WORLD ECONOMIC FORUM

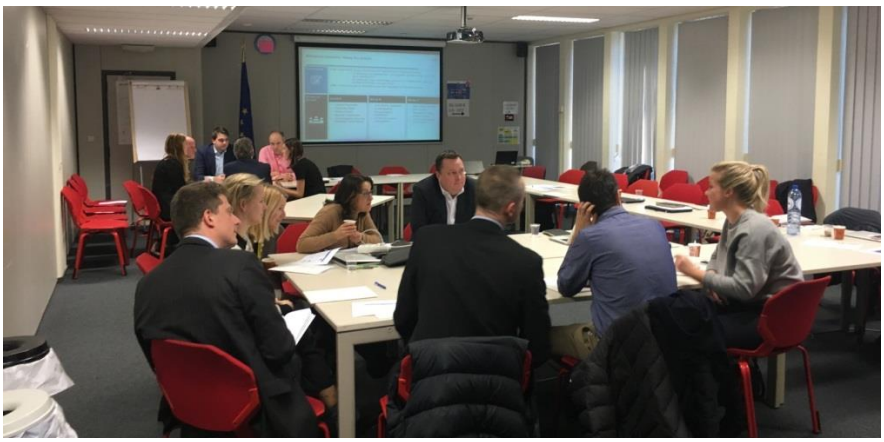
COMMITTED TO IMPROVING THE STATE OF THE WORLD

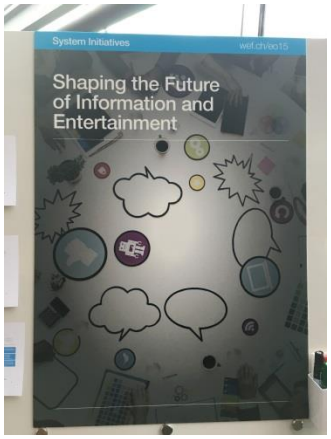
Meeting Summary

Shaping the Future Implications of Digital Media for Society

Rebuilding Trust for a Sustainable Media Environment

28 November 2016, European Commission, Brussels





Introduction

On 28 November, 2016, the World Economic Forum hosted an interactive, half-day session on the topic of building end user trust in digital media. This event was the second of two workshop-style meetings held as part of phase 2 of the project *Shaping the Future Implications of Digital Media for Society*.

Participants joined from three sectors – business, government, and civil society / international organizations – to address a critical question: **how can industry and policy-makers address tensions to build a quality media environment?** After a brief presentation, focused on framing the issues and providing insight from the Forum's primary research into this topic, the attendees spent the afternoon sharing their thoughts, through a series of break-out sessions and roundtable discussions.

The meeting had three objectives:

1. Establish a common understanding of the state of tensions in the use of digital platforms and services, including deficits in end user trust, their causes, and the importance of addressing them.
2. Develop actionable recommendations for closing widening gaps in trust between key stakeholders. What adjustments can industry make to increase the economic and social sustainability of digital media service and platform use by end users? How can the end user community contribute to these outcomes?
3. Begin to build momentum for greater collaboration between policy makers and industry in the conversation on resolving areas of tension between end users and industry. What is the range of approaches for policy to proactively nurture – rather than reactively enforce – positive consumer-business relationships? For example, is more industry self-regulation required?

The remainder of this document is a summary of the key issues, experiences, insights, and other points of discussion that surfaced throughout the day.

Overall insights

Existence of a trust deficit: There are clear signs of tension in digital media use – for example, 47% of German respondents in a new survey conducted by the Forum say they have avoided or stopped using a service because it did not provide enough control over their personal data. This type of end user behaviour is underlined by a deficit in trust – over 60% of German respondents do not trust their main service providers to define fair terms and conditions around personal data. Dissatisfaction with end user controls provides further evidence for – and may even contribute to – the trust deficit. 48% of German respondents don't trust that end user controls work the way they are supposed to. Regardless of levels of trust and controls, the results of the survey suggest that most German end users are simply not comfortable with their data being collected, stored, and used. A related finding from the survey is that up to half of people may lack basic digital media literacy – this could be "low-hanging fruit" for improving trust.

Nature of the trust deficit: The trust deficit is complex and is not yet universally accepted as a pressing issue. While it is clear that end users have multifaceted concerns about their data and privacy, these are not always reflected in their actual behaviour. Some meeting participants see this as a reason to do nothing; others see this as proof that something must be done to protect users. Several factors, ranging from human psychology, to levels of digital media literacy, to the diversity in individual levels of trust, are likely at play.

Causes: Trust can suffer when data collection is viewed as unnecessary or intrusive relative to the benefit being provided. Trust also suffers from a lack of transparency, and regulations that require lengthy and technical privacy policies do not generally empower end users.

Risks: Conventional wisdom says that irresponsible companies risk losing business, and responsible companies risk being caught in the crossfire. However, there is not always a visible, lasting financial effect in the wake of a security or privacy breach. To understand risks to companies, we must understand the value of privacy to individuals – privacy is not just about hiding "bad" things; it is also about protecting individual liberties.

Roles of stakeholders: All types of stakeholders, including industry, governments, and civil society, have several roles to play. Companies, for example, can foster trust by first establishing a set of principles that galvanize an internal commitment to end users. Civil society can help by educating citizens, providing expertise to companies, and acting as a check and balance on industry practices. Governments have several roles to play, and should not just act as legislators.

Multi-stakeholder collaboration: There may be value in having an international body, made of diverse stakeholders, focused on setting best practices for personal data collection and management, fostering adherence, and providing resources and tools to member organizations. However, it is not clear that a single, comprehensive body is the right solution; competing approaches and viewpoints may produce better results for society. There is also a need to better harness the insights from existing multi-stakeholder discussions to accelerate progress.

Challenges to overcome: The importance of the trust deficit must be made clear to all stakeholders, given competing priorities that can have more immediate and visible impacts to industry and society. When designing solutions, it is important to anticipate the evolving implications of personal data for end users, because today's consequences may not reflect the innovations of tomorrow.

Digital Media Literacy: Two out of three breakout groups suggested multi-stakeholder approaches to raise levels of digital media literacy among end users. The challenge is that meaningful gains in this skillset are only achieved in the long term; however, digital media literacy is a key lever to have impact on trust.

Roundtable 1: The trust deficit

Nature of the trust deficit

Some participants, especially from industry, expressed skepticism about the utility of self-reported levels of end user trust. What ultimately matters to companies is how users behave when presented with a choice: what are they willing to give up for more privacy? For example, there are search engines that do not store any data; they end up being worse search engines and fewer people use them.

Others observed that civil society tends to be concerned by *excesses* of end user trust, in contrast to the *deficit* revealed by the Forum's research. For example, half of the people in the UK think that Google is a reputable source of information (despite it not being a source of information at all).

On the surface, trust appears to be a paradox. End users say they have concerns about personal data collection, storage, and use, but this can be hard to discern from their use of services, and they may sometimes act in a way that is arguably too trusting (i.e., naïve). One explanation for these inconsistencies between what end users say and do is that they are simply "lazy" or otherwise subject to the flaws of human psychology. An alternative interpretation is that those who harbour a general sense of mistrust towards their services lack the digital media literacy needed to act on it in specific situations. Digital media literacy includes being sensitized to the consequences of personal data collection and the knowledge and skills to do something about it. Another factor to consider is that not all end users are the same – on the individual level, the most distrusting end users, and the most trusting end users, might both be acting consistently with their attitudes.

For the purposes of this topic, the consumer and the end user are two different concepts. Consumers proactively seek knowledge about what they consume. On the other hand, most end users spend less effort on understanding the implications of a service, so they do not fully know what they are signing up for. Is *end user* protection needed even more greatly than *consumer* protection?

When thinking about personal data, it is helpful to use an established taxonomy, such as personally identifiable information (PII), non-identifiable information, and aggregate level information. However, end users may be skeptical about the privacy of "non-identifiable" information, given that data from different sources can be matched to reconstruct an individual's identity.

Causes

From an end user viewpoint, data collection is inherently neither good nor bad. The use of data collection can be

something positive as long as end users see a benefit, but becomes a negative as soon as it is seen as intrusive (e.g., unnecessary to provide the benefit in question).

Terms and conditions are drawn up "by lawyers, for lawyers" (specifically, privacy professionals), and the reason is because of regulations that require it. Regulations are messy, and this is reflected in the disclosures in privacy policies. Regulations can also have unintended effects; for instance, consider a regulation requiring a company to say upfront that it may use location data at some point and asking for consent. This could actually be less informative than saying nothing upfront, and then asking for permission to use this data only when it is needed.

Risks

To understand the risks to business, we first have to understand the importance of privacy to the individual. 40% of the internet is the "dark side" that nobody talks about in these forums. People visiting poorly governed websites or illegally downloading movies have good reason to be concerned about their data. However, privacy is not just about hiding bad things, but it is also about protecting users' freedom to do good things – similar to how you should care about protecting freedom of expression, even if you are not being oppressed.

Responsible companies use consumer data to hold onto their consumers; companies that are not as careful, risk losing business. However, some observers challenge this conventional wisdom. The infamous Target credit card data breach has not had any visible, lasting, financial effects on the retailer. Is this further evidence of a discontinuity between what consumers do and what they say? Is this evidence that consumers have sufficient recourse in the event of credit card fraud?

If some organizations act in an irresponsible manner, could responsible organizations be negatively impacted? End users are at an information disadvantage and often cannot tell the difference between such companies – actions by one company may colour perceptions of other companies in an industry. Besides industry, another factor to consider is geography – for example, companies operating in certain developing markets have access to data that would be considered taboo elsewhere.

Solutions

Providing end users with something of value in exchange for data can help to earn their trust. For this to work there must also be clear awareness of the value provided and how it flows from any data shared. A recent study attempted to quantify the value of free services to consumers in monetary terms. Some would like today's free model to be replaced with a paid model to facilitate small player market entry and reduce network effects. A related, but distinct, approach is to ask end users to pay for their privacy. This is controversial as it risks turning privacy into a luxury good.

One participant noted that there is considerable scope for platform governance to evolve and levels of transparency from business to improve.

To educate people about privacy, they must be reached at the right time and in the right way. This is necessary because people using a platform are not online in order to learn about privacy; they are using the service for other reasons. An example of reaching people at the right time is flagging the privacy consequences of an action when a user decides to update their privacy controls for the first time, and offering to provide more information. Regulations that require blanket notifications are not aligned with this principle of targeting users when they are likely to be most receptive to privacy related information.

It was noted that the principle of targeting users at the "right time" risks being seen as disingenuous, because it can be applied to selectively provide information and choices when users are more likely to comply with a request to share their personal data.

There is an existing initiative that convenes industry leadership in the UK to examine trust around data. However, this type of forum does not bring together diverse stakeholders – "If it's 100% industry driven, end users won't trust us." Similarly, it was noted that people do not trust governments either – collaboration among different stakeholder types may help to create trust.

One participant noted that one way to empower citizens is to "teach them to *distrust*" – for example, teaching critical thinking skills can help people to avoid being stuck in a filter bubble.

Breakout session: Ideas for action

Industry

What is their role and what can they do?

Companies cannot build trust externally until they have their house in order internally – as a company, you truly have to believe you are doing the right thing. This can be achieved with sound principals-based internal policies and processes. Once principles are set on what will be done with consumer data, they must be communicated to consumers in a very simple way.

Ideas for multi-stakeholder collaboration

More alignment between industry and government is needed to successfully integrate regulation. In the short term, changes must come from industry; these could initially be supported by some principles or a regulatory framework. Longer term, more extensive regulation would follow, building on the initial principles or regulatory framework.

The "Big Brother Awards" focus on which company is worst in terms of abusing personal data. Having a positive award (e.g., who has been positively empowering end users with more control over their personal data?), instead, would help to foster a more constructive conversation that collaboratively engages industry.

Personally Identifiable Information (PII) is the most dangerous form of data, despite what people may think. Many end users are not concerned about providing their name and address – but these identifiers can be used, for example, to license other data from credit bureaus and build a deeper customer profile. Non-personally identifiable information is also dangerous, because it can sometimes be traced back to a user's identity when matched with other data. Is there a need to regulate how PII is matched?

Civil society and IOs

What is their role and what can they do?

Civil society and International Organizations have three roles to play: (1) end user education – helping people understand so they can make the right choices; (2) expertise – helping companies to develop business practices and policies that are both legally compliant and that take into consideration the ethical consequences of the way they set up services and products; and (3) "policing" – exposing

companies that misuse and abuse data, whether by doing things that are unethical or illegal.

The OECD was one of the first organizations to work on internationally acceptable privacy principles. There is precedent for civil society as a convener that brings together regulators, companies, and end users for multi-stakeholder discussions. Already, there are people working on all of these ideas, but there is a need for more work to be done. What can we do to get more out of the conversations that are already happening? There is a need to better collect and harness the insights of existing work in order to accelerate learning and impact on society.

Ideas for multi-stakeholder collaboration

It might be better to have multiple forums, instead of a single comprehensive collaboration in which this happens. Having competing initiatives and perspectives could be a good thing for society. Further, there is a tendency in multi-stakeholder forums to have multiple debates happening at the same time – keeping separate forums would help to separate the issues.

Government

What is their role and what can they do?

The basic roles of government should be to (1) create principles and foster incentives, (2) be open to small experiments and have a testing mentality, (3) promote benefits and success stories of trust in media, (4) legislate and enforce existing legislation, and (5) engage in nudge strategies for citizens (e.g., where terms and conditions are hard to understand).

Governments should aim to create an environment that promotes transparency and disclosure through a proactive approach that includes highlighting success stories and leading by good example.

Governments should also use their convening power to engage in "unsiloed global conversations," because the nature of these platforms is that they do not stop at jurisdictional borders.

Proprietary or emerging practices (e.g., derived data, by definition, is a "black box" to the end user). Further, in some cases, the information that is out there is too abstract, fragmented, or technical for users to act on.

Is the government well placed to provide lessons on digital privacy? Some age groups are too young to be reached, and others are too old. Rather than focusing solely on education as a way to get this right, governments can focus on creating the right systems to promote transparency, etc.

Governments should avoid inadvertently causing digital exclusion. The goal is to be an agile government that tries not to stop transformation and development.

Roundtable 2: Collaborative solutions

There are existing privacy certification schemes that companies can pay to join, but these are not yet widespread. End users do not know which ones are the best, and are often not aware of them in the first place.

In general, the right multi-stakeholder approach can work, if correctly designed and scoped and supported by the right constituents. It might be valuable to have an "international *body*" (not an "international *organization*") focused on good personal data management conduct.

The role of such a body could be to define the right set of practices, and act as an incentive mechanism to ensure they are followed. The practices must be easily understandable – e.g., not written "by lawyers, for lawyers." Rather than playing a proactive enforcer role, it could be a body where users or members can file complaints. There is precedent in advertising for a self-regulated complaint process.

The role of such a body need not focus only on compliance activities, which can reinforce a "bad data" narrative. It could also be a platform to promote shared investment in developing tools and resources that could be deployed by many players to improve trust. For example, in response to EU data protection laws, Google asked users to complete a simple tutorial (an introduction to MyAccount) that walked them through key points of its privacy policy. Even though the primary purpose was not to educate and build trust, it had that impact on some users. If this type of measure were standardized and

It is important for any efforts to anticipate the changing implications of personal data for end users. For example, the nature of "data monetization" is sure to evolve. Today, data monetization is all about serving targeted ads, which an

delivered proactively by multiple platform companies with the primary purpose of promoting trust, it could be even more effective.

Tackling personal data and privacy issues will continue to be an uphill battle, for several reasons.

- First, data privacy is perceived by some industry players to be a niche issue. This is in contrast to internet protocols, where there was a clear incentive to address challenges because they were necessary for the internet to function. Convincing industry players that there is some sort of bottom line impact is the key enabler to get them behind improving platforms in a manner that increases trust from end users
- Second, ethics and values around data vary by geography, while data is not constrained to national boundaries
- Third, in the case of artificial intelligence, many participants have said it could be worse than nuclear weapons, but even then, organizing to address issues is difficult

One participant raised the point that the asymmetry of knowledge is a core competitive advantage of many companies, and argued that we should not expect them to see value in voluntarily increasing their transparency or changing their practices. If true, this means that there are only two basic levers for progress: either (1) improving literacy and awareness of end users, which is a lengthy process and may leave out some segments, or (2) enforcing transparency and responsible practices through regulation or self-regulation according to a set of standards. The latter may be the most effective, because in the end, human psychology has its limitations.

If sufficient information is publicly available to end users, can we say at some point that it is the fault of the individual for not taking responsibility for their actions? Some believe that sufficient information is available to end users for them to make informed decisions; others believe that there are gaps in information with respect to

individual can arguably choose to ignore. How will data be monetized tomorrow – and will end users be empowered to manage the consequences?

Appendix: List of participants

Organization	Role	Country
Civil society and International Organizations		
ALLIED FOR START-UPS	Director of European Affairs	Belgium
CENTER FOR DEMOCRACY & TECHNOLOGY	Director, European Affairs	Belgium
INTERACTIVE ADVERTISING BUREAU	European Public Policy Manager	Belgium
WORLD BANK	Lead ICT Policy Specialist	Belgium
Industry		
UNILEVER	CMI VP, Global Head of Data and Marketing Analytics	UK
360 AGENCY BERLIN	Partner	Germany
VIMPELCOM	Director of Government Relations	Netherlands
MCKINSEY & COMPANY	Associate Partner, High Tech, Media, and Telecom Practice	UK
DENTSU AEGIS NETWORKS	Strategy Partner	UK
NIELSEN	VP Government Affairs and Privacy	Belgium
FACEBOOK	Managing Director for EU Affairs	Belgium
Public sector		
EUROPEAN COMMISSION	Policy Officer, Media convergence, DG Connect	Belgium
EUROPEAN COMMISSION	Senior Policy Officer	Belgium
EUROPEAN COMMISSION	Policy Officer	Belgium
EUROPEAN COMMISSION	Team Leader, Converging Media and Content, DG Connect	Belgium
EUROPEAN COMMISSION	Policy Officer, Regulatory aspects for culture in digital policies, DG EAC	Belgium
EUROPEAN COMMISSION	Policy Officer, Union citizenship rights and free movement, DG JUST	Belgium
EUROPEAN COMMISSION	Deputy Head of Converging Media and Content, DG Connect	Belgium
EUROPEAN COMMISSION	Policy Officer, Hate speech in AVMSD, DG Connect	Belgium
EUROPEAN COMMISSION	Policy Officer, Electronic Communications Policy, DG Connect	Belgium
EUROPEAN COMMISSION	Legal Officer, Media literacy, DG Connect	Belgium
EUROPEAN COMMISSION	Policy Officer, Media Freedom Team, DG Connect	Belgium
EUROPEAN COMMISSION	Scientific Policy Officer, Investment in High Capacity Networks, DG Connect	Belgium