3.5 Trust and Trustworthiness

Organisations seek to build trust in data use. This is increasingly about being more 'trustworthy', which is focused on being truthful and more transparent.

In the workshops around the world, there was a widespread sense that very few organisations, if any, can be trusted with data. Indeed, just as increasing levels of trust are needed, apart from some nations where trust in government remains high, the sense from most discussions was that levels of trust are in decline. The emerging challenge for organisations, policy makers, and regulators is, what does it take to demonstrate trustworthiness? On what basis can/should organisations be trusted with data?

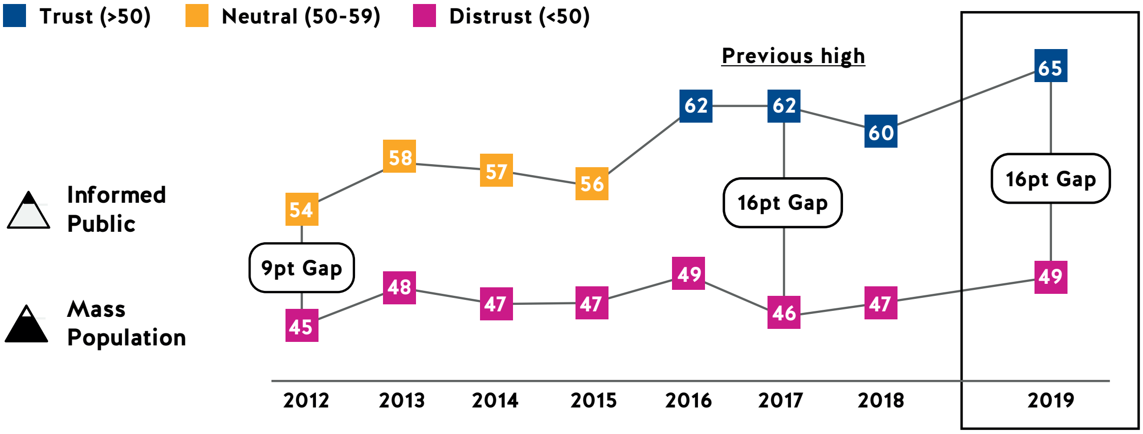
Context

Trust is an economically potent force. When people trust each other, the costs of doing business fall (as less time and effort is spent negotiating, manoeuvring, strategising, monitoring, policing, and enforcing), while opportunities open up, because people are more willing to work and co-operate with one another, including sharing data. Likewise, low trust environments tend to create high operating costs (because of all that time effort invested in negotiating, manoeuvring, strategising, monitoring, policing, and enforcing), while opportunities close down as fewer people are prepared to risk working with others, or for example, to share data with them.

> "As concern around security continues and the confidence of African developers increases, there is growing appetite for Ivorians to look after the data they produce and become less dependent on western (or other) nations."
>
> Abidjan workshop

Globally, our workshops took place at a highly particular time: the Cambridge Analytica scandal was unfolding with clear impacts on the degree to which users trusted, not only Facebook with their personal data, but also organisations more widely, as questions were raised about the tech sector as whole. As one student put it, Facebook, Amazon, and Uber are all *"brands that we trust less than we used to."*[16]

The 2019 Edelman report found there is a wide gap between the more trusting informed public and the far-more-sceptical mass population, marking a return to record highs of trust inequality. The phenomenon fuelling this divide was a pronounced rise in trust among the informed public. Markets such as the U.S., UK, Canada, South Korea and Hong Kong saw trust gains of 12 points or more among the informed public. In 18 markets, there is now a double-digit trust gap between the informed public and the mass population



Edelman Trust Barometer (2019)

The Trust Divide: There is a 16-point gap between the more trusting informed public and the far more sceptical mass population, marking a return to record highs of trust inequality

This specific context added another layer of controversy to an issue which is already extremely complex. When it comes to trust, there are many dimensions to consider, such as:

- **Trust in who?** Are we talking about trusting big businesses, small businesses, national governments, supra-national organisations, or citizens? Each of these has different relationships with each other. Whether or not customers trust companies, or citizens trust governments may throw up very different issues and dynamics to regulators trusting/not trusting global companies, or global companies trusting/not trusting politicians.
- **Trust to do what?** We may have 100% trust in someone's capability and competence, but 0% in their motives, or vice versa. There may be multiple boundaries, where we trust a party within a certain range of constraints, but not beyond them.

Within this context, what it takes to earn and keep trust can differ greatly from situation to situation. Further complications arise from the dynamics of how trust works.

One of these complications is the relationship between trust and transparency. If one party isn't aware of another party's actions, their trust levels may be high, but misplaced. In such cases of 'ignorance is bliss', trust levels can fall precipitately as people are shocked to discover the truth. A climate of mistrust and suspicion can then set in, as the pendulum swings the other way, so that even good, trustworthy actors are not given the benefit of the doubt.

A common, but mistaken, assumption is that changing levels of trust translates directly into changing degrees of behaviour - for example, willingness to share information. However, multiple factors can intervene to break this connection. For example, one party might not trust another, but still feel they have to share information, because otherwise they would forfeit access to a service. In such circumstances, actors that are not trusted (and who may indeed be untrustworthy) are not directly 'punished' for not being trusted. The proliferation of new technologies such as the Internet of Things (IOT) and Artificial Intelligence (AI), may mean that for simple operational reasons, whether they like it or not, citizens will be obliged to 'trust' more.

> "We need to recognise that data is not truth; it just presents information in different ways. We must learn to recognise bias or lose our freedom of choice."
>
> Madrid workshop

Sometimes trust is bilateral: it's all to do with whether Party A trusts Party B to do something specific. But sometimes it's general: for example, a sense that 'no one out there can be trusted'. These different dynamics generate different behaviours. Levels of bilateral trust can influence whether and how two parties deal with each other. A general sense that 'no one can be trusted' is more likely to increase pressure for 'system-wide' political or regulatory interventions.

Issues and questions such as these came up time and time again in our workshops around the world. For example, there was widespread suspicion of the motives of some Big Tech companies and their desires to monetise data (Edelman's 2019 Trust Barometer shows that more than 60 percent of respondents, globally, believe "tech companies have too much power and won't prioritise our welfare over their profits").

There were also strong differences of opinion as to who is trustworthy: some cultures trust 'government', but not 'big business'; in other cultures, most noticeably in the US, it is the opposite. This is in stark contrast to attitudes in some parts of Asia, particularly Japan and Singapore, where there is confidence that the majority of government operates in the best interest of its citizens - but less confidence in business to behave in a similar way. The same is true in Canada and Scandinavia. Across Africa there was widespread acceptance that corruption is rife – both in government and in the private sector; trust there is effectively absent. (One issue this throws up, as we'll see later, is that in Africa, it's common for many individuals to lie when asked for data, creating a significant knock-on effect relating to the trustworthiness of data that is collected.)

What We Heard

Although there was widespread excitement about the way data is transforming society, and recognition of the multiple benefits this brings, some in our workshops expressed caution. There were fears that the mere fact that data is becoming so ubiquitous means that we will trust it too much and fail to question its accuracy or its provenance. *"We need to recognise that data is not truth; it just presents information in different ways. We must learn to recognise bias or lose our freedom of choice."* This was the view in Madrid, where participants argued that the issue is, in a way, "over-trust," as there is a growing disconnect between our dependence on data to manage our lives and our understanding of the ways it can be interpreted. They suggested that the public risks becoming increasingly vulnerable to exploitation both by political and commercial actors; *"increasingly data will be used to control emotions, particularly amongst the young and the susceptible. Brands and governments will be keen to exploit this, to exercise new ways of influencing consumers."*[17]

"Low levels of trust in government, institutions, and Big Tech, devalues data by making databases unreliable. Citizens are choosing not to share accurate information."

Washing DC workshop

This is all well and good if organisations behave responsibly, but if there is a *"trust Chernobyl"* [18] trust between is broken , the consequence may well mean that people are no longer prepared to share their personal data and are less likely to believe the information they receive from government or other organisations. *"It will be interesting to see to what extent we allow our intimacy to be breached (health, financial, personal information)."* [19]

In general, our conversations around trust were divided in two ways; trust in the management and control of data, and trust in the accuracy of data.

Who can we Trust?

In Madrid, it was observed that our increasing familiarity with technology and growing confidence in our ability to access data is re-shaping how we trust – rather than refer to an expert, for example, we use crowd-sourced data to make a broad range of decisions, from where to eat, to treatment recommendations. At the same time, the popularity of social networks has changed who we trust. *"We have seen the transition of power from nations to corporates, and now it is from corporates to the people."* Certainly, throughout our conversations there was a sense that trust has shifted to greater confidence in peer groups or communities, rather than in traditional institutions or in those of a supposedly superior status. Many who are searching for reliable alternatives to traditional trusted sources of news and information are going online to use social media and a network of "friends" or opinion-sharing communities to find what they believe to be true.

Cultural differences are also important when considering who to trust. In Abidjan, lack of trust in the intentions of Western organisations is galvanising support for the Communauté Economique des États de l'Afrique de l'Ouest (CEDEAO). This has coincided with increased confidence in the ability of African technology skills, *"As concern around security continues and confidence of African developers increases, there is growing appetite for Ivorians to look after the data they produce and become less dependent on Western (or other) nations."*

"Big data and AI provide a huge opportunity for intended and unintended discrimination."

Bangalore workshop

Inaccurate Data

Many workshops felt that trust in data that is publicly available and free to use is declining, because it is increasingly difficult to discern if the information that we are presented with is, in fact, accurate. This is true both for government data and also for information received on social media. There was acknowledgement that distinguishing truth on social media channels is particularly challenging, as it is often difficult to identify the original source for a post or news item. Given this, the recommendation from Hong Kong was that citizens need to become more adept at understanding what is factual and what is not; *"there is a need to recognise that data is not truth, it just presents information in different ways and we must learn to recognise the bias, or lose our freedom of choice."* Failure to ensure citizens have the sufficient skills to distinguish fact from fiction has the potential to lead to a breakdown in trust, and could potentially lead to disturbance and even civil unrest; *"there is a feedback loop – fake data leads to low trust leads to fake data. There are diminishing returns, and trust needs to be maintained in order to ensure a safe and successful society."*

The potential negative feedback between lack of trust in government and government's subsequent ability to provide trustworthy data was highlighted in a Washington DC discussion of people deliberately providing false information. The example given was about research into US Census data, which suggests that around 20% of the information given is false, because citizens do not trust government not to use the data against them. A comment was: *"low levels of trust in government, institutions, and Big Tech, devalues data by making databases unreliable. Citizens are choosing not to share accurate information."*

We heard the same in Lagos, where we were told that such is the level of distrust in both the national government and the private sector, that citizens are unwilling to share their personal data with anyone – this in turn renders government statistics so inaccurate that they are rendered almost useless for meaningful analysis. One suggested solution to this was to implement robust regulation around the collection and use of public data. *"Improved data policies will improve trust in government – currently there is limited trust, because there is limited accountability."* [20] However, certainly in Nigeria, there was little hope that this could be implemented any time soon.

Concern was also expressed on growing reliance on AI, especially relating to the delivery of government services. Workshop participants were particularly concerned about programmers' ability to exclude bias in the selection of data used to train AI, or indeed identify it quickly should it occur. In Bangalore for example, it was felt that *"Big data and AI provide a huge opportunity for intended and unintended discrimination."* In Johannesburg the view was that if pubic concerns around data bias grows, there is a chance that they will no longer trust the products and services that are delivered, and certainly would not wish to participate in sharing their personal data. To address this, it was suggested that data should be labelled with, *"data dignity metrics," which could be used to measure and monitor the use of data for the common good, while maintaining the "dignity" (appropriate levels of privacy, for example) of individuals."*

Irresponsible Use of Data

The main actors in the data-driven economy, large tech firms and governments, were both widely criticised in our workshops. Time and again we heard discussions on the way that the many technology firms, particularly social media companies, exploit the data that we share, with little regard to personal safety or privacy. Few believed that lessons had been learned from the Cambridge Analytica scandal and that in the future we could be more confident in the organisations which have control over our personal data. In Hong Kong, it was observed that *"as understanding of the current Big Tech companies grows, expect more disagreement about their current business models."* In Bogota, they said, *"manipulation of the people will continue."*[21]

In addition, there was clear frustration with what was seen as a lack of leadership within the technology sector. In London, the perception was that it is this that has generated the real crisis in trust; *"it's not a crisis of trust – more a crisis of leadership. We can't impose trust downwards."*[22] The conversation went on to focus on the importance of trustworthy behaviour – and the need to make it accountable, *"…it's about confirmation, not trust."* Similar views were expressed in Singapore and Toronto.

Sometimes we heard debates about national security and the need to protect citizens from bad actors. This mistrust can seep into many, perhaps unexpected, areas. For example, participants in Singapore and South Africa both stated that one reason why DNA data is not shared with the US, is national security.

A number of different alternatives were identified, which could help rebuild trust in the use of data and data organisations. These are some of the solutions:

- **Greater transparency.** In Dakar, it was agreed that the public revelations around data lapses and the exploitation of personal data by some technology companies, have demonstrated a failure of self-regulation. The consequence of this is that *"tech companies will be obliged to be transparent about the data they collect, and the uses they make of it. This will be driven by increasing consumer pressure, and a competitive environment in which transparency and responsible data use become a point of differentiation."* Others agreed; from Madrid to Hong Kong, Singapore to Bogota, it was felt that social media companies in particular, should be more proactive in helping to distinguish between truth and inaccuracies on their platforms. There were numerous examples about how misinformation has influenced behaviours in both rich and poor countries, including overt bias in elections and online scams.

Full transparency may not, however, be a silver bullet; too much information can also be confusing. In London, it was observed that *"full transparency is only really needed if trust is absent. It certainly does not mean a requirement to share mountains of information as a means to ensure ethical behaviour."* In Frankfurt, the view was that as private citizens become aware of just how much personal data about them is being accumulated and traded, the demand for greater transparency will grow, and regulation will likely follow; *"if there is no transparency, it will block acceptance of online services."*

- **More Accountability:** There was universal consensus that greater accountability could increase trust, but there were differences in opinion about how this could be achieved. Ensuring that government data is accurate was of particular importance in the Washington DC, Tokyo, Singapore, Lagos, and Copenhagen workshops. In Lagos, the view was that the only way to achieve this is through open multi-party collaboration. *"Improved data policies agreed by multiple stakeholders will improve trust in government - currently there is little trust in government use of data, because there is limited accountability."* A suggestion from Denmark was that there would be greater public confidence in public institutions if there was *"Data NATO or a UN organisation, which could develop and oversee guidelines, codes of conduct, and shared standards."*

- **Technical solutions:** Some in the workshops suggested that new technologies such as blockchain may go part of the way to providing a reliable safeguard against abuse, and therefore help rebuild trust. In Tokyo, the view was that it *"spreads responsibility and increases trust in the system."* Creating a distributed, immutable record of information — which can never be deleted or modified — would at least provide a degree of transparency. Data could be recorded and distributed in a more transparent fashion, and could not be changed without amending all records across most users. Content creators could use distribution channels that guarantee that their content does not get altered, filtered, or blocked by a third party. Equally, a distribution channel leveraging blockchain could make it more difficult to censor and limit access to information.

> "Improved data policies agreed by multiple stakeholders will improve trust in government - currently there is little trust in government use of data, because there is limited accountability."
>
> Lagos workshop

- **Consumer influence:** In Bangalore, it was felt that regulation has been too slow to control the behaviour of some of the technology companies in their exploitation of data. Therefore, they suggested that public opinion is more likely to drive change in advance of any regulatory response to the decline in trust. *"The public response to unethical behaviour often happens before the law is enforced, or indeed appropriate regulation created,*" and from a personal data perspective, *"growing public understanding of potential harm to the individual will lead to increasing demands for better rights and greater accountability."* Those in Copenhagen built on this idea, suggesting that encouraging greater citizen involvement in monitoring the use and accuracy of data might help build trust. *"Is there, maybe, a role for something like Wikipedia in the mix here?"*[23]

- **Digital literacy:** Many felt that greater public education around the use of personal data would both help to build public trust in open data for public services, and give citizens sufficient skills to be able to identify when that trust could be misplaced. In Santiago, the hope was that recognition of this, alongside some hefty fines, would moderate corporate behaviour; *"when the public is more involved, accountability becomes "horizontal" rather than vertical."* As awareness grows, the ability to *"watch the watcher" and "critically understand"* will mean that large organisations of all kinds will temper their actions and take greater account of what is considered to be acceptable – both off and online.

- **Generational shift:** There was a recognition that trust in technology and the data that it delivers, is dependent on generational expectation. Some, for example, suggest that millennials are much more likely to be data-savvy around security and privacy and so on, than older generations, and may be less likely to be concerned about it. *"Gen X is the last pre-digital generation – the generation after will have better understanding of the importance of management and control."*[24] However, some fear that the next generation will be so dependent on technology, that "any data will be believed to be fact, and its veracity will not be questioned.[25] But we also heard the opposite view; *"in ten years' time, things will be more balanced. We are currently in a transitional phase and in a state of flux – people were scared of the car when it was first invented."*

Looking Forward

Throughout all our workshop discussions, it is clear that we are at a point of transition. Technology innovations, powered in the main by a select number of hugely powerful global organisations, several of which are not widely known, are triggering dramatic changes across all sectors of society, and influencing how millions of people live their lives. Often these changes are for the better, but not always. Such is the momentum, that many citizens feel that these changes are being 'done to them', whether they like it or not. This makes trust all the more important.

Building trust is not one, single challenge. It is multi-faceted. Data-based systems rely on the accuracy of the data that is fed into them. They only work effectively if enough people trust them to share accurate data, and believe in the accuracy of the information that they get in return. When incidents occur which reveal irregularities, corruption, or incompetence, trust is damaged, making individuals less confident about the benefits of participation. The risk is that growing numbers decide to scale back participation, or provide inaccurate data. If enough people do this, the system fails.

This aspect of trust is primarily technical - of creating systems that are fit for purpose. A second, more complicated and controversial dimension of trust relates to the motives and intentions of different stakeholders. The challenge for those organisations and institutions leading the transition to a data-driven economy and society, is to demonstrate that they are *trustworthy.*

Being trustworthy is not the same as being trusted. It means that organisations accept they should be held to account; that they demonstrate that they have 'good intentions'; that ethics are not something to talk about for PR purposes, but actually shape what decisions are made and how they are implemented. Greater transparency helps, but is not the only answer, particularly when trust in corporates is at a low ebb. A robust regulatory framework, either developed globally or regionally, would do much to create standards, along with checks and balances to curtail the power of the large corporates, which many we spoke to felt are still largely unaccountable. Individuals also have a role to play by becoming more aware of their rights and responsibilities online. If successful, and we create a lasting, robust, and trustworthy system, then the next generation can only benefit from its potent force.

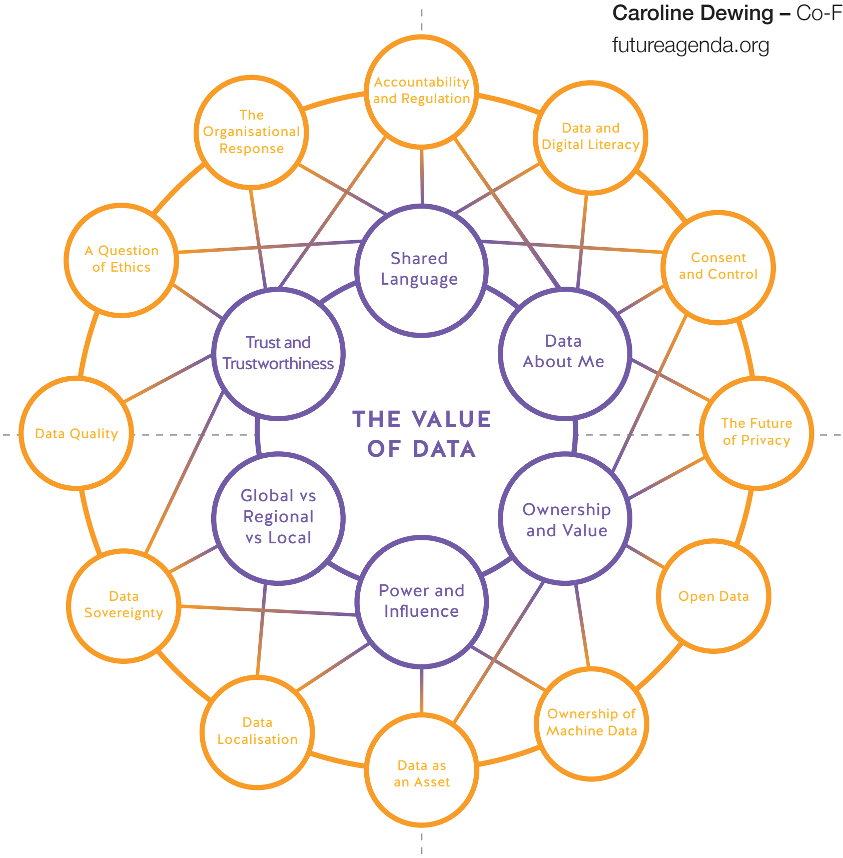
Context

This is one of 18 key insights to emerge from a major global open foresight project exploring the future value of data.

Throughout 2018, Future Agenda canvassed the views of a wide range of 900 experts with different backgrounds and perspectives from around the world, to provide their insights on the future value of data. Supported by Facebook and many other organisations, we held 30 workshops across 24 countries in Africa, Asia, the Americas, and Europe. In them, we reviewed the data landscape across the globe, as it is now, and how experts think it will evolve over the next five to ten years.

The aim of the project was to gain a better understanding of how perspectives and priorities differ across the world, and to use the diverse voices and viewpoints to help governments, organisations, and individuals to better understand what they need to do to realise data's full potential.

From the multiple discussions 6 over-arching themes were identified alongside 12 additional, related future shifts as summarised in the diagram below.



Details of each of these, a full report and additional supporting information can all be found on the dedicated mini-site: www.deliveringvaluethroughdata.org

About Future Agenda

Future Agenda is an open source think tank and advisory firm. It runs a global open foresight programme, helping organisations to identify emerging opportunities, and make more informed decisions. Future Agenda also supports leading organisations, large and small, on strategy, growth and innovation.

Founded in 2010, Future Agenda has pioneered an open foresight approach bringing together senior leaders across business, academia, NFP and government to challenge assumptions about the next ten years, build an informed view and establish robust growth strategies focused on major emerging opportunities. We connect the informed and influential to help drive lasting impact.

For more information please see:
www.futureagenda.org

For more details of this project contact:
Dr Tim Jones – Programme Director,
tim.jones@futureagenda.org
Caroline Dewing – Co-Founder, caroline.dewing@futureagenda.org

Text © Future Agenda
Images © istockimages.com
First published November 2019 by:
Future Agenda Limited
84 Brook Street
London
W1K 5EH