MRS Reports/2018

Great expectations

How technology impacts consumer trust

MRS Delphi Group
Includes new research
from Kantar TNS

MRS Evidence Matters™

Contents

This report has three parts. The first explores the findings from new research. The second examines how technology can drive or destroy trust in more detail, including case studies from several organisations for whom trust is particularly important. Finally we offer a 12 step trust programme for organisations to follow.

About MRS Delphi Group

The MRS Delphi Group is led by a collection of the most respected thinkers in the marketing and research sectors. The Group delivers valuable insight across a range of important business, social and political issues.

The Steering Board includes:
Dr. Nick Baker, Chair of MRS Delphi Group; Phil Sutcliffe, Kantar TNS UK; Colin Strong, Ipsos; Zoe Ruffels, Samsung; Nick Bonney; Tim Britton, Springer Nature; Cat Wiles, VCCP; Jake Steadman, Twitter; Chet Henderson, Unilever; Jane Frost, CEO of MRS.

Thanks to Kantar TNS and Lightspeed for undertaking the research and to Ed Newton, Prospect Consulting, for his help in devising the research methodology.

Executive summary

WPP's BrandZ tracking shows that, over 10 years, brands with above-average trust have grown by 170%, while those with below average trust have growth of -13%. So trust, unsurprisingly, is one of the factors that we use to make purchasing decisions.

Therefore it is a worry for brands that trust in all our major institutions is in decline. This decline in trust has an aggregate effect, but also a negative impact on innovation. It is imperative that brands seek to reverse this decline, both collectively (through regulation and norms of good behaviour) and individually (by improving their performance in areas that respondents tell us affect their level of trust).

This research shows us that:

– **Security of personal data is the largest single driver of trust.** Respondents placed this at number one in six of seven sectors. This shows that the impact of news stories into data breaches, or their personal experience of it, affects who they choose to do business with.

– **Dependability isn't the biggest driver of trust.** The only category in which this ranked first was (understandably) transport.

– **Emotional affinity with a brand in general isn't a dominant driver of trust.** Standards of customer service ranks third, but other concerns about the use of personal data make up the top five. This shows the importance of processes that will be covered by GDPR in 2018, and the critical role of regulation as an across-the-board engine of trust.

– **Capturing and using personal data is a norm for millennials.** Only one in three respondents were happy for brands to use personal information to improve services. But a majority of those 34 and under were happy (54%), while only one in five (22%) of those aged 55 or over felt the same way.

– **But young people punish sloppy data-handling the most.** The younger group were nevertheless more negative about brands who put them at risk through poor security, or misused the data.

– **An online retailer is the most trusted brand.** The brand that consistently performed well for all drivers of trust is also one of the most intensive and innovative users of personal data. While Amazon is an unashamed advocate of technology in creating and delivering service, it has shown that careful use of the opportunities (for example, giving equal priority to bad and good reviews) has increased trust in the brand that is transferable to new business ventures.

See page 4 for full research findings and research methodology.

Foreword

Jane Frost, CEO, Market Research Society

We are all used to hearing about data leaks and the subsequent cover-ups. Many of us experience frustratingly obtuse customer service, and personalisation can be misguided or downright creepy.

The story of tech is often negative, and that's a real opportunity for some organisations. The ones that get it right will build a brand that doesn't disappoint and exasperate; a brand that really puts customers first, which they can trust.

This report sets out to explore some of the positive aspects of how technology can have an impact on consumer trust.

Three years ago, the MRS Delphi Group published a privacy report 'Private Lives' and since then we've seen many epic fails from brands that didn't read the writing on the wall.

Of course, any definition of trust is fluid and there are many aspects to trust that are not touched on here. But for the purpose of this report, we have focused on trust as experienced through technology, and our survey included 18 consumer 'trust expectations' spanning the themes of transparency, control, relevance, security and fulfillment.

As we will see, some trends may be taking longer to play out than originally expected and many of us are still in quite a traditional frame of mind when it comes to our personal data. For example, marketers and planners may delight in the potential that data provides to microtarget customers, but are customers as delighted?

Our research reveals that many consumers first want to be convinced that a brand can meet basic needs in terms of safety and security, before they embrace a deeper relationship founded on more sophisticated proposals like data value exchange.

Working within the framework of Maslow's hierarchy of needs, all organisations need to identify the'deficiency needs'of their customers. These are the minimum customer trust expectations, the table stakes, that every organisation is now expected to deliver. This foundational level of trust is required before an individual will progress to allowing a brand to fulfil their 'growth needs'. A clear warning from this report is for those brands who think they can leapfrog the first step and provide their customers with sophisticated services and technology before establishing their credentials in meeting these foundational needs.

Amazon gets top marks, in part because the public does not associate it with data breaches and so meets the foundational trust expectations. Also, we don't feel the rub when personalisation kicks in. The data value exchange is frictionless, not an irritant, and the pay off is a good efficient dependable service. Technology is certainly in this instance a large contributor to brand loyalty.

This report raises critical questions for brands – not least whether you are measuring against these expectations as part of your reputation index?

How much of this is merely a function of transparency, and how much is the wider emotion of trust? Back to definitions. When customers trust they remain loyal to a brand in the face of uncertainty and risk. When push comes to shove will Amazon go beyond the Ts&Cs to help you? Could you the customer take a risk, leap into the known, and rely on your favourite brand to catch you?

In some ways we already take huge risks, and we do so increasingly. Each new service stretches our definition of trust a little bit further. Today it's common to get into a stranger's car. Tomorrow that car may be driverless.

The MRS Delhi Group's hypothesis is that these consumer trust expectations are evolving, in some instances faster than organisations can keep up with, and in some surprising directions. Our research suggests that millenials have a heightened understanding of what can go wrong and brands should not underestimate their capacity to punish those that fail to protect their data.

With GDPR providing a corrective to some of these trust issues, it is important that we understand where our customers sit within the framework of these trust expectations and how their expectations change depending on, for example, sector (see page 6).

This report raises critical questions for brands – not least whether you are measuring against these expectations as part of your reputation index?

Another clear message in this report is that meeting trust expectations needs to be a cross departmental effort, driven from the top down. Investment in tech is strategic and long term. If you measure against these trust expectations your business case for investment in technology to improve customer services and experience will be much stronger.

We live in an era of marginal competitive advantage. Getting data security right is now the cost of doing business. In this environment shiny and new doesn't count for anything if you haven't established whether you are keeping up with these evolving trust expectations.

Technology is critical to transparency, and transparency is critical to trust. The difficulty we have in establishing where one starts and the other ends reflects the shifting sands of customer needs, and the need to measure, monitor and analyse them constantly to ensure future growth.

Phil Sutcliffe, Director,
Offer and Innovation, Kantar TNS UK

Trust is vital for brands. WPP's BrandZ study shows that brands with above average levels of trust have grown their brand value by an average of 170% since 2006, whilst those brands with below average trust have declined by 13% brand value. Yet business operates in an environment where there are declining levels of consumer trust. The Edelman Trust Barometer found significantly declining levels of trust for each of media (36% to 24%), the Government (37% to 26%) and business (49% to 33%) since 2013.

We live in a technology driven world where connected devices provide a flow of data from consumers to business. In recent years there have been a number of well publicised breaches of these data from companies including Uber, Yahoo and Talk Talk. Consequently consumer concern about the security of their data and how it is being used by organisations has been posited as one of the key factors driving the decline in trust. More broadly, the story of 'tech' in the media is often discussed in the context of biased algorithms, devaluation of the workforce and the dehumanisation of society.

The MRS Delphi Group wanted to investigate this issue of trust with a particular focus on technology and data. We wanted to understand how important technology and the data it produces are to perceptions of consumer trust in business and what other factors are important. And we want to inspire organisations to turn the prevailing negative narrative on its head by looking at how technology can build trust by meeting new consumer expectations of transparency, control, relevance, security and fulfilment.

Kantar TNS and Lightspeed Research conducted research on behalf of the MRS Delphi Group with 1001 people in the UK to understand the drivers of trust across telecoms, banks, retailers, fashion retail, media, transport and public services and to look at public perceptions of the trustworthiness of different brands and organisations.

We found great consistency in the drivers of trust across all sectors. Data security through consumers wanting to be reassured that their *information is completely secure* was the most important driver in six of the seven sectors. Additionally, ensuring that *my participation will never put me at personal risk* was one of the top five drivers. So it is clear that customer fear of data leakage is incredibly important and organisations need to consider how technology such as blockchain can increase security and build greater trust with customers.

With regard to data security, there is some good news for the oft-maligned financial services sector. Banks, and especially the big, longer established banks are best regarded among the 42 businesses and organisations we asked about, with Lloyds coming out on top. At the other end of the spectrum there is more work to do on providing reassurance about data security among media companies, with both traditional media brands like The Sun and Sky News as well as newer media businesses like Facebook and You Tube having much weaker perceptions for data security.

> With regard to data security there is some good news for the oft-maligned financial services sector. Banks, and especially the big, longer established banks are best regarded.

Attributes related to the fulfilment of customer service were the second and third biggest drivers of trust through *providing a dependable service* (highest driver in transport) and *always offer high standards of customer service*. Customers wanting to feel a sense of control through *there always being someone available if I have a query or complaint* was also a key driver, especially for banks, retailers, public services and transport. In these areas Lloyds, Nationwide, BT, Tesco, John Lewis, Amazon and the NHS are among the top performers.

For the fulfilment of customer service, businesses should be thinking about how technology in the form of virtual agents (chatbots) working alongside human representatives can deliver improved customer service and how digitisation can be used to deliver a seamless omnichannel experience. In certain sectors, notably transport, technology can be used to keep customers better informed of service delays and changes, to manage improved traffic flow and increase customer safety.

The final key driver of trust again relates to data and specifically, *they do not take advantage of the information available about me*. Whilst this need for a fair value exchange in the use of data is clearly important, organisations have work to do to establish the best ways to provide this value. It's interesting that *using my personal information to provide a tailored service unique to me* was the lowest driver of trust.

Transparency around how organisations use customer data and the value exchange they provide will become increasingly important and not just due to the impact of GDPR. The key differences in trust drivers between millennials and older people relate to use of data. Millennials have both a greater acceptance that organisations will use their data (being less concerned about permission being asked to use their data or being able to tell organisations to erase their data) but also a keener understanding of the risks than older people. Concern about being taken advantage of via their data and misuse of data putting them at personal risk is higher among millennials.

> Millennials have both a greater acceptance that organisations will use their data... but also a keener understanding of the risks than older people.

In summary, there are three overarching areas that organisations need to focus on to build trust:

1 Providing guarantees on data security

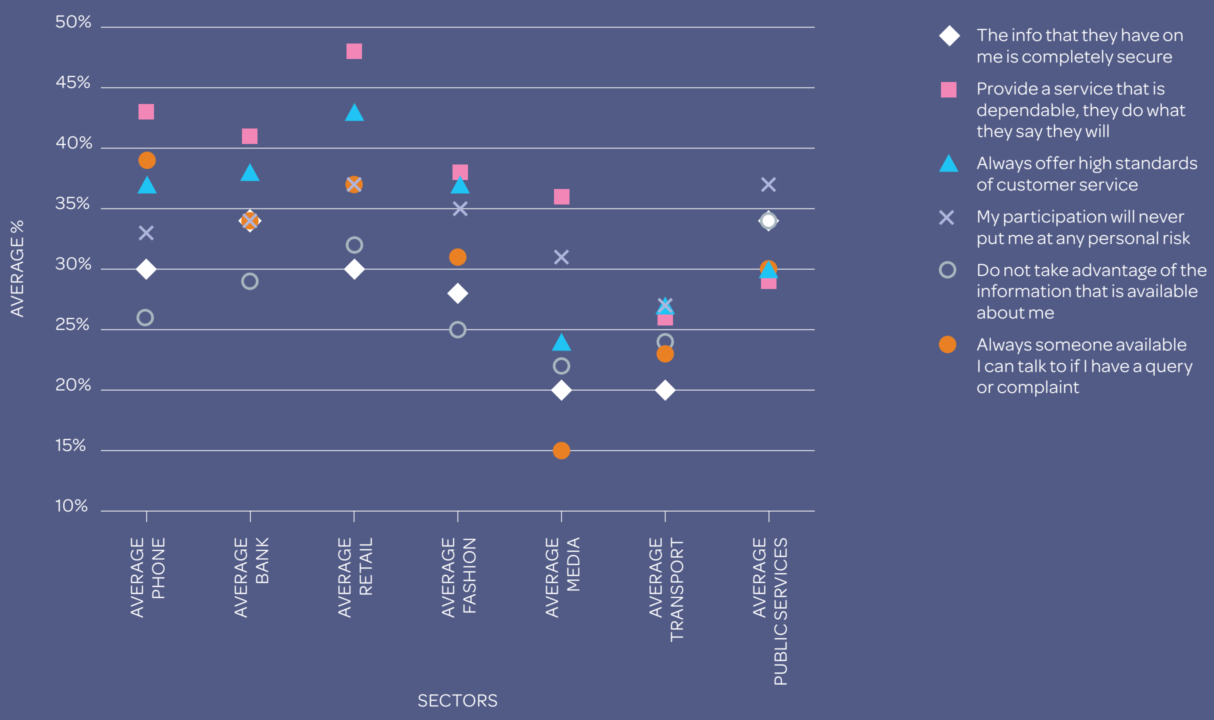
2 Transparency about how data is being used

3 Delivering utility through a strong customer service

Savvy brands and organisations should be thinking about how they can use technology to provide reassurance and value in these three areas and build more enduring, trusted relationships with customers as a result.

For inspiration about how technology can be used to build this trust, there is one stand out brand that organisations can look to – the business that scored highest on average across all of our trust attributes? Amazon.

FIGURE 1: PERFORMANCE OF EACH SECTOR ON THE TRUST DRIVERS: DATA POINTS SHOW THE PERCEPTION OF EACH SECTOR AGAINST THE TRUST DRIVERS, BASED ON THE AVERAGE SCORE OF SIX BRANDS IN THE SECTOR.



Note on methodology
This was a conjoint exercise where participants were asked to trade off against pairs of attributes ('trust expectations') across each of the seven categories. The research with a national sample of 1001 UK adults was conducted online by Lightspeed.

Fieldwork was conducted between 5–9 January 2018 with quotas set to be representative of the UK online population. You can view the percentages and wording of questions. If you have queries about this research email tnsuk.enquiries@tnsglobal.com

From transparency to the uncanny valley, business journalist Tim Phillips talks to five very different brands about how they view the role of technology in building trust in their organisation.

"Trust and influence now lie more with 'the people' – families, friends, classmates, colleagues, even strangers – than with top-down elites, experts and authorities," claims Rachel Botsman in her book *Who Can You Trust?* (Penguin, 2017). Retailers lose our data, and attempt to cover it up. Supermarkets sell horsemeat from suppliers that they fail to monitor effectively. Security holes in hospital networks make them, and their patients, vulnerable to hackers. Loyal customers are no longer targeted for discounts. Brands claim to be ethical, but use slave labour in their supply chain.

In all these examples of trust betrayed, and many more, technology is seen as being at least partly to blame. It has simultaneously made it easier for brands to create messages and communicate them, but also for brands to be undermined when they slip up. For customers, technology offers a wider array of choice in the ways they entertain themselves, shop, learn or play, but we also struggle to find the reliable information we need to place our trust in one institution or brand.

Therefore the dominant narrative is that technology has undermined trust. Whether we are citizens or chief executives, we regularly feel out of control, unable to keep up, or vulnerable to fake news.

Yet there is another role for technology. It can inspire trust. It does this in at least five ways.

1. **It can provide security and protection, whether through encryption, identity management or distributed trust systems such as blockchain.**
2. **It can create the structures and processes in which incentives are aligned, whether inside an organisation or across a supply chain, that deepen trust in relationships.**
3. **It can make it possible for brands to be open and vulnerable, by sharing more information with customers or other stakeholders automatically.**
4. **It can create managed platforms on which buyers and sellers meet, do business, and rate each other.**
5. **Finally, it can use artificial intelligence to understand us better.**

For each of these there are risks and rewards. But there is also a risk to not engaging with the evolving potential of digital trust, one that we are already seeing. Technology is also a force for transparency, and institutions and brands who close their eyes to the opportunities may open them to find they have been undermined.

1

Trust through security

This is often seen as basic hygiene for a brand, but it is far more than that. For all sectors, it is the basic foundation of trust, and for some it dominates all other drivers – for example, in financial services. It has also been the dominant creator of "technology undermines trust" news stories for many years.

On one hand, this is justified. We know that attacks are still prevalent, and that the impact of an attack is mostly in the indirect costs of dealing with unhappy customers. For 12 years, the Ponemon Institute has measured the extent and the cost of data breaches. In 2017, for the UK, the average cost per customer of a data breach was £98. More than half of this (£53) is the indirect costs, including "abnormal turnover or churn of customers". Half of these breaches (the more expensive half) were from malicious attacks, and those organisations that has a churn rate above 4% after the attack has an average cost of breach (£4.5 million) three times that of companies with less than 2% churn.

£98

The average cost per customer, in the UK, of a data breach in 2017

On the other hand, not being afraid to discuss the challenges of security can be a driver of trust. The ability to provide enhanced security features (for example, two-factor identification) and provide education – including warnings – to customers has a positive impact on trust, research shows.

2

Managing incentives

Trust incentives need to be aligned throughout an organisation. For example: Wells Fargo in the US was fined $185 million, after staff created 3.5 million fraudulent checking and credit card accounts for their customers between 2011 and 2016, by accessing their personal accounts and ordering products in their names. Since the scandal broke, the bank has also admitted that it secretly increased the cost of 800,000 car insurance contracts. They did this to meet branch sales incentive targets that were so stringent that employees reported vomiting through stress. Management later denied this was a cultural problem, and reacted by firing 5,300 employees between 2011 and 2016 for fraud. So while policy was to ask customers to trust the bank, and individuals working at the bank may have been trustworthy in other contexts, a combination of unrealistic sales incentives (motive) and the vulnerability of internal processes to manipulation (means and opportunity) undermined the norm of trust between bank and employee, and inevitably bank and customer.

Case study

Nationwide

"We're not a bank and we have members not customers, so our entire language is entirely different," says Sara Bennison, CMO of Nationwide, explaining why many of the signals of trust are entirely different in her organisation.

Nationwide is one of the few remaining building societies in the UK, and so it is owned by exactly the same people who trust their money to the organisation. When it comes to generating trust between members and the organisation, the fundamental difference between Nationwide's mutually-owned structure and a plc is that incentives are aligned, she says:

"The AGMs are different, when you are face-to-face with members, justifying the decisions you made is very different. Explaining why you made often difficult decisions, which aren't immediately going to be popular with the membership but were the right thing to do to keep the society safe, secure and well-capitalised. We are held to account by ordinary people who have their life savings with us. There isn't a filter between what we do and the people we do it for."

The mutual structure also clarifies the trust relationship in strategic decisions. "We are working out how we can pay the best rate to our savers, whereas if you work in a bank you need to work out how you pay savers as little as possible in order to manage the rest of the balance sheet," Bennison says, "that is also fine in a different context, but it is a different purpose, and functional level of trust. For us there is no conflict of interest in which you are trusted by your institutional investors to double their profits but also by your customers to give them the best deal. In that case you have trust with different stakeholders, who may be trusting you to do different things."

This also is reflected in the conduct of staff, who are trusted to take the initiative, to "do the right thing" when dealing with members in branches. It may also mean that strategies to grow are more often based on long-run value, with a five-to-10 year horizon, rather than short-run profitability.

"It is a culture that favours collectivism and commitment to a cause rather than isolated acts of brilliance," Bennison says.

The role of technology at Nationwide:

Technology has no instrumental role in promoting trust, but it acts as a way to monitor, measure, and create alternatives for members who feel comfortable using it. For example, in its research Nationwide tracks trust metrics, but does not try to influence them directly. Similarly, its phone banking product offers a service to customers who need it, but has not been created to do away with branches. "We're not in the business of mass closures. We absolutely believe there's an important part of the business that is human contact. Getting that balance between channels is important," Bennison says.

3

Openness

This has many dimensions: the idea that brand can have humanity, that it is real and not an artificial construct that hides behind a screen, that it embraces transparency, and that companies allow themselves to be vulnerable are all drivers of trust. Clearly this is more about an emotional trust connection than a transactional relationship, but this does not mean that technology does not have a role.

Case study

SkinNinja

The message that SkinNinja, a simple mobile app, sends to brands is that if they don't take care of their transparency, someone is likely to do it for them. Charlotte Morris, cofounder, asks "Who wouldn't want to know what's going onto their skin?"

The inspiration for the app was the skin allergies of Morris's cofounder, Jo Osborne, and the obscure language of the average cosmetics bottle. You scan the product barcode, and if tells you what those complex words mean. "The average woman puts on 16 products per day," Morris explains, "there's 30 ingredients in each of those products."

The ingredients are reported as green (all clear), amber (not 100% clear science) and red (pollutants, carcinogens, and so on). SkinNinja does not commission its own research, choosing to make existing peer-reviewed data possible for non-scientists to understand. The app also isn't campaigning for a particular cause, in favour of or against any brand. It focuses instead on trust: Morris argues that consumers are "basically being lied to by marketing. As a marketer, it's been interesting to get a better insight into this."

The role of technology at SkinNinja:

Technology creates trust through clarity. SkinNinja does not create information. It organises it (by taking the results from existing research and making then accessible to the general public), and it uses it to provide access (by linking barcodes to data).

Case study

Monzo

"For some British millennials, Monzo is as close to a cult as a bank can be," the Economist reported in February 2018. The startup bank has only existed since 2015, and only received a banking licence in 2017, but already has 370,000 current account holders. The bank claims to have spent "practically nothing" on marketing. What has caused hundreds of thousands of people to trust a startup with their savings?

Tristan Thomas, head of marketing says that the brand was created out of frustration with the opaque structures and communication of traditional banks. "This isn't an opportunity that we're 'targeting' for marketing purposes, it's just the way we think things should be done.

Traditional banks are slow to innovate, don't put the best interests of their customers first, and the way they do business is incredibly opaque. We wanted to change that."

Monzo is joining the ranks of digital-first brands that are built around community. Research by the Nobel prize-winning economist Elinor Ostrom has shown the importance within informal communities of norms of trust that exceed compliance to laws or regulations: in these communities, we tend to reward those who satisfy our expectations, and disproportionately punish those who disappoint us. Monzo is attempting to create a similar non-hierarchical community in the way it finds customers and provides the service they want. The result: more than four out of five new accounts are opened through word-of-mouth.

"We're trying to build a company and brand that puts our community of customers at its heart, and I think that can only get stronger as we scale," Thomas argues, "There's no reason transparency, customer centricity and fairness shouldn't scale up to millions or billions of customers."

Examples of this approach to making itself open and vulnerable are the way it raises investment by crowdfunding among accountholders, and its "transparency dashboard", including diversity, investment ethics, and financial reporting that is far more detailed than regulatory requirements. Monzo also measures the impact of transparency on its growth. "We can now track whether customers who use our 24/7 chat support are more likely to tell their friends about us compared with those who haven't, or how much more supportive our crowdfunding investors are compared to new customers," Thomas says.

Although still a young brand, Monzo's structure has echoes of the cooperative movement with 21st century technology applied to it. The cooperative movement relied on trust in small communities. In the 20th century, banks relied on the institutional trust, of the type that we know is in long-term decline. Monzo has created a more distributed form of trust, almost like a human blockchain. It has devolved its marketing not to advertising (it doesn't do any), or to branches and branch staff (it doesn't have any), but to the people who use the service.

"I think we're building something different: something that takes aspects of the cooperative movement by involving our customers in what we're building, aspects of the startup world by innovating and improving quickly, and aspects from the nonprofit world with our commitment to transparency and accountability," Thomas says, "The one industry we aren't taking much inspiration from is banking.

4

Platforms

Technology platforms are rapidly becoming the default markets for many types of interaction. Amazon in North America and Europe, and Alibaba in China are both dominant retailers. But AirBnB, eBay, Uber and many others have also had a profound effect on how we interact.

Trust derived from technology makes these platforms practical, because the platform, in economics terms, evens up the information asymmetry which prevents business being done (or buts one side of the trade at a disadvantage). The idea is to expose as much information about each party as is useful. We commonly think of this as performance ratings, but other aspects also apply: tracking a package, clearing payments, resolving disputes are all enhanced by technology. Good measurement, especially of the impact of advertising, is an essential component of digital trust.

The Pew Research Center finds that 82% of people read reviews before purchasing for the first time (more for younger purchasers).

On the other hand, if these environments are systematically manipulated, this undermines trust. This is an example of misaligned incentives: if there is an incentive to pay someone to post fake reviews for a restaurant, then a restaurant will pay for reviews, and others will then have an incentive to post fake reviews too. In 2017, the Vice journalist Oobah Butler famously made his garden shed, or "the Shed at Dulwich" as it became, into the number one rated restaurant in TripAdvisor, before he had ever served a meal.

There are two ways in which technology might solve this problem. The first is that, if there are competing platforms, the one with the least trustworthy information about counterparties is seen as risky, yet this has the problem that even this informal rating is open to manipulation. The second is the potential for blockchain to become the engine of trust for "to partner with restaurants and other food services to provide discounts or rewards to users who participate in the platform. By providing a digital currency that users can redeem or trade, blockchain applications are incentivising quality control and platform advancement," according to Chelsea Lam, who is now the cofounder of Munchee, a food and social networking mobile application, but who previously led the midmarket sales programme at Google.

82%

of people read reviews before purchasing for the first time

Case study

ITV

"It's a brilliant time to be a viewer," says Rufus Radcliffe, group marketing and research director, ITV. "I've worked in TV for 20 years. For years you'd sit in research groups and viewers complained there was nothing to watch, or it was all repeats, or it was all boring. Now there are the equivalent of book clubs for TV, and people will get together to talk about quality drama they like."

Radcliffe joined ITV in 2011 to lead a transformation of ITV's marketing and research activities, but has witnessed a transformation of the role of television that has increased the role of, and opportunities for, trust relationships. As he says, "TV is no longer considered by viewers as a guilty pleasure. It's considered, quite rightly, as a cultural pursuit. As a big mainstream entertaining brand, we're at the heart of those conversations."

Because ITV is almost entirely free-to-air, funded by its advertisers, in many ways it is a two-sided platform business: if it attracts enough advertisers, it can fund the programming that viewers aspire to. If it attract enough viewers to watch those programmes, it protect advertising revenue. Therefore, on one side, advertisers must trust that audiences are measured correctly (through BARB), and that regulation, tone and quality are protected.

On the other side of the platform, the ITV brand must be a signal of a trust relationship with viewers. At a basic level, this ensures that content is suitable and recognisably an ITV product. But there must also be a deeper connection, Radcliffe argues, which cuts through in an increasingly crowded market.

"When I joined ITV we did a whole quite radical redesign of our brand, across all our on-demand and channels. The market that we compete in is much more competitive than it was. We have to work much harder to keep our viewers happy and to continue to grow."

The threat for media brands is that viewer trust is placed not in the platform, but in individual personalities or shows, and that ITV's trust signal becomes less relevant. Radcliffe argues that currently, for ITV the opposite is the case: that his brand is seen by many viewers as a curator in a world of potentially disorientating media overload, "All of our research also says that viewers care about the brand that brings the programme to you. The brand means something, it's an editor of choice," he says.

The role of technology at ITV:

"About 50% of all viewers have decided what they're going to watch when they switch the TV on. Technology will help people find content in new ways, but you've got to be the brand that triggers them to search for it in the first place. Being the curator implies we're taking responsibility, and we are signalling accurately what's inside the package.

"The viewer journey to finding that content is likely to evolve over the next few years. Our trust with viewers will be that if they give us their data, tell us who they are and what they like and don't like, we have to ensure that we give them a brilliant personalised experience. When we send out emails or a mobile push notification, we need to understand what they watch, and that is a mutually beneficial relationship between ITV and our viewers."

5

Artificial intelligence

One of the problems with using technology to build a picture of who to trust is that there is simply too much data. If you have ever consulted three different online ratings systems for a restaurant and found yourself less able to decide which to choose than when you started, this is the problem.

Artificial intelligence is a way to simplify this problem by doing some, or all, of the work. This is not without problems. The most pressing is that an AI is unable to explain how it reaches a decision (see box). Personally, we can choose to accept its film recommendation or suggested route to work, or trust our own instincts, with little risk. But as AIs become more highly specialised, and we trust them for our medical care or to solve crimes, society demands a level of accountability.

We will need to understand that an AI will have bias, Ron Tolido, CTO at CapGemini says, because they learned from a world which is also biased. "At least they can be transparent in their bias. The bias in unavoidable, but we can see it. This is interesting: it can be a trigger for a foundational discussion that the organisation should have had anyway. Do you think the bias wasn't there before? Of course it was. Now we have to discuss whether we can live with it."

The other problem in using AI is that it can become too good. A system that is one step ahead of us all the time falls into the "uncanny valley", where computers mimic humans so well that we are instinctively weirded out. Its actions might be seen as supernatural, and we interpret it as a threat. One solution: bots that have a cartoon-like look, and that announce themselves as bots immediately rather than try to convince customers that they are human, often are trusted more by consumers.

Case study

CapGemini and the "grey box"

Machine learning has the ability to pool vast amounts of data from transaction histories, websites, in-store behaviour and CX research and combine that with other external data to make much better predictions, and "know" the customer far better than is currently possible. But will this enhance trust (because the recommendation is good), or destroy it (because it seems weird)?

Ron Tolido, CTO at CapGemini, suggests that AI-driven communication needs to be carefully managed if it is not to destroy trust. Adaptive filtering (people who also bought this, bought that) has been powerful and effective, he says. One of the advantages is that it is easy to explain.

However, as AI becomes more complex, it becomes harder for customers and citizens to understand why decisions were taken. This is a challenge for the emerging world of data ethics. "Neural networks are not based on an algorithm. They are essentially a black box. That makes explaining what they did very difficult. A neural network cannot explain what it did," Tolido says.

He and his team have been working on what they call a "grey box" AI, which can at least report the logical steps on the way to reaching a conclusion. While it will remain impossible for a neural network to explain itself (it learns by examining thousands of data points and finding what works, rather than following predetermined rules), some reporting is better than none. We might not know how Netflix decides that one film is a 98% match and another is only an 83% match for our preferences, but it gives information and leaves power in the hands of the viewer, which is a basis for trust, Tolido says.

12 steps to greater trust

Organisations that want to build trust with their customers should be addressing each of these steps in their policies, planning and technology investment. Thanks to Anjali Puri, Kantar Global Director, Qualitative Offer and Expertise, who drew on Kantar TNS's annual Connected Life study to help develop this guide.

1

You can hurt us

Trust relationships for electronic commerce are also deepened by a sense that the all-powerful brand makes itself vulnerable. For example, no-questions-asked returns on Amazon, or the opportunity to try a premium mattress (a non-traditional technology purchase) for 100 days. This is the technology-era equivalent of letting a car buyer go for a test drive. Aviva, for example, is reducing the number of questions it asks customers when deciding on policies, as part of a campaign to use its customer data to strive for "get a quote not a quiz" insurance with less red tape.

2

Align incentives

Some companies (Starbucks, or Nationwide) successfully devolve the task of inspiring trust to frontline employees. Technology can create new ways to grow business, but it will destroy trust if the incentives of employees and management must be aligned, as the Wells Fargo case (page 8) shows.

3

A human face on technology

Though the emphasis put on this differs by culture, consumers (especially in countries in which feelings of emotional affiliation are important) are more likely to trust relationships that are intermediated by technology when there is a "human face" for the organisation. The best example for this is Jack Ma, the CEO and face of Alibaba. As Rachel Botsman explains in Who Can You Trust?, "what makes Ma's story extraordinary is that he achieved this in China", a country in which few believed that internet commerce could displace the traditional relationship-building that made trade possible. When Alibaba had its IPO, Ma became the "face" of trust itself. As Botsman reports, he deliberately used the word repeatedly in interviews: "Trust the new technology... Everything you've been worrying about, I've been worrying about for the last 15 years."

4

You are not your bot

Customer service bots are popular and relatively-well accepted by consumers, but unless they can be used flexibly, they are seen as a barrier, not a service. Therefore it is important to use them to create flexibility. It might be that some problems are quickly escalated to a human who can employ judgement. It might simply be that the bot is not programmed to treat all customers identically.

5

Walk the talk

Customers have respect for brands that signal their values in the technology world, as long as they are prepared to back it up. In February 2016, the FBI asked Apple to create and software that would enable the FBI to unlock an iPhone 5C that had been used in a terrorist attack in San Bernardino, California, which killed 14 people. In a strategy that was initially condemned by the public and politicians, Apple refused. This refusal was eventually supported by Microsoft, Facebook, Twitter, Amazon, the ACLU, the United Nations High Commissioner for Human Rights, and even general Michael Hayden, former head of both the NSA and the CIA. A survey by Piper Jaffray conducted immediately afterwards showed no negative brand effect.

6

This might hurt

As consumers have easier ways to establish whether what you say aligns with what you do (see SkinNinja on page 10), there is an increased emphasis on messaging that demonstrates some things are more important than sales. The most famous example: Patagonia's advertising campaign for Black Friday 2011, that announced "don't buy this jacket". It is just one of founder Yvon Chouinard's commitments to responsible growth, which involved running the company debt-free since 1991. Sacrifice, even when the customer does not directly benefit, acts as a trust signal every bit as potent as the "face".

7

Don't hide the negative

Can we increase trust by using the internet to reveal failings? In research, customers repeatedly say yes. Even if you own the platform, customers notice when negative reviews are downgraded or de-emphasised. Showing them ratings gives them a sense of agency, because it removes the information asymmetry that makes people unwilling to commit to doing business (This also applies across the supply chain, where many offshoring relationships, for example, are not transparent – meaning that consumers are unable to make ethical judgements about the origins or provenance of the things they buy). Therefore, giving the opportunity to view bad ratings is trust-enhancing in the long run, even if the act of making yourself vulnerable in this way may not increase sales today.

8

Treat me as an equal

In an episode of Seinfeld, Jerry tries to get rid of a pushy sales caller. "I have an idea, why don't you give me your home number and I'll call you back later?" he says. "We're not allowed to do that," the caller replies. "I guess because you don't want strangers calling you at home," Seinfeld says, "now you know how I feel." The message is that we often use technology to treat customers in ways that demonstrate the brand holds all the power: for example, by removing a contact phone numberon a website. There may be good short-term operational reasons to do this, but research shows a long-term erosion of trust.

9

Fair warning

Everything is risky, including commercial transactions. Warning customers about the levels of risk is often viewed as a compliance problem, when it could more appropriately be viewed as an opportunity to signal the quality of trust in a relationship. Complete data security is impossible, but openness about exactly how data is protected (clearly, within reason), and what would happen if anything went wrong is a signal not of weakness, but that the customer is treated as an equal who deserves to know. This creates a different type of trust relationship. It's less about convincing customers to trust your brand, and more about encouraging them to trust themselves.

10

Do not cross boundaries

Friends also respect boundaries. Data protection regulation has for decades specified that you do not collect data for anything other than the purpose intended, and that you are precise about the uses to which this data is put. Basic compliance isn't optional ("if you don't have security, governance and ownership, everything else you do is useless," as one contributor to the report put it). But, even if you are compliant, there is also a trade-off: is the operational benefit from collecting more customer data greater than the potential penalty of creeping out your customers?

11

Why are you selling this to me?

AI is great at suggesting what consumers should do, but less good at explaining why they should do it. For example, a film recommendation might be spot on, but is likely to inspire as much unease as trust without some justification for why it was suggested. At its most basic level, associative matching is "because you watched this". It's simple, and intuitive. More complex matching becomes a black box, but even a percentage rating for the strength of the recommendation can deepen trust in it.

12

What is measured is managed

The multiple dimensions of trust rely on processes that happen in different parts of the organisation, with different managers, and are parts of different processes. It's also easier to measure an operational achievement (99% success) than its impact on customer trust (would they rely on you? Has this changed?). A measure of trust, and its impact for any business has to be based on a clear evaluation of which trust drivers customers value, their relative importance, and the way their impact is evaluated.

Download all Delphi reports here: mrs.org.uk/reports

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

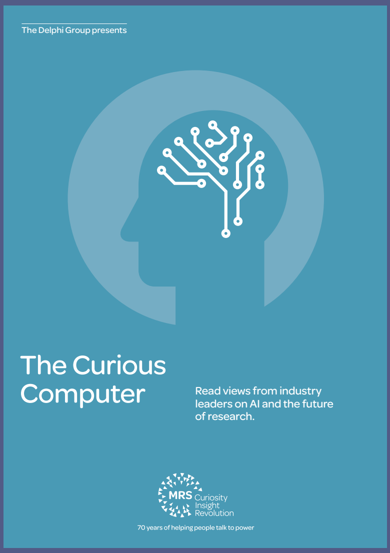
Private Lives?

A look at privacy issues through the lens of the consumer.

MRS Reports/2015
The politics of persuasion
New research reveals what influences voters
Commissioned by
MRS Delphi Group
MRS Evidence Matters

The Politics of Persuasion

What influences voters and how to improve democratic engagement.


The Delphi Group presents
The Curious Computer
Read views from industry leaders on AI and the future of research.
MRS Curiosity Insight Revolution
70 years of helping people talk to power

The Curious Computer

The impact of AI on the research and insight sector.

MRS Reports/2016
Towards an insight driven organisation
How to create an insight culture that drives business growth
MRS Delphi Group
With a foreward from Professor Patrick Barwise
MRS Curiosity Insight Revolution
70 years of helping people talk to power

Towards an Insight Driven Organisation

The people, skills and processes that enable insight to drive business growth.

MRS Reports/2017
Prediction and planning in an uncertain world
How insight and research can help organisations connect with the future
MRS Delphi Group
With contributions from Twitter, Kantar TNS and ABA Research
MRS Evidence Matters

Prediction and planning in an uncertain world

How insight and research can help organisations connect with the future.

MRS Reports/2018
Great expectations
How technology impacts consumer trust
MRS Delphi Group
Includes new research from Kantar TNS
MRS Evidence Matters

Great Expectations

How technology impacts consumer trust.