantage is gained.

In an increasingly digital society, personal data has become a new form of currency. The biggest challenge for political and business leaders is to establish the trust that enables that currency to keep flowing.

The Value of Digital Identity, Boston Consulting Group[21]

Due to the sheer quantity and value of data, the Personal Information Market Services (PIMS) is a burgeoning industry. Ctrl-Shift[22] found the market to be worth £16.5 billion in 2014, making up 1.2% of the UK economy. This is a greater percentage than either automotive (0.7%) or the pharmaceutical industries (0.97%).

Consumers consider the cumulative value of a common set of their personal data to be worth approximately £140, a figure businesses need to bear in mind when balancing the use of personal data and supplying services in return. However, consumers place a higher value on their data when sharing it with a company they are unfamiliar with – rising to nearly £200 for the full set of data commonly shared online.

The Future of Digital Trust, Orange[23]

6.2 VALUE FOR ORGANISATIONS

According to an Accenture Guarding and Growing Personal Data Value Survey[23], there are big advantages to be gained from the use of data. The ability to deliver better customer experiences (77% of respondents) and entry to new markets and insight that drives product innovation (52%) are two of the top advantages.

So while there is a lot more value that can be extracted from data, it can be done only with the understanding of individuals. Because individuals now recognise the value of their data, they will want to know what it's being used for and the added value that they will gain.

This will help drive product and services strategies, marketing, financial forecasts and all manner of decision making and planning, but only if the data has been obtained using the relevant processing justifications - ensuring full transparency.

72% of consumers agreed that data sharing is part of the modern economy.

81% of consumers believe the data is theirs to exchange for value.

But only 7% believe they get the most benefit from the exchange, while 80% think the brand gets the most benefit.

Data Privacy: What the Consumer Really Thinks
DMA 2015[24]

6.3 VALUE FOR INDIVIDUALS

With individuals waking up to the fact that their personal data has value, the question is: What added value are organisations providing?

We can point to greater choice, increased convenience, higher discounts and a more personalised experience. But while this makes the experience more enjoyable, and satisfies consumer needs and desires, it does not equate to real and sustainable value. Not for the individual. And usually, not for society.

The challenges facing leaders today regarding accountability are essentially the same as 30 years ago: how can we ensure data protection while enabling the personal and societal benefits that come from its use?

Rethinking Personal Data: A New Lens for Strengthening Trust, WEF[25]

The most important takeaway from this study's research is this: Consumers want to share their data – if the benefits and the privacy controls are right.

The Value of Digital Identity, Boston Consulting Group[26]

67% of respondents believe organisations benefit the most from the sharing of data, and just 6% believing the consumer benefits the most – illustrating a pronounced sense of imbalance in the data-sharing relationship between consumers and businesses.

The Future of Digital Trust, Orange[27]

While we might think that value is purely financial gain or reward, that is not the only driver for individuals.

Yes, they will be looking for what benefits them directly, like improved products and services, but they are also concerned about whether their personal data has added benefit to the society as a whole. If organisations can demonstrate how the use of data can improve services or outcomes, fulfilling a broader societal need, individuals will be more willing to share their personal information.

7

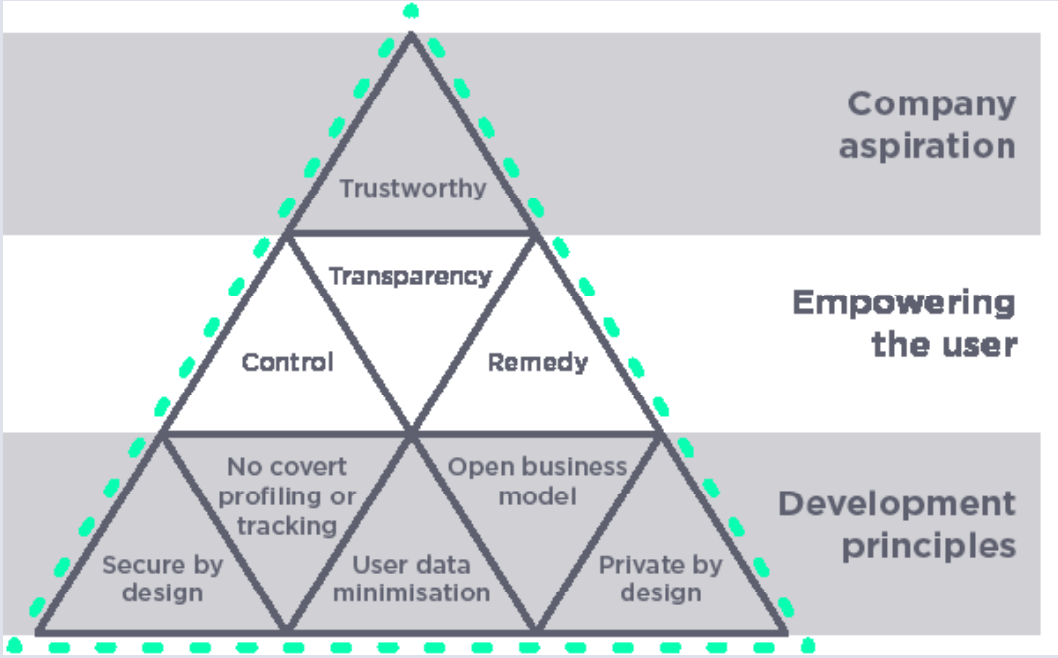
It is not enough for an organisation just to state its aspiration to be trustworthy. They have to put their words into actions and earn back the trust they've spent years destroying.

Trustworthy Digital Engagement
Krowd 2016[29]

A MODEL FOR DIGITAL TRUST

If organisations have the aspiration to be trustworthy - trust needs to be present in every aspect of how organisations engage with their individuals.

The Krowd model for Trustworthy Digital Engagement[28] sums up core principles that should be adhered to.



The Krowd model for Digital engagement Krowd Conference 2016

7.1 DEVELOPMENT PRINCIPLES

These principles are the foundation for how organisations can rebuild trust in the digital world. We've looked at how organisations can address the issues of **Secure by Design** and **Private by Design**.

There are some aspects of this model that challenge conventional marketing and business practices. **Covert Profiling and Tracking** outlaws the use of tracking or monitoring devices that the user is unaware of. Regulations include the Privacy and Electronic Communications Regulations, especially the latest amendment in May 2016.

The PECR covers several areas:

- Marketing by electronic means
- The use of cookies or similar technology that tracks information about people accessing a website or other electronic service
- Security of public electronic communications services
- Privacy of customers using communications networks or services

We have seen that individuals believe companies ask for too much personal information, particularly online. **User Data Minimisation** ensures that the organisation is only collecting data that is required for a specific purpose. This, in turn, protects the privacy of the individual, as less data requires less security.

Krowd's belief is that "The pervasive sentiment that because I go online, the normal rules of society no longer apply is driving dishonest engagement, reluctant sharing and active obfuscation. A digital society that drives these norms is not a constructive one, it's destructive."

7.2 EMPOWERING THE USER

Empowering the user is about placing **control** in the hands of the individual, regarding the use of their data. This in itself provides the perfect opportunity for an organisation to re-engage with their users. If they can show the value they're delivering and the benefit to the individual, and also to society as a whole, they can create the culture of trust that they aspire to.

Organisations need to be **transparent** about what data they hold and the purpose they use it for.

The **remedy** can often be seen as adhering to regulation and legislation. However, Krowd says: "The law is always the lowest possible trust bar; it's a codification of privacy and security principles that sets the lowest standard for operation."

GDPR does give the individual the power to do something about this. If **trust** has been broken beyond repair the ultimate remedy is that they can request that their data is ported to another organisation, and have they have the power to delete their data. The right to erasure.

What's needed is a strategy for the company that gets stronger as time reveals the company's true activities. Hence fostering a company culture that seeks the unattainable goal of being trustworthy is the only sustainable approach to addressing the online trust deficit built up by 15 years of business models that gamify the customer engagement process.

Trustworthy Digital Engagement, Krowd 2016[30]

7.3 CONCLUSION

The call is for a new type of business model. One that is based on **trust**, where **transparency** is central and individual's data is secure and private by design. Where organisation recognise they are **accountable** and their customers are **empowered**.

This is our company aspiration and also the reason why we've developed the Consentric Platform. We call it a trust platform. Our company is somewhere citizen's trust is placed firmly at the centre of everything we do.

We believe it's about finding the **meaning**, **value** and **power** in data.

> "With Consentric, we deliver trust. More than products and services, we're about communicating differently. Developing new and deeper relationships with your market. We enable people partnerships that gain you powerful insights. That add value to the individual, to the organisation and to society as a whole. So everyone benefits. That's the shape of the new digital economy. One that's based on trust."

John Hall
Chief Executive Officer,
MyLife Digital

SOURCES

1 http://www.itpro.co.uk/data-protection/27428/90-of-businesses-think-its-too-hard-to-delete-customer-data

2 How to Fix Capitalism, Harvard Business Review, Michael Porter & Mark Kramer. 2011.

3 WEF, Rethinking Personal Data: A New Lens for Strengthening Trust

4 https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust

5 Edelman Trust Baramoter, 2017. https://www.edelman.com/executive-summary/

6 ICO issues eleven charities with Notices of Intent to fine them Jan 2017. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/ico-issues-eleven-charities-with-notices-of-intent-to-fine-them/

7 http://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-facebook-terms-private-data-sharing-opt-out-how-to-a7210841.html

8 PwC - Total Retail 2017. https://www.pwc.co.uk/industries/retail-consumer/insights/total-retail-2017.html

9 https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust

10 BCG Global Consumer Sentiment Survey 2013 and Big Data and Trust Consumer Survey 2015

11 http://webarchive.nationalarchives.gov.uk/20130107105354/http:/www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4068404.pdf

12 http://www3.weforum.org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014.pdf

13 Boston Consulting Group. The Value of Our Digital Identity.

14 http://www.itpro.co.uk/data-protection/27428/90-of-businesses-think-its-too-hard-to-delete-customer-data

15 https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

16 WEF, Rethinking Personal Data: A New Lens for Strengthening Trust

17 Ctrl-Shift, Personal Information Management Services: An analysis of an emerging market.

18 http://www.bookdepository.com/The-Privacy-Engineers-Manifesto-Getting-from-Policy-to-Code-to-QA-to-Value-Michelle-Dennedy/9781430263555?redirected=true&utm_medium=Google&utm_campaign=Base6&utm_source=UK&utm_content=The-Privacy-Engineers-Manifesto-Getting-from-Policy-to-Code-to-QA-to-Value&selectCurrency=GBP&w=AFC7AU96GZ764TA8ZT1R&pdg=kwd-104399445939:cmp-177155787:adg-15139031667:crv-44091921627:pid-9781430263555&gclid=COHMkPHVodACFQzhGwod9y0Jmw

19 https://www.truste.com/about-truste/press-room/study-finds-more-british-internet-users-concerned-about-data-privacy-than-losing-their-income/

20 Want to talk to me? What customers want in exchange for their personal information. Royal Mail. June 2015.

21 https://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf

22 Ctrl Shift https://www.ctrl-shift.co.uk/news/general/2014/07/28/executive-summary-personal-information-management-services-an-analysis-of-an-emerging-market/

22 Orange, The Future of Digital Trust, 2014

23 Accenture, Guarding and Growing Personal Data Value: https://www.accenture.com/gb-en/insight-guarding-growing-personal-data-value

24 https://dma.org.uk/article/nine-numbers-on-what-the-consumer-really-thinks

25 WEF, Rethinking Personal Data: A New Lens for Strengthening Trust

26 https://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf

27 Orange, The Future of Digital Trust, 2014

28 https://maninthekrowd.com/2016/06/21/redefining-trust-in-digital-engagement/

29 https://maninthekrowd.com/2016/06/21/redefining-trust-in-digital-engagement/

30 https://maninthekrowd.com/2016/06/21/redefining-trust-in-digital-engagement/

ABOUT MYLIFE DIGITAL

MyLife Digital helps organisations and individuals realise the value, meaning and power of their data.

Meaning: An individual gives permission for the use of their data. An organisation gains insights. Both parties improve decision-making.

Value: Redefining the relationship between individuals and organisations. Where there is mutual benefit.

Power: Data is powerful. It gives the opportunity to gain insights. To see patterns. Insights that deliver change.

Using the Consentric Platform, with citizen consent at the heart of the system, data can be collected, collated and shared to better understand needs and issues, increase effectiveness of delivery, and improve outcomes.

Informed insight from informed consent

www.mylifedigital.co.uk | www.consentric.io

T: +44 (0)1225 636 280

E: contact@consentric.io

MyLife Digital Ltd, Reg Office: Citizen House, Crescent Office Park, Clarks Way, Rush Hill, Bath, BA2 2AF

mylife digital