4.2 Culture, Governance and Privacy

Differences in culture and governance drive different attitudes towards privacy. Some believe in the right to data privacy; others see this is a contradictory and outdated concept.

Context

Greater availability and access to data is changing attitudes to data privacy and security. Our workshops revealed a diversity of opinion about this, depending on geography, culture, and age. There were a wide range of views about the definition of privacy itself. Is it about unedifying and unjustified snooping? Keeping potentially embarrassing information private? Threats to civil liberties? Risks arising from the ability to use private information to harm an individual? Our discussions divided broadly between those who felt that privacy is a hard-won human right and should be protected, and those who argued that, in our data driven world, guaranteeing privacy is impractical and may even compromise national security.

The European and international institutions such as the EU and the UN, as well as several governments, are firm believers in privacy as a human right. But not everyone agrees. Conversations in Abuja and Dakar, Tokyo, Jakarta, and Singapore, revealed an ambivalence about the issue. In both the US workshops, there was support for the "third-party doctrine," which has long governed privacy law and holds that there can be no privacy expectation on data that is shared with a third party. In Shanghai, we were told that, although views are changing, privacy is not considered important in China; indeed, there is no direct Mandarin translation - the Chinese word for privacy, yinsi, is mainly associated with secrecy and poor mental health.

As with so many of our discussions, building consensus was complicated by a lack of clarity around language and what privacy really means in practice. The concept is abstract and touches multiple issues, including the implications for national security, the protection of minors, consideration around what are the legitimate boundaries over who has access to and benefits from data, and many highly specific areas about, for example, IOT data or facial recognition. Furthermore, generalisations are unhelpful because privacy is defined by its context. It does not mean absolute secrecy - we share sensitive information with doctors, friends, families - but when we reveal information in one situation, we trust that it won't surprise us in another.

To privacy advocates, there is a growing personalisation-privacy paradox: we want to have products and services that are customised to our needs and actions, but also want our data to be private, shared when we want and only to the actors we authorise for its use. Some people - those who are not privacy advocates - saw 'privacy' as an anachronism – an issue which has been overtaken by events and which maybe didn't matter very much in the first place. Others see it as pivotally important, defining the shape and future of the entire Internet age. Although recent data breaches and the consequent news headlines have raised public awareness around the issue, this has yet to significantly influence behaviour. So, policymakers are faced with a dilemma; should they legislate on the basis of how people actually behave online, apply a set of idealised archetypes, or suggest how they *ought* to behave? The view from our workshops was that, as understanding of just how much of our personal data is traded online increases, there will be greater clarity about what information people are prepared to share, and who to share it with, in exchange for better service or an improved quality of life.

To date, the primary focus for the privacy agenda has been around the exploitation of personal data – the collection, use, and value extraction of data by companies. However, the collection and use of data by governments is a growing issue, particularly as data-driven decision-making, including AI, is being more widely adopted. For governments, provided the right checks and balances are in place, there are huge benefits; it can help to address financial shortfalls and investment needs aimed at improved healthcare, transport systems, and public services, for example. Such is its transformation, some in our workshops argued, that democracies will not only have to collect data for the improvement of public services, they need it to remain competitive. If the West enacts too stringent privacy laws, it will have less data — a key raw material for artificial intelligence — and as a result, will put itself at a competitive disadvantage to the likes of China, where surveillance is becoming pervasive.

"People are prepared to exchange information about themselves for a better life. At worst, they are indifferent. As we share more data, in ten years' time, concerns about privacy will reduce still further."

Tokyo workshop

In some instances, differences in privacy laws are acting as an unintended trade barrier, and restricting innovation. The recent roll-out of GDPR across the EU was, in part, designed to address this. Compliance is not easy. However, it is clear that, for the first time, the hefty fines and associated publicity which is generated from a failure to comply, gives regulators sharper teeth than they have had in the past, and provides companies a compelling reason to assert more control over digital supply chains to better control data flows.[36] Many regulators are keen to learn from the successes and failures of GDPR, and are watching its roll-out with interest.

Generational Shift

Whatever the view today, attitudes to on-line privacy are changing, as the next generation, which has not known life before the internet, matures. This does not mean that we will find alignment. Again, we saw diversity in opinion about how this would play out, as everyone struggles to find a balance between privacy, convenience, and security. In London, it was suggested that, because of the compelling nature of new and enticing data services, there is a strong chance that privacy, as we know it, even in Europe, will no longer be an issue. The workshop in Johannesburg took the opposite approach, arguing that rising data literacy among both citizens and states will lead to greater understanding of the negative consequences of oversharing, and therefore sensitivities about privacy are likely to increase.[37] There was divergence as to how to manage this. Some see that technical solutions such as encryption will ensure that the right to privacy is maintained, but others advocated the need for more transparency so that individuals are more informed, and therefore better able to control how their data is used.

A Global Approach?

The big challenge ahead is whether or not privacy can be addressed via global agreements. There is general acceptance that there is a need for it. As different regions all seek to progress data regulation via the likes of APEC and GDPR, the emergence of a global privacy framework is championed by those looking for better control and greater transparency. The World Economic Forum is just one of several major organisations trying to develop an international, collaborative, global, approach.[38] Key focus areas are on delivering meaningful transparency, strengthening accountability, and empowering individuals. The inventor of the web, Sir Tim Berners Lee, is also working on the issue. He advocates a new "Contract for the Web," which aims to protect people's rights and freedoms. It states that governments must ensure that its citizens have access to all of the internet, all of the time, and that their privacy is respected, so they can be online "freely, safely, and without fear." As Sir Tim himself observes, "no one group should do this alone, and all input will be appreciated."

> "The massive increase in data will enable massive personalisation. There will be no privacy, because of the compelling nature of the services available."
>
> London workshop

Inevitably, not all countries or even states are moving at the same speed and in the same direction, so it is likely that regional regulation will continue for some time. In America, for example, the U.S. Constitution does not contain any explicit protection of privacy, so the judiciary has been searching for ways of connecting existing constitutional protections with the privacy issues of the day, such as the Fourth Amendment's protection against unreasonable search and seizure. Despite calls from a range of CEOs for better policy legislation, the US at a federal level has lagged behind other regions. This might be addressed if other states follow the example set by the recent California Consumer Privacy Act (CCPA). However, the appetite for change may be low; privacy was not seen as a priority for discussion at either of our workshops in San Francisco and Washington DC. This is despite research from the likes of Pew suggesting that US citizens *do* care about privacy, but don't know how to address it.[39]

China and India, each of which have more people online than either Europe or America have citizens, have diverging and contradictory approaches to privacy. Interestingly, India, one of the world's most populous countries, has taken a somewhat contradictory approach to privacy legislation. It recently announced a draft data protection bill. Companies and the government must generally abide by legal principles similar to the EU, and as with GDPR, this law would apply to all entities, everywhere, that process Indians' data. At the same time, it is also supportive of data localisation, and mandates that Indians' data should remain within national boundaries. It has also proposed Chinese-style rules to extend the state's surveillance powers. In March 2019, the government put out a draft ecommerce policy, arguing that the personal data of Indians should be treated as a 'national' asset.[40]

In China, although the law did not even define what counts as personal information until 2018, there is increasing clarity around security obligations and responsibilities, due to public concern about the impact of data theft, and the ambition of Chinese companies such as TenCent and Alibaba to enter Western markets. This sits uncomfortably beside the government's appetite for surveillance, which has led to a tightening of data protection rules for companies, while making it easier for the state to capture more private information.

Given these complexities, it is unsurprising that some see that companies are using privacy issues for competitive advantage. Apple's 2019 marketing campaign launched at CED in Las Vegas, includes a major privacy pitch, "What happens on your iPhone, stays on your iPhone." Recently, Facebook promised that the content of all messages will be encrypted, regardless of the platform they are on.

"Nigerians are not confident about privacy, which is why many protect themselves by having an online alias - this guards them from interest groups and government surveillance."

Abuja workshop

What We Heard

Changing Attitudes to Privacy

Our workshops revealed that national attitudes towards privacy varied dependent on the levels of trust . In Tokyo, we were told that *"people are prepared to exchange information about themselves for a better life. At worst, they are indifferent. As we share more data, in ten years' time, concerns about privacy will reduce still further."* In Jakarta, they said, *"Indonesia is a very sharing country – across all cultures and all demographics, and also culturally, Indonesians are inclined to overshare."* In Africa, there was a similar response. In Dakar, for example, it was noted that *"in Europe, privacy is a big concern. There are historical reasons for this. We are a more open society."* In contrast, in Lagos, we heard that *"Nigerians are not confident about privacy, which is why many protect themselves by having an online alias - this guards them from interest groups and government surveillance."*

Some suggest the concept of privacy is losing its appeal. In London, one suggestion was that that *"the massive increase in data will enable massive personalisation. There will be no privacy, because of the compelling nature of the services available without it."* It was also pointed out that accepting this will take time to become culturally acceptable; *"change will be slower than expected. We are high on the hype cycle for data. Some realism around its limitations will emerge."* In Manila, it was observed that this sort of behaviour by corporates and the very wealthy could *"lead to an economy of scarcity around data. How we manage privacy in the digital age, therefore, will be a key determinant of the future value of data."*

Whatever the view today, attitudes to on-line privacy are changing, as the next generation, which has not known life before the internet, matures. Again, we saw diversity in opinion about how this would play out. In London, it was suggested that privacy as we know it will no longer be an issue. Because of the compelling nature of the services provided, there is a strong chance that *"society will have ownership of everyone's data."* They disagreed in Bangalore, where it was said that *"privacy will become more of a public issue. There will be growing concern around state surveillance and how to minimise the harm of governments having access to "all" data."*

> "How we manage privacy in the digital age will be a key determinant of the future value of data."
>
> Manila workshop

Regulatory Choices

There are huge benefits of sharing data to improve the workings of financial shortfalls and investment needs aimed at transport systems and public services. But still, the danger of excessive surveillance is worrying for many. Although technology itself is agnostic, without the right checks and balances, it can still be used to cause harm. In Dakar, it was said, *"there should be clear rules on which data is collected and for which reasons. We need ways to protect vulnerable people."* For example, although law enforcement officials around the world can use AI to identify criminals, it can also mean that they (or others) are able to eavesdrop on ordinary citizens. Both the China and the US governments are introducing facial recognition to track their citizens. Some consider this to be a step too far.[41] Many argued that new, globally agreed principles will be needed to ensure consensus on what degree of monitoring is reasonable. In Jakarta, the suggestion was that *"if we have or hold data, we can't shy away from responsibility, but we need a globalisation of data framework."*

The big challenge ahead is whether or not privacy can be addressed via global agreements. There is general acceptance that there is a need for them. In London, the assessment was, *"today we have a patchwork of data privacy laws, but data flows globally. We will need to see global privacy principles."* As different regions all seek to progress data regulation, the emergence of a global privacy framework is championed by those looking for better control and greater transparency. In Bangalore, it was observed that *"the creation of a world data council may facilitate international negotiations. Currently, there is little consensus around data sovereignty – cultural differences around privacy, just one example."* But who, or which organisation, will be trusted, and able to take the lead on this? As attempts at Internet governance have shown, creating a supranational entity is challenging, owing to conflicting political imperatives and competing commercial interests.

Many within our workshops believe that GDPR has set the standard which others should follow.[42] In Mexico City, the view was that *"there are already some global standards, and some nations are already acting transnationally. GDPR is having impact beyond European boundaries."* In Nigeria, just one of many cases, it is seen that *"GDPR will change the data landscape and bring in new standards. It offers a template for localised legislation, and has highlighted some of the key issues around data that are not yet a priority in Nigeria, but will increase in significance over the next decade."*

> "Today we have a patchwork of data privacy laws, but data flows globally. We will need to see global privacy principles."
>
> London workshop

Across Australia, Asia, Africa, and South America, we consistently heard 'GDPR-lite' as the shorthand for what was needed locally as well as globally. Similarly, in Jakarta, the perspective was that *"there will be an Asian alternative to GDPR, driven by Asian ethics and principles."* These may, for example, be less focused on the individual. Across Africa, there was also interest in developing locally relevant regulation. In Lagos, a thought was that, with slow progress to date, moving ahead, *"the private sector will put pressure on government to ensure that there is clear legislation around accountability, and demand the creation of a Nigerian Data Protection Policy that reflects the same principles as those articulated in GDPR."*

Implications for Data Value

Global consensus on what are appropriate levels of privacy is still out of reach – and current views are often defined by culture. However, with common frameworks now being adapted and adopted for several different regions, the potential for some alignment is emerging. While several believe that privacy will not be an issue in the longer term, most agree that for the next decade, particularly for multinationals and many of the more democratic governments, it will continue to be a primary concern. With privacy also now being used as a source of competitive advantage, and used as a mechanism to build trust and credibility, several companies are trying to use it as a point of differentiation.[43]

"There will be an Asian alternative to GDPR, driven by Asian ethics and principles."

Jakarta workshop

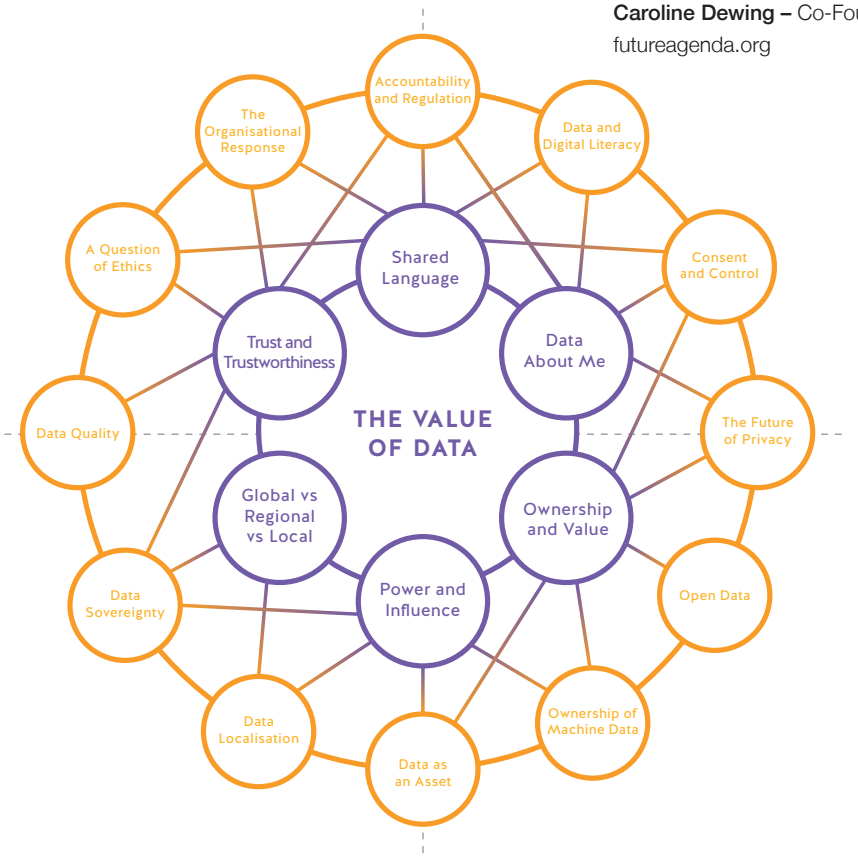
Context

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

First published November 2019 by:
Future Agenda Limited
84 Brook Street
London
W1K 5EH