WORLD ECONOMIC FORUM

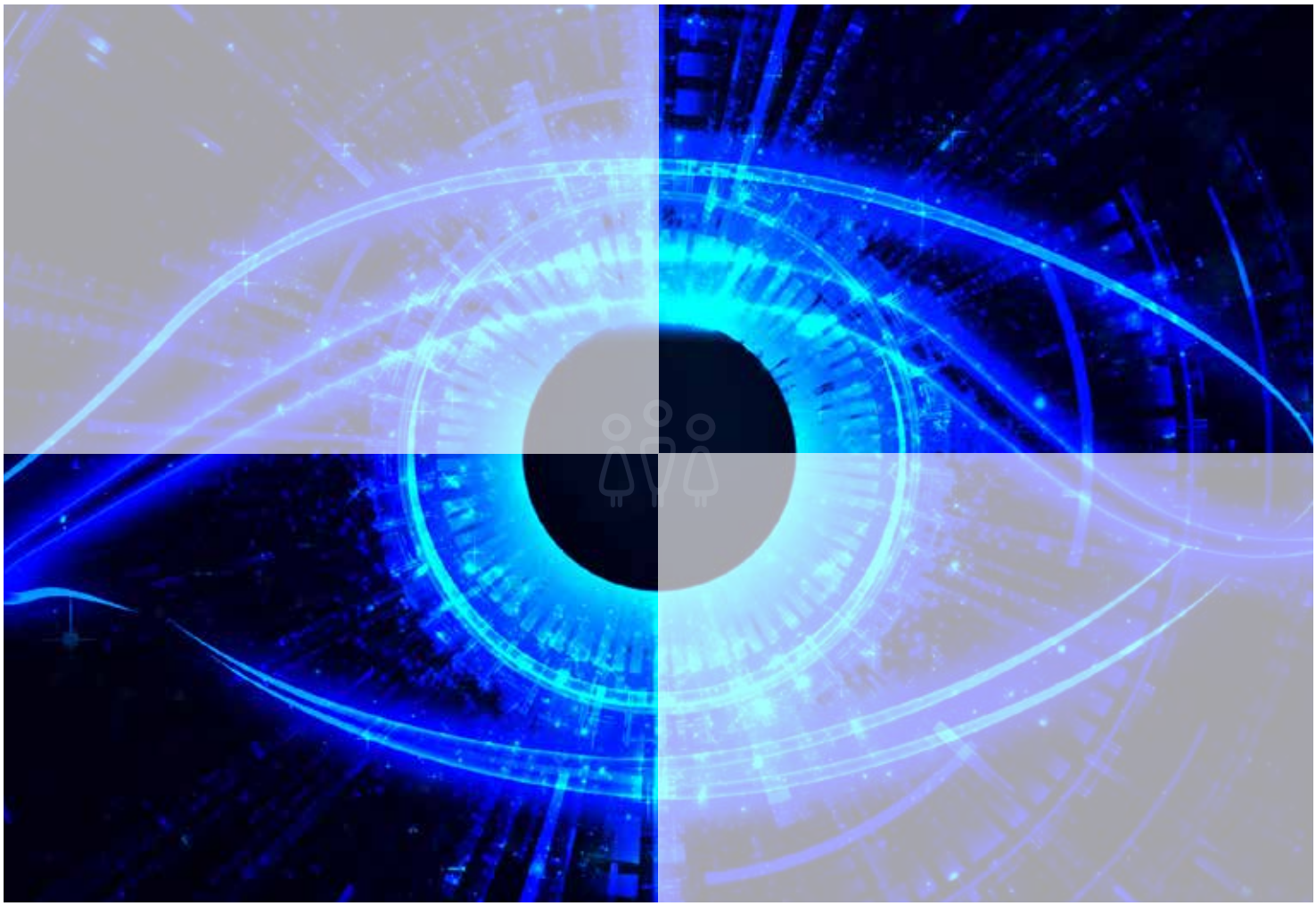
COMMITTED TO IMPROVING THE STATE OF THE WORLD

Industry Agenda

Rethinking Personal Data: A New Lens for Strengthening Trust

Prepared in collaboration with A.T. Kearney

May 2014



Contents

Executive Summary

As we look at the dynamic change shaping today's data-driven world, one thing is becoming increasingly clear. We really do not know that much about it. Polarized along competing but fundamental principles, the global dialogue on personal data is inchoate and pulled in a variety of directions. It is complicated, conflated and often fueled by emotional reactions more than informed understandings.

The World Economic Forum's global dialogue on personal data seeks to cut through this complexity. A multi-year initiative with global insights from the highest levels of leadership from industry, governments, civil society and academia, this work aims to articulate an ascendant vision of the value a balanced and human-centred personal data ecosystem can create.

Yet despite these aspirations, there is a crisis in trust. Concerns are voiced from a variety of viewpoints at a variety of scales. Industry, government and civil society are all uncertain on how to create a personal data ecosystem that is adaptive, reliable, trustworthy and fair.

The shared anxieties stem from the overwhelming challenge of transitioning into a hyperconnected world. The growth of data, the sophistication of ubiquitous computing and the borderless flow of data are all outstripping the ability to effectively govern on a global basis. We need the means to effectively uphold fundamental principles in ways fit for today's world.

Yet despite the size and scope of the complexity, it cannot become a reason for inaction. The need for pragmatic and scalable approaches which strengthen transparency, accountability and the empowerment of individuals has become a global priority.

Tools are needed to answer fundamental questions: Who has the data? Where is the data? What is being done with it? All of these uncertainties need to be addressed for meaningful progress to occur.

Insights from the Global Dialogue

- **Deliver meaningful transparency**
  Transparency practices need to be reframed to be more meaningful, actionable and relevant for individuals. Greater emphasis is needed on presenting individuals with understandable and relevant information on how data is being used. Organizations need to simplify the ways in which they communicate their data practices to reduce the complexity of transparency for individuals. Also needed are policies and tools for understanding how data flows "out the back door" of institutions. The forward transfer of data throughout the ecosystem is complex, opaque and drives uncertainty and suspicion.

- **Strengthen accountability**
  As the calls increase for shifting the primary focus of governance to be more usage-based and contextual, holding relevant stakeholders of all sizes accountable in a defined and measureable way is a priority. There are significant supply-chain vulnerabilities in how data flows throughout the value chain. Trust networks and holistic incentive structures are needed to ensure principled and enforceable data use.

- **Empower individuals**
  As the value and volumes of data originating from sensors and analytics increases, individuals are increasingly unaware and distanced from the decisions on how all this data is being used. Individuals need to be empowered in two ways: having a say in how data about them is used by organizations and having the capacities to use data for their own purposes. Additionally, as the predictive power of algorithms increases, individuals need to more effectively engage in understanding (and managing) the intended impact of data usage.

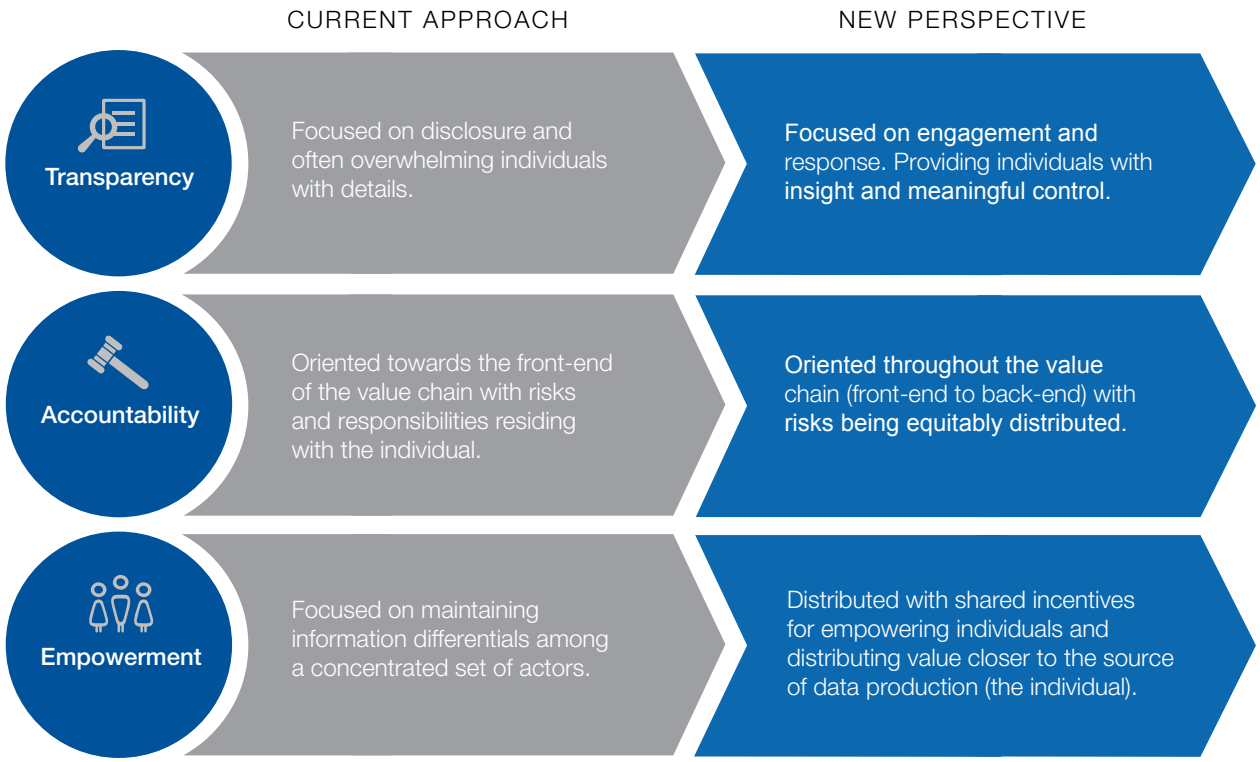
Objectives need to be set. The benefits and harms for using personal data need be more precisely defined. The ambiguity surrounding privacy needs to be demystified and placed into a real-world context.

Individuals need to be meaningfully empowered. Better engagement over how data is used by third parties is one opportunity for strengthening trust. Supporting the ability for individuals to use personal data for their own purposes is another area for innovation and growth. But combined, the overall lack of engagement is undermining trust.

Collaboration is essential. The need for interdisciplinary collaboration between technologists, business leaders, social scientists, economists and policy-makers is vital. The complexities for delivering a sustainable and balanced personal data ecosystem require that these multifaceted perspectives are all taken into consideration.

With a new lens for using personal data, progress can occur.

Figure 1: A new lens for strengthening trust



Source: World Economic Forum

World Economic Forum global dialogue: A new lens for strengthening trust

Dalian, China
(September 2013)
Identifying risks

New York, USA
(October 2013)
Interdependencies of hyperconnected systems

Dublin, Ireland
(October 2013)
Upholding human rights in the era of Big Data

Abu Dhabi, UAE
(November 2013)
Drivers and constraints for transformative growth

London, England
(November 2013)
The value of risk-based approaches

Brussels, Belgium
(December 2013)
Strengthening trust across industry sectors

Davos, Switzerland
(January, 2014)
Applying the insights from enhanced transparency, empowerment and accountability

Source: World Economic Forum

The Challenges for Strengthening Trust

It goes without saying that the data-driven economy is increasingly complex. Its rewards and risks are an emerging phenomenon beyond the control of any one actor.[1] Against this fluid backdrop, the World Economic Forum's global dialogue has coalesced around three pillars: delivering meaningful transparency, strengthening accountability, and empowering the individual.

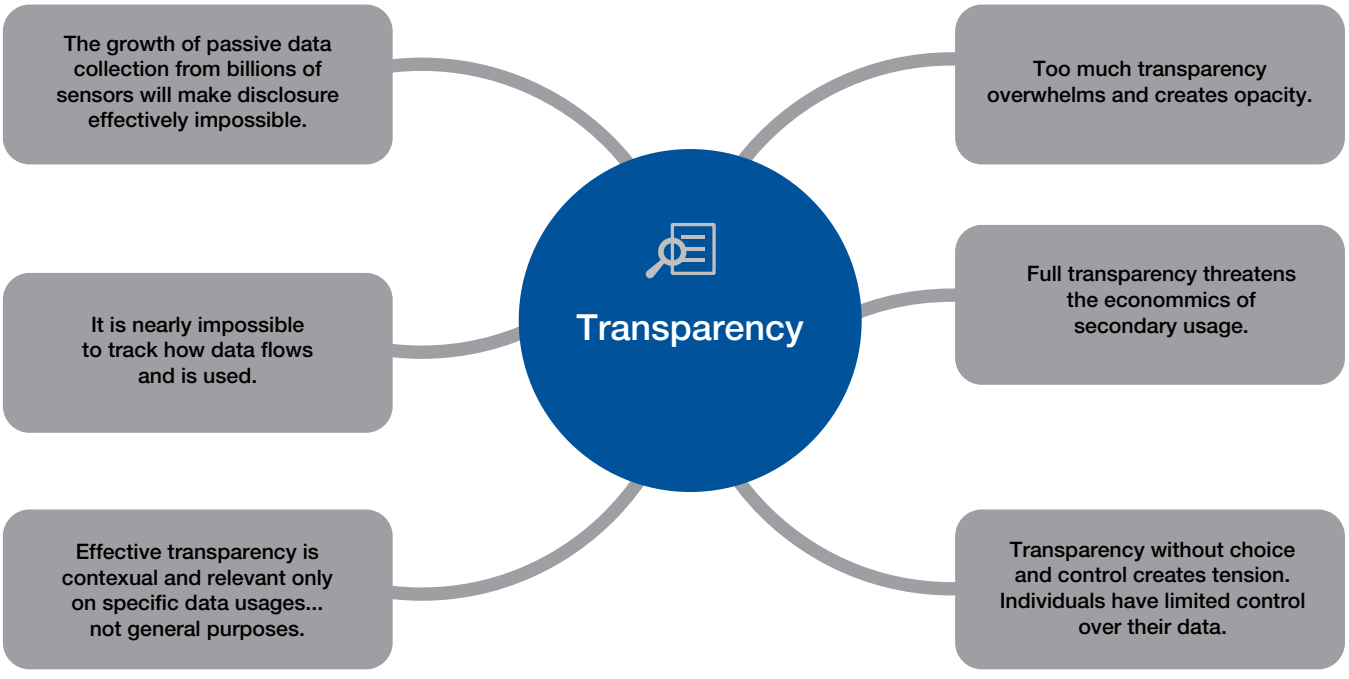
Meaningful transparency

The global anxiety over how personal data is used stems from the fact that we are all somewhat in the dark. According to author David Brin: "We're in a fog of data ignorance." Fluidly moving between jurisdictions, organizations and functions, the movement of personal data exceeds our ability to completely understand it. As noted privacy scholar Helen Nissenbaum writes, "The realm is in constant flux, with new firms entering the picture, new analytics and new back-end contracts continually being forged. We are dealing with a recursive capacity that is infinitely extensible."[2]

When it comes to transparency, restoring trust demands balance. Either too little transparency or too much can undermine the larger goals.

Transparency is more than access— a one way street that is "outbound only" and reduces individuals to being spectators

Figure 2: Key factors shaping transparency



Source: World Economic Forum

on how their data is used. Meaningful transparency requires institutions to listen, to have "inbound" capacities that provide individuals with the ability to influence outcomes.

Fully 78% of consumers think it is hard to trust companies when it comes to use of their personal data

Orange, *The Future of Digital Trust*, 2014

A growing movement is afoot to strengthen meaningful transparency and information sharing. Terms of service agreements are being simplified, standardized and put into machine-readable formats. Personal data dashboards are growing in number and functionality on a global basis.

But transparency cannot be shouldered by individuals alone. The focus of transparency needs to expand beyond the front end of the value chain. Organizations and institutions need to more effectively align (and communicate to individuals) on the shared norms of acceptable data uses. An ecosystem-wide focus on being transparent on the business-to-business processes of data handling needs to be strengthened.

The current momentum behind the drive for greater engagement is oriented towards customer-facing entities and their drive to strengthen the relationships they hold with their customers. When it comes to the back end of the data value chain behind the scenes, there is less progress. Helping individuals understand the back office of the "data-industrial complex" and the ways that data flows out the back door of customer-facing institutions remains largely opaque. Competing incentives, supply chain complexity and a lack of technical interoperability are major points of friction within the ecosystem. The question of "Who has access to what data?" remains a nearly impossible question to answer.

Figure 3: Concerns related to online privacy

Valid N listwise (10495). Percentage of people who answered 5, 6 or 7 on a 7-point scale of a global survey conducted in 2012.

Source: 2014 World Economic Forum T*he Internet Trust Bubble: Global Values, Beliefs and Practices (William H Dutton, Ginette Law, Gillian Bolsover and Soumitra Dutta)*

While positive steps are being taken by large and highly resourced organizations – within the business-to-business context – it does not fully address the operational challenges smaller sized, yet increasingly influential, commercial entities may face. There needs to be a more coherent and coordinated set of actions and liabilities defined for the fragmented supply chain so it can manage it failures as well as its success.

Absent broader adoption of trust networks, business risks to particular members of the supply chain will be offloaded onto consumers. Industry leaders within the digital advertising sector have noted this stating that "the supply chain by which digital advertising is created, delivered, measured and optimized is so porous and perilous that it jeopardizes consumer trust and business growth. The risk is so severe that the underlying innovativeness of the internet itself is in danger of grinding to a halt".[3] This challenge will only increase with the increasing adoption of wearable technologies (i.e. Google Glass) where individuals themselves will be able to collect, store, analyse and share information that is increasingly intimate.

The underlying tensions of transparency centre on the incentives to either facilitate or create friction for individuals. There are approaches which can be labelled as "user-centred" and those that are "user-centric". User-centred approaches are collaborative in nature and focused on all stakeholders working to facilitate data flows which empower individuals in meaningful transactions and experiences that are consistent with their expectations. User-centric approaches, in contrast, place all the decisions and responsibilities at the feet of individuals to manage by themselves. From this perspective, individuals are responsible for managing the data flows and permissions related to them. Often they are based upon limited capacities and tools for making appropriate decisions to preserve their interests.

Another factor fuelling the transparency challenge relates to the redistribution of power. Transparency creates social, political and economic risk, particularly for incumbents. These power dynamics serve to frame the narrative for many of the digital dilemmas shaping the personal data ecosystem. Debates on collection vs usage, anonymous vs identified, freedom vs security, and public vs private are generally all framed by incumbent interests from a highly concentrated set of powerful actors.

The power dynamics can be acutely seen in the narrative between freedom of expression and national security. It goes without saying that the nature and number of technology-related threats will grow as the digital economy expands. The impact of technology is never neutral. Yet the rhetoric of fear and uncertainty too often dominates the conversation. A one-dimensional debate persists where the interests of privacy are traded off against public safety and security.

Global leaders are recognizing the need to expand the dimensions of these conversations. As Ann Cavoukian, Information and Privacy Commissioner of Ontario, Canada, writes: "It's not a zero-sum game. Privacy and counter-terrorism measures can co-exist, with both values being respected, instead of being positioned as opposing forces requiring unnecessary trade-offs and false dichotomies."[4]

Strengthening Accountability

The challenges facing leaders today regarding accountability are essentially the same as 30 years ago: "How can we ensure data protection while enabling the personal and societal benefits that come from its use".[5] Despite a commitment on the part of industry, regulators and civil society for greater accountability, this principle has been elusive to fully uphold in practice. The principles and rights which have served as the foundation for the data ecosystem remain vitally important; ensuring they can be effectively applied is the challenge.

The Article 29 Working Party of the European Union describes accountability as "showing how responsibility is exercised and making this verifiable".[6] Along with the need for organizations to maintain effective privacy programmes with specific individuals who are answerable for their ongoing management and monitoring, a fundamental element of accountability is evidence; there needs to be verifiable evidence that appropriate measures are being taken.

The need for verifiable evidence presents a core challenge to the personal data ecosystem. There are structural limits on the tools and capacities to monitor, measure and enforce discrete uses of personal data. Accounting for the complex realities of today's data flows in a precise and granular manner remains a grand challenge for accountability. There is a need to develop systems and legal frameworks that recognise context and do so in a way that simplifies rather than adds to the complexity of the environment.[7] However, going down the path where every data interaction is context-dependent and requires its own set of rules will overwhelm the system in complexity. Approaches which simplify complexity and look to a broad set of conditions which apply to a general range of interactions has been identified as a good way to simplify, automate and facilitate trustworthy data flows.[8]

The tensions regarding accountability stem from an underlying pivot away from pre-emptive and generally prescriptive interventions to those which still require protection measures in advance but are more adaptive, contextual and evidence-based. Additionally, the scope of concerns are not isolated to the domain of privacy. A number of sectors now face significant governance issues in the use of personal data. National security, disaster response, automotive, health, education, retail, logistics and financial services are just some of the sectors struggling with how to balance the innovations which arise from the use of data with the need to protect the rights and claims of individuals.

As wearable technologies and the Internet of Things achieve scale, the origination of passively generated data will increase. Additionally, with billions of individuals from emerging economies connecting to the digital economy, the complexity of the issue will only multiply and accelerate.[9]

Figure 4: Key factors shaping accountability

Source: World Economic Forum

Empowered individuals

A third challenge undermining trust is the lack of empowerment among individuals. As mentioned, the current system reflects an asymmetry in power that broadly favours institutions (both public and private). Large institutions have greater resources to orient notice and consent agreements to advance their interests. As legal scholar Professor Ryan Calo writes: "We are only beginning to understand how vast asymmetries of information coupled with the unilateral power to design the legal and visual terms of the transaction could alter the consumer landscape."[10]

The tensions fueling the issue of individual empowerment can be viewed along two dimensions. There are a set of issues stemming from the relationships between individuals and the institutions which use data (i.e. the notice and consent challenges). There are another set of concerns based on individuals being able to use "their own data" for their own purposes. This emerging "bottom up" alternative model looks at the ways that data could be used as a utility by or with the individual.[11]

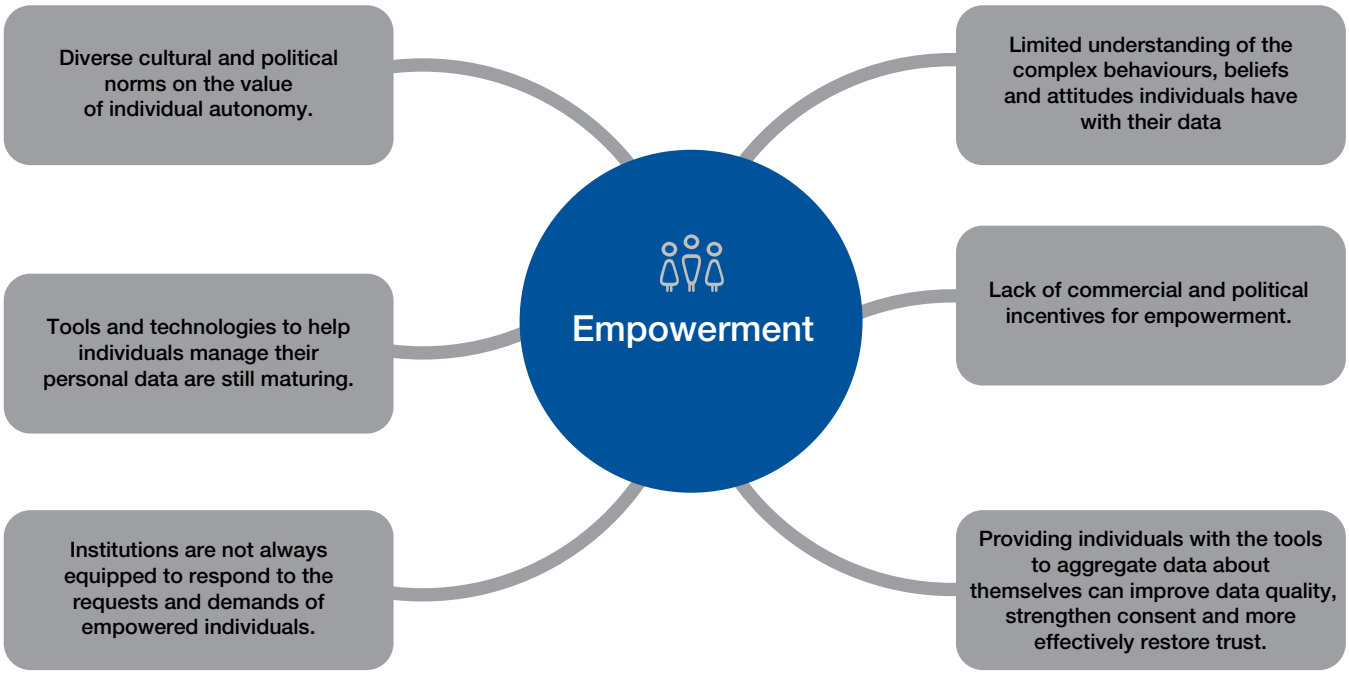
The issue of empowerment is most acutely seen regarding the issue of consent and purpose specification. With an increasing proportion of personal data now being passively collected by sensors or synthetically generated by algorithms, engaging individuals for consent to use data they know nothing about (and for purposes which are yet to be defined) remains problematic. Similarly, ex-ante limits on the ways that data can be used restrict innovation and growth. Combined, these two challenges create a Gordian knot that is highly complex and will continue to destabilize the ecosystem if left unchecked.

Despite the complexity of the issue, it is clear that individuals are taking additional steps to control their data. A fall 2013 study from the PewResearch Internet project found that more than half of the Americans surveyed "are concerned about the amount of personal data on the internet" and that "86% of internet users have taken steps online to remove or mask their digital footprints—ranging from clearing cookies to encrypting their email, from avoiding using their name to using virtual networks that mask their internet protocol (IP) address." Individuals are using increasingly sophisticated privacy enhancing technologies which provide visibility into how their online activity is being monitored, block ad tracking, encrypt messages and generally hide their online activities.

The second dimension of empowerment — individuals having access to their data to be used for their own purposes — is where the power dynamics come into play. As writer and computer scientist Jaron Lanier notes: "The dominant principle of the new economy, the information economy, has lately been to conceal the value of information."[12] A meaningful and multistakeholder dialogue on "fair value" exchange is just beginning to emerge. Disciplines such as behavioural economics and neuroscience can provide insights into these issues and also help understand how users are motivated in a society where data can be valued in multiple ways.

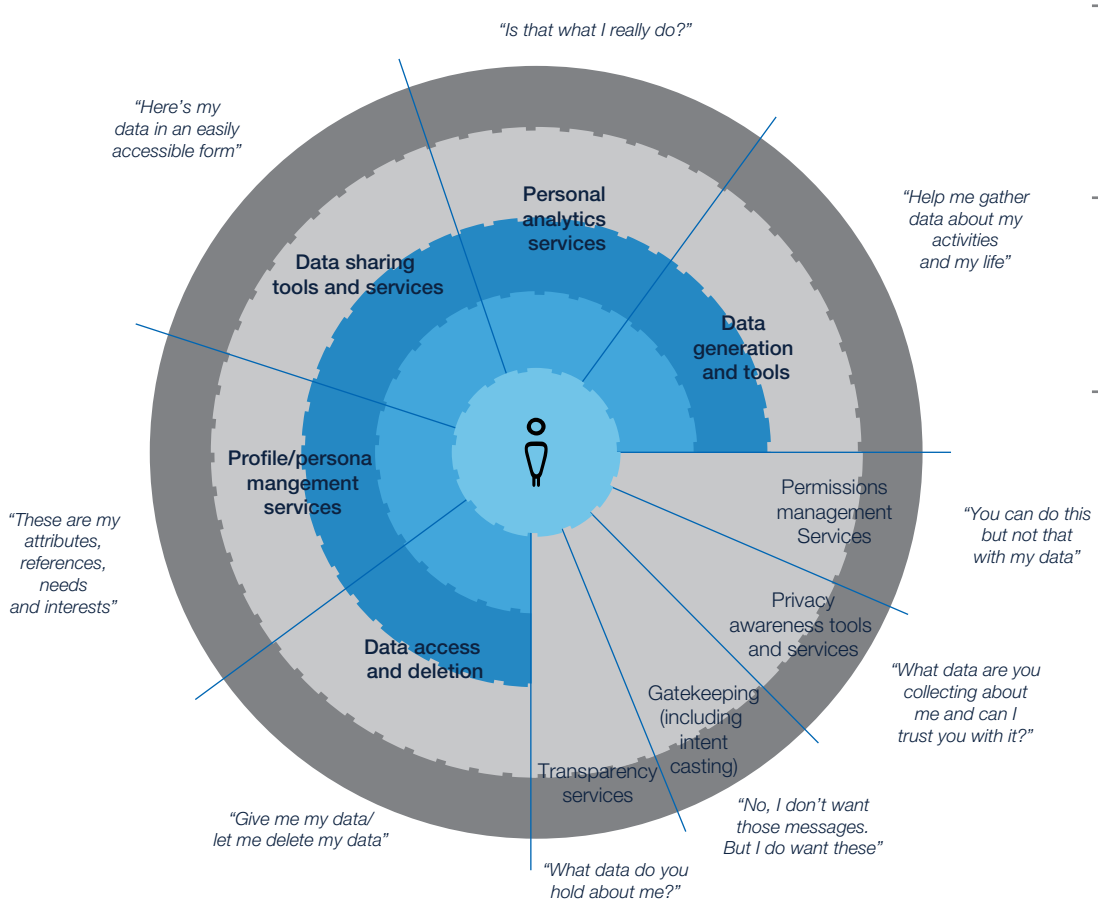
From a commercial innovation perspective, there is growing momentum in the area of Personal Data Management Services (PDMS) which can help individuals assert more control over how personal data is leveraged and value distributed. From January 2013 to January 2014 more than one new personal data service was launched per week. Areas of particular activity included data storage and management, anonymization services, identity management and personal analytics.[13]

Figure 5: Key factors shaping empowerment



Source: World Economic Forum

Figure 6: Personal data management services: A mapping of the market



Source: Mapping the Market for Personal Data Management Services, Ctrl-Shift, 2014.

Important distinctions on individual empowerment arise across different industry sectors. As new models of healthcare emerge and new strategies are identified, patient engagement is central for policies targeted to improving health and cost outcomes.

There is increasing recognition of the role of the individual as both contributor and consumer of data. In that light, a greater sense of data literacy among individuals is essential to facilitate the sharing of data for health and wellness outcomes. The role of context and the relative control of the individual are centrally important. Medical research, particularly in the area of genomics, requires large-scale data sets of uniquely identifiable and sensitive data where missing individuals can alter the findings. For medical treatment, individuals can unintentionally put themselves (and patient communities) at medical risk with too much control over the flow of health data.

The increasing adoption of digital fitness tracking devices presents a new level of complexity and highlights the importance of context for the degree of individual control. While there is an opportunity to combine and commingle these new intimate, high-resolution, activity-based health data with other data sets to provide a daily health dashboard for individuals, there are a range of new uncertainties on the data quality and how these combined data sets could be used for non-health related uses.[14]

Personal data generated from health tracking devices present new challenges for sharing data.

- Can such data be combined with traditional medical records for research and treatment?
- Is the device reliable and accurate?
- Can the data be authenticated and linked to only one person?
- Can insurance companies use the data in their coverage decisions?

World Economic Forum, *Rethinking Personal Data: From Collection to Usage* 2013

The need for primary research

A deeper understanding of individuals' sensitivities toward personal data is needed. What levels of transparency and control are needed to establish trust? What types of data carry greater sensitivities? Which personal risks are the most sensitive? What are the proper metrics to help answer these questions? The need for open and coordinated research about individuals and how they relate to data has become a top priority for sustaining trust.

Focusing on understanding the complex needs of individuals as it relates to empowerment and personal data management, a collaborative research project with more than 9,500 global respondents was established with Microsoft (full details are available in Appendix 1 of this report). The study identified seven separate variables which can influence individuals' perceptions of trust within a given context. The four factors which had the most impact were collection method, data usage, trust and value exchange. Overall, individuals want trustworthy behaviours throughout the ecosystem which extends beyond protecting privacy to encompass data security, data accuracy, the purpose for which data are used and any "code of ethics" that helps determine "appropriate" uses.[15]

To globally assess the attitudes, beliefs and practices of Internet users towards the use of data, an additional collaborative research project was done with the World Economic Forum, Oxford Internet Institute, INSEAD and Cornell University. Results from 11,000 online respondents found broad support for the freedom of expression the Internet enables as well as concerns related to privacy, security, trust and perceptions of governmental surveillance.

Figure 7: Perceptions of trust through the eyes of of Internet users

Perceived violation of privacy

HOW MUCH DO YOU AGREE...	% WHO AGREE
Organizations, companies and agencies ask for too much personal information online.	67%
People who go on the internet put their privacy at risk.	61%
There is personal information about me that is collected on the internet for reasons that I do not know.	58%
People I do not know may have access to my online personal information.	57%

N (9790) Percentage of people who answered 5, 6 or 7 on a 7-point scale of a global survey conducted in 2012.

Offline actors

TO WHAT EXTENT DO YOU TRUST THE FOLLOWING INSTITUTIONS TO PROTECT YOUR PERSONAL DATA...	% WHO TRUST
Banks and financial institutions	61%
Those providing health and medical services	55%
Government authorities (e.g. tax authorities, social security authorities)	53%
Telephone companies	44%
Shops and department stores	39%

Valid N listwise (10417) Percentage of people who answered 5, 6 or 7 on a 7-point scale of a global survey conducted in 2012.

Online actors

TO WHAT EXTENT DO YOU TRUST THE FOLLOWING INSTITUTIONS TO PROTECT YOUR PERSONAL DATA...	% WHO TRUST
Internet service providers (ISPs)	45%
Mobile phone operators	44%
Search engine companies	40%
Companies that provide social networking services	37%
Online marketers and advertisers	29%

Valid N listwise (10291) Percentage of people who answered 5, 6 or 7 on a 7-point scale of a global survey conducted in 2012.

Source: 2014 World Economic Forum *The Internet Trust Bubble: Global Values, Beliefs and Practices (William H Dutton, Ginette Law, Gillian Bolsover and Soumitra Dutta)*

Figure 8: The impact of context on acceptable uses of data

CONTEXTUAL FACTOR	GENERAL IMPACT	COUNTRY DIFFERENCES
Collection method	In general, scenarios with active data collection were favoured; scenarios where personal data is provided by "a person I know" or collected passively have negative impacts on user sensitivity.	Except for Sweden, "collection method" had the largest impact of all the factors considered in all countries.
Data usage	Scenarios where data is used as agreed were uniformly positive; whereas scenarios where data is used to automatically make decisions for users were uniformly negative.	In Sweden, "data usage" had the largest impact of all the factors considered. For the remaining countries, except for China and India, it had the second most significant impact on user sensitivity.
Trust in service provider	Participants favoured situations where the service provider is well-known over those where the service provider is unfamiliar.	Except for Sweden, China and India, "trust" had the third largest impact on user sensitivity of all the factors considered, although the impact in the US is relatively moderate. In China, a service provider providing free services is a positive factor.
Value exchange	Scenarios where the data is used to provide something of value or save time and/or money are regarded positively.	In China, "value exchange" had the second largest impact. Relative to other countries, it has the smallest impact in Canada. Providing a benefit to the community was also perceived positively in both China and India.
Type of data	For data that is actively provided, scenarios that involve sharing of bank account number were generally regarded negatively.	In India, "data type" had the second largest impact on user sensitivity.
Device context	Using computers for the transactions was regarded much more positive than using mobile devices.	In China and India, "device context" was not considered important.
Type of entity	No generalizations could be made about the impact of the type of entity, except that it was a factor.	Responses were negative when the "entity" was a service provider in Australia, China and especially India.

Source: World Economic Forum 2014, *Trust and Context in User-centered Data Ecosystems*

Near-Term Priorities for Strengthening Trust

Strengthening trust requires innovation along multiple fronts and over a longer time horizon. Despite the long-term nature of the evolution, participants in the global dialogue stressed the need to focus on near-term pragmatic actions to ensure progress.

The value of taxonomies

Before trust in the use of personal data can be strengthened in a meaningful way, a more efficient dialogue is needed. The current dialogue has been shaped by vague and imprecise terms which generally precede the word "data". Big, small, open, personal – all of these qualifiers are used to fence off a portion of the conversation regarding the use of data. A more holistic approach is needed. What are concrete objectives for regulators? What new types of thinking and insights are needed to be a responsible and accountable organization in the era of big data?

Shared taxonomies on how data originates is an area that can drive meaningful progress in the near term.[16] As Dr Linnet Taylor writes: "A new taxonomy of data is badly needed. Industry, government and citizens are too frequently in disagreement as to what exactly constitutes personal data and what does not – and without an understanding of how data gets positioned in each category, or flows between them, it is impossible to have a discussion about how to govern and regulate those flows."[17] Many existing privacy regulatory frameworks do not take this into account. The effect is that they indiscriminately apply the same rules to different types of data, resulting in an inefficient and less than trustworthy ecosystem.

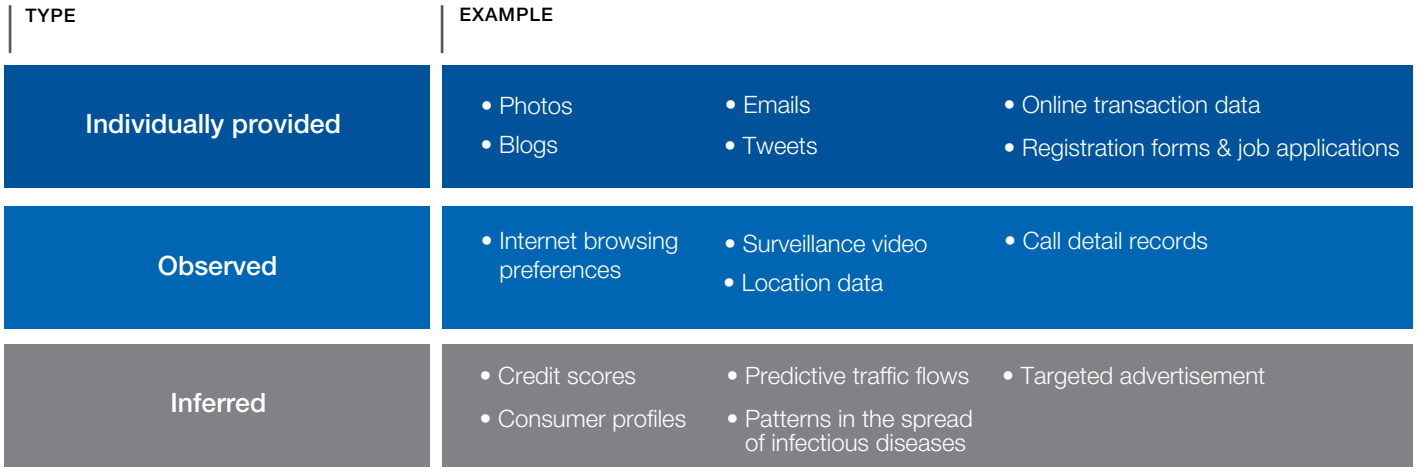
While the call for taxonomies is not new, the growing public concern on the issue of privacy increases the need for meaningful dialogue. Adoption of a common taxonomy can serve to align on shared understandings on the unique differences in the data being generated in today's world – both on the quantitative change in the amount of personal data being created as well as the qualitative differences based upon the origin of the different data types.

Figure 9: Linking near-term solutions to core challenges

	Transparency	Accountability	Empowerment
Standard data taxonomies	• Drives transparency by creating a common language. • Enables meaningful transparency by filtering what is relevant from what is not. • Facilitates interoperable identity and trust frameworks.	• Provide a baseline for interoperable permissions.	• At the coarse-grained, after level, I can translate technical details into personally relevant themes. • Empowers individuals with context-aware data usage and interoperable data use policies.
Measuring risks and benefits	• Assist data controllers and regulators to set priorities. • Promote global interoperability and leverage existing risk management methodologies.	• Creates a workable measure by which to hold organizations accountable.	• Restructures risk around the concerns and needs of individuals. • Provides institutions with the ability to understand perceived harms through the eyes of individuals.

Source: World Economic Forum

Figure 10: A taxonomy of personal data by origin



Source: Information Accountability Foundation, World Economic Forum, Marc E. Davis

An increasing (and accelerating) proportion of personal data is either passively observed about individuals or computationally inferred about them. By 2020, an estimated 50 billion devices will be wirelessly connected to the internet.[18] At the same time, from 2012 to 2017, machine-to-machine traffic will grow an estimated 24 times to 6 × 1017 bytes per month, a compound annual growth rate of 89%.[19] The majority of data will be collected passively through machine-to-machine transactions. Although still projected to grow rapidly, the overall proportion of data actively generated by individuals will decline.

Because of this change, the guidelines and protection mechanisms for governing the use of personal data need to adapt. Legacy privacy guidelines and data protection mechanisms were based on a presumption that data is actively collected from the individual with some level of direct awareness.[20] As billions of sensors come online that passively collect data (without individuals being aware of it) and as computer analytics generate and synthesize more "bits about bits", understanding how data is generated and how engaged the individual is in its creation has become essential for balance and effective governance.

All too frequently, data is grouped into "types" based on whether or not its handling is the subject of a law or regulatory framework. This is particularly true in the US, where valid distinctions can be made at the legal level between financial data, health data and educational data based on whether or not the collection, use, disposal, etc. of the data is subject to Gramm-Leach-Bliley, HIPAA and FERPA, respectively. These "types" are not, however, based on generic categories, and so lead analytical "stovepipes" that tend to defeat interoperable structures.

A framework which can foster a more structured dialogue (and supported by the World Economic Forum's community of leaders for years) is based upon three categories of data:[21]

1. Individually provided data
Data can be either "volunteered" by individuals when they explicitly share information about themselves through electronic media, for example, when someone creates a social network profile or enters credit card information for online purchases. Additionally, individuals may also be "compelled" to share data either through governments or commercial entities. The individual is generally aware of the action he or she is taking, and in many instances it has a transactional nature to it (filling out forms, providing medical history, providing an ID and password to install an app). When the volunteered data is more "by me" than "about me", it typically involves a deeper sense of unique ownership. These personal expressions (such as photos, videos, blog posts, tweets and emails) hold a unique set of claims held by individuals and often have strong emotional ties. Although this is the model assumed by existing data protection regulations, going forward this category will have the least amount of data.

2. Observed data
"Observed" data is captured by recording activities of individuals and can be grouped along a continuum of how aware individuals are of its capture and use. Some observed data is actively generated with a general awareness of the individual (browser cookies, credit card transactions, security cameras, location data from mobile device, etc.). Other forms of observational data are more passive and unexpected (RFID chips on automobiles, facial recognition technologies, WiFi scanners at retail establishments, etc.). In general, there is a lack of awareness by individuals regarding how much observed data is being captured about them, how it is being used and the value that can be extracted in selling (and reselling) it. The rise of mediated information systems (particularly mobile phone applications which have access to address books and location data) have made it much easier to observe an array of behaviours and actions. With passively collected data, the sense of ownership and control tends to shift to the institution which originally captured it. The majority of data generated in an "Internet of Things" world will be observed data – driven by sensors that automatically collect as people go about their day.

3. Inferred data
Advanced computational analytics and machine learning create a third category of data that is "inferred" and synthesized from an array of different data types (including data directly related to individuals and data that is not connected to them). Inferred

data is generally more of an amalgam of different originating data types and is generally used for predictive purposes. A higher degree of capital investment and utilization of intellectual property (often proprietary) is applied in generating inferred data. Along with being even further away from the individual in terms of awareness, there is also a loss of control by individuals on how it is used. With inferred data, claims of personal data being "a new asset class" are the strongest. Institutions assert much stronger claims over the inferred data they possess about individuals on the basis that they invested the time, energy and resources in creating it. Additionally, because of the unique, detailed and powerful insights inferred data can provide at multiple scales (individuals, communities and societies), there are competing tensions on how inferred data can be used, which level of impact takes priority, and who gets to determine whether those uses were fair and done with consent. This class of data has the greatest potential to drive innovation and economic growth.

From a policy perspective, the growing proportion of observed and inferred data raises the need for approaches that address concerns when data originates at a distance from the immediate perception of individuals and where consent, participation and awareness are seldom feasible. Additionally, given the fluid and recursive nature of data flows, guidance on upholding the principles of purpose specification and use limitations requires approaches which are much more suited to the increased volume, variety and velocity of how data moves.[22]

While a taxonomy on the various types of data provides a functional meta-description and a high level tool for guiding policies for acceptable data uses, it does not address the huge variety of contexts for how data is utilised nor the contextual attributes that foster trust (i.e. purpose, risk, value exchange, honesty and transparency and control).[23] Plus, given how extensively various types of data are mashed up and iterated upon in today's environment, it can become an exercise in false precision trying to identify which specific types of data were uniquely responsible for delivering specific insights and outcomes. The algorithms are too complex and constantly changing.

In that light, there is a growing call for a structured vocabulary on the different classes of data uses. At their core, usage taxonomies are focused on understanding the ways that data is used within a particular context. Uses need to be defined somewhat generically in order to accommodate the evolution of new technologies. As such, usage types need to have sector-specific definitions. Research, for example, is a very different use in a health-related context than in marketing.

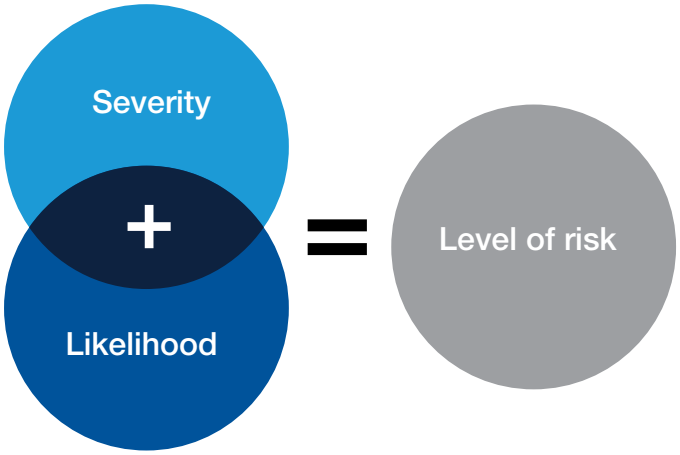
A particular usage could contain a set of permissions on who would be authorized for certain uses as well as policies that determine the appropriateness of that use. These use policies would reflect a number of factors, including preferences stated by the individual and would be based on the capacities of organizations to comply with internal policies, codes of conduct, as well as jurisdictional and sectoral regulations. Understanding various data types and uses, and their relationships as they interact, are essential components of introducing concepts of contextual understanding into personal data governance.

Underlying this approach will need to be a series of innovations in the area of identity management. In particular, there will need to be approaches which can connect legally recognized online identities with individual people as well as the multiple personas they adopt in their daily lives. There is also a growing recognition that identity per se is not the issue (coming to a widespread agreement on what that means is just too difficult). Rather, it is the flow of relevant reputational attributes about an individual that can strengthen the trusted flow of goods and services.[24] Many feel that the rapid growth in the area of collaborative consumption (the sharing of cars, apartments, skills, etc.) has been fueled by the rise of reputation currencies which allow strangers to connect in a trusted and contextually relevant manner.[25]

Focusing on impact, severity and likelihood

With nearly universal agreement that privacy is critically important yet elusive to uphold, the need for greater clarity on the underlying regulatory objectives and the specific ways to uphold it in the real world is increasing. What precise impacts in the use of data should be prioritized and acted upon? If online privacy is just as important as human rights, how can it be made easier for non-experts to uphold?[26] What are the ways to resolve the trade-offs when there are competing interests at the individual, community and societal level?

Figure 11: Assessing the likelihood and severity of impact



Source: World Economic Forum

A growing community of policy, private sector and civil society actors are looking to the discipline of risk management to provide insight into these questions.[27] With greater understanding and measurement of the risks and benefits in how data is used, it can serve as a near-term way for creating value, strengthening global interoperability and for existing data protection regimes to incrementally evolve. Calibrated, risk-based approaches can strengthen the ability to establish concrete policy objectives and establish pragmatic approaches for data holders to uphold those objectives in an adaptive, ethical and resource-efficient manner.[28]

The central idea is to expand the analysis of privacy through the eyes of the individual.[29] By extending the lens of analysis to a first person perspective, there is an opportunity for institutions to better identify, classify and assess privacy risks in terms of likelihood and seriousness of impact. An emphasis on what outcomes can be achieved can supplement the questions of *how* to be privacy compliant.

A starting point begins with asking: What is the intended impact of using data? How severe is that impact? How likely is it to occur? Who holds the risk? In pursuing this analysis it is also important to differentiate between threats in the stewardship of data and the associated benefits or harms they could create. This provides a way to organize threats (i.e. security breaches, loss of confidentiality, inappropriate usage or inappropriate access) and classes of harms. Some harms are tangible (loss of life, freedom of movement, property theft and physical injury) and some are intangible (such as restrictions on personal expression, social anxieties, emotional distress and reputational damages). The scale of the potential impact and who holds the risk also need to be addressed. Is the anticipated impact intended for a particular individual, a community or is it societal?

Risk-based approaches to privacy: Factors to consider

- Prioritisation based on the seriousness and likelihood of harm and impact to individuals
- Improves clarity on what it means for stakeholders to be accountable
- Clarifies regulatory uncertainty
- Addresses the emerging technology challenges of data-driven economies
- Strengthens global interoperability

Center for Information Policy Leadership Project, 2014

Additionally, a qualitative assessment of the different threats can be useful. Perceived (but unlikely) threats can result in a disproportionate amount of attention being paid to their prevention relative to their likelihood of actually occurring. Perceived threats can often lead to regulations based on "assume the worst" outcomes. The effect of "dread control" can distort the focus of regulatory efforts because of disproportionate fears on trying to control unlikely but dreaded events.[30]

The differences in how the perception of harms can internally vary from one individual to another add yet another layer of complexity. The risks and benefits of using data for one individual simply may not apply to others. Demographics, cultural norms, socioeconomic status, geography, politics and psychological profile are just some of the factors shaping the nature of perceived harms of data use.[31] More research is needed to identify some of these human-centred complexities.

Along with a greater understanding of the impact, severity and likelihood of a given use of personal data, the ability to measure these elements in a consistent and reliable manner is a critical enabler for strengthening trust. With commonly shared and agreed upon metrics of impacts, the discipline of risk management can be applied to address privacy concerns. Risk management can be applied across the data value chain to more granularly assess systemic reliability, codes of conduct and legal compliance.[32] Valuation and risk calculation can be established. Additionally, normative cross referencing of existing regulatory statutes can occur across jurisdictional boundaries. Measurements enable reliability and trust.

The lens of risk management should *not* be viewed as a replacement to existing policy frameworks and regulations. Rather, it can serve as an adaptive and more granular means to move past the vague notions of "creep", which currently guide much of the decision-making on personal data usage. The call to more broadly adopt the discipline of risk management is an ascendant theme within the privacy community. A shift to assessing the potential harms and benefits "is more intuitive, better reflects the importance of context, is more consistent with broader consumer protection law and, most importantly, it shifts the burden of protecting personal data away from individuals to the data handlers".[33] Notice and consent practices could be developed that were easier to understand for individuals and which could grow in line with technological innovation to the benefit of all stakeholders.

Figure 12: Framework for assessing benefits and harms of data processing

	Tangible impact to individuals	Intangible impact to individuals	Community and/or societal impact
Example benefits	Improved health and wellness outcomes Freedom of movement Increased earning power and access to employment opportunities Access to educational resources	Freedom of speech, beliefs, association, etc. Identity integrity assurance Development of "reputation capital" and the trusted flow of information Establishment of private spaces which are safe and protected Fair and non-discriminatory uses of advanced analytics	Strengthened ability to uphold political, civil, economic and human rights Strengthening of social trust and accountability Ability to understand, act and adapt to crisis situations and public safety concerns with more precision and flexibility Optimized food, energy and water resource allocation to address environmental issues from climate change
Example harms	Bodily harm Loss of liberty or freedom of movement Damage to earning power Other significant damage to economic interests	Chilling effect on freedom of speech, association, etc. Detriment arising from monitoring or exposure of identity, characteristics, activity, associations or opinions Reputational harm Personal, family, worplace or social fear, embarrassment or anxiety Unacceptable intrusion into private life	Damage to democratic institutions (e.g. excessive state or police power) Loss of social trust ("Who knows What about Whom?")

Source: Centre for Information Policy Leadership, World Economic Forum

Long-Term Issues and Insights

In addition to the near-term measures of establishing data taxonomies and measuring intended impact, a focus on longer term strategic issues will also contribute to strengthening trust and sustainability of the personal data ecosystem.

Strategic technological and business innovations

A core set of longer term issues will require business, legal and technical systems to more effectively interoperate at the pace and complexity of today's socio-technical world. Given the challenges for effectively preventing and managing against harmful uses of data, technological innovation can be applied to address some of these concerns. Progress needs to occur within three layers: infrastructure, data management and user interaction.[34] The dynamism and distributed nature of how the world is evolving requires a focus on the technological enablers, which will play a critical role in meaningful transparency, accountability and more effectively engaging individuals.

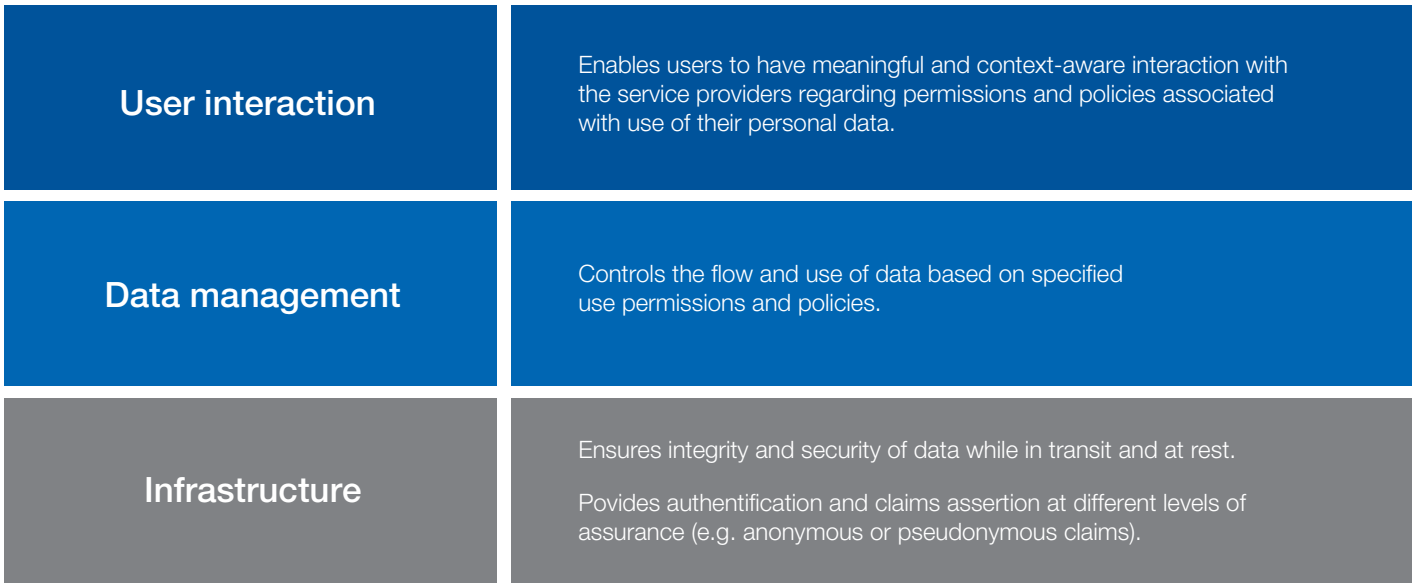
From a technology perspective, a key innovation that will need to be developed (and scaled) is the adoption of "smart data", where policies for using data are logically bound to the data for when it crosses trust boundaries.[35] Entities that touch the data are required to add a signature to the metadata for the purposes of auditing and provenance.

Figure 13: Linking long-term solutions to core challenges

	Transparency	Accountability	Empowerment
Context-aware personal data management	• Demonstrate that the flow and usage of data (and metadata) is consistent with agreed upon norms and legal requirements. • Meaningful user agreements. With better data accounting, risks can be redistributed.	• Provide the technical means to uphold shared principles in a dynamic, recursive and complex ecosystem. • Strengthen confidence on restitution across jurisdictions.	• Enable individuals to express their unique preferences and controls via metadata. • Individuals can dynamically manage data within a defined context.
Accountable algorithms	• Focus on communicating the intended impact to individuals. • Transparency into the underlying values, principles, decision criteria and outcomes of algorithms.	• Cross-disciplinary "algorithmists" who are collectively responsible for auditing the ethics and anticipated social impact of data driven outcomes.	• Strengthened popular understanding on the economic, sociological and ethical value of the sovereign individual who is both a data producer and consumer.

Source: World Economic Forum

Figure 14: Context-aware personal data management: A reference model



Source: Microsoft

With such capabilities in place, new contexts of data usage can be explored as the overarching code of conduct for legitimate purposes prevent against uses which are legally prohibited or were not agreed upon through the codes of conduct.

Infrastructure
The infrastructure layer contains the technology, services and applications required to assure the availability, confidentiality, security and integrity of the data, both while in transit and at rest. Seven areas of interoperable technical innovation have been identified as key enablers from a technology perspective: personal clouds, semantic data interchange, trust frameworks, identity and data portability, data-by-reference (and subscription), accountable pseudonyms, and contractual data anonymization.[36] Additional technical considerations at this layer would include measures needed to protect against unintended data breaches and system attacks. Authentication services can verify identities. Federated identity services can operate across trust boundaries and provide claims assurances including anonymous and pseudonymous identities which are essential elements. Establishing trustworthiness at this layer may utilize a combination of market-based mechanisms (reputation, brands, price), codes of conduct with enforcement, or via direct forms of governance.[37]

Data management
The data management layer focuses on the flow and use of personal data based on specified permissions and policies (established via legal contracts). Metadata technology can be utilized to create an architecture that links permissions and provenance with the data to provide the means for upholding the enforcement and auditing of the agreed upon policies. This interoperable architecture for sharing claims involves associating data with a "tag" containing relevant information such as provenance, permissions and policies which remain attached throughout the data lifecycle. Sticky policy and "privacy by design" can ensure that individual privacy settings remain embedded in the data or metadata as these are processed.[38] Policies will need to support context to enable context-aware user experience and data use. In addition to allowing for a dynamic level of individual control over data uses, this approach can provide regulators with the opportunity to focus upon principles and outcomes.

To address the coordination and accountability of various stakeholders, trust frameworks – which document the specifications established by a particular community – can serve as an effective means to govern the laws, contracts and policies of the system. It is in this capacity where the ability for actors to not only prevent but to respond (and provide restitution for the impacted individuals) can be strengthened. If individuals are well protected and processes for restitution are defined, it could become the seed for greater innovation where there is a commercial incentive for delivering privacy and trust. Combined with a new "social stack"[39] at the identity level, this new data and policy management layer could enable data flows across jurisdictional boundaries. In this sense, the confidence of individuals would be strengthened knowing that in whatever jurisdiction things went wrong, the individual would be assured of restitution.[40]

To deliver these types of systems which can prevent, detect and respond to the misuse of data, an area of focus brought up multiple times is the need for "smart contracts": integrating legal code with digital code. For centuries, contract law has been essential for establishing sustainable markets where the interests of all stakeholders can be equitably represented through legal agreements. The notion that has been suggested for further exploration is to automate the execution of legal code so it can uphold and enforce principles with contextually-based data usage at faster cycle times. Just as iron served as the "combustion chamber" for putting fire to work in the engines of the industrial era, automating the provisions contained within contracts can serve that purpose in the digital era.[41]

Significant development is needed for this approach to be technologically feasible. Security mechanisms are required to ensure that the provisions specified by individuals in a tag are not altered without permission. Further, there are challenges to creating a system with sufficient scale to be relevant in an internet economy context. These issues cannot be solved independently by either industry or government and will require a multistakeholder approach to gain traction.

User interaction

The user interaction layer includes the elements that enable individuals to have a meaningful interaction with service providers regarding the permissions and policies associated with the use of their personal data. Individual, cultural and local/national legal jurisdictional considerations would need to be addressed to ensure that the richness of personal choice and autonomy could be addressed.

The user interaction layer is clearly the area where further research is needed to gain better insight on some of the underlying issues that make personal data so unique, complex and contradictory. Contributions from the fields of economics, behavioural decision research, psychology, usability, human-computer interaction and many others would be valuable.[42] Focusing on how users define an "acceptable" use and the contextual elements surrounding that decision, the role of trust in establishing that context, what do individuals expect of other institutions for maintaining trust, and an array of cultural and regional norms are just some of the areas that have been identified for further research.[43]

Looking ahead: Accountable algorithms and the post-digital world

In many ways, the world is now post-digital. The achievements of digitizing and connecting everyone (and every thing) are largely taken for granted. The discourse is no longer about technology but how it is applied for socioeconomic change.[44] The focus is on a new nexus of control and influence: the algorithm.

"A sociological analysis must not conceive of algorithms as abstract, technical achievements, but must unpack the warm human and institutional choices that lie behind these cold mechanisms."

Tarleton Gillespie, *The Relevance of Algorithms* 2013

Complex and opaque, algorithms generate the predictions, recommendations and inferences for decision-making in a data-driven society. While easily dismissed as abstract empirical processes, algorithms are deeply human. They reflect the intentions and values of the individuals and institutions which design and deploy them.[45] The ability for algorithms to augment existing power asymmetries gives rise to an emerging set of questions on their influence over data-driven policy-making.[46] "At some point, you're in the hands of the algorithm," notes John Clippinger, Chief Executive Officer of the Institute for Data Driven Design, a non-profit research and educational organization. "You're whistling in the dark if you don't think that day is coming."[47]

Accountable algorithms: Key questions for strengthening trust

How significant and likely are the intended consequences of the algorithm? How many people might be affected (or perceive an effect)? Who holds the risk if things go wrong?

Are there errors that may be acceptable to the algorithm creator, but not the public? If so, who decides what's fair? Why was the algorithm tuned that way?

How might the algorithm steer public attention and perceptions in meaningful ways?

Is the algorithm's output lawful and consistent with social norms? If not, what's driving that inconsistency—a bug, an incidental programming decision, or a deep seated design intent?

What are the risks of transparency? Would publishing an algorithm negatively affect any individuals? Would it help those looking to game the system and establish an unfair advantage?

Source: Nicholas Diakopoulos, *Algorithmic Accountability Reporting,* Tow Centre for Digital Journalism, 2013.

As the socioeconomic impact of predictive machine learning and algorithms grows stronger, long-term concerns are emerging on the concentrated set of stakeholders (who both mediate communications and have access to powerful algorithms) and their influence over individuals. The focal point of these conversations centres on how data can be potentially abused to proactively anticipate, persuade and manipulate individuals and markets. The nature of these debates are complex, value-laden and give rise to some fundamental societal choices. Questions of individual autonomy, the sovereignty of individuals, digital human rights, equitable value distribution and free will are all a part of these conversations. There are no easy answers.

Through this long-term lens on the impact of proactive computing, the focal point for discussion begins to shift away from personal data, per se, to computer-based profiles of individuals and groups of individuals.[48] These profiles — fueled by fine-grained behavioral and sensor data — make it possible to monitor, predict and instrument social phenomena at the micro and macro levels. Noted legal scholar Mireille Hildebrandt writes: "What we need is a complementary focus on the dynamically inferred group profiles that need not be derived from one's personal data at all, but may nevertheless contain knowledge about the probability of one's intentions, affiliations, risk taking and behaviours."[49] Alexander Pentland of the MIT Media Lab also notes: "Individuals are largely determined by their social context. One can tell all sorts of things about a person, even though it's not explicitly in the data, because people are so enmeshed in the surrounding social fabric."[50]

The world of "smart" environments, where cars, toothbrushes, toasters, eyeglasses and just about everything else coalesce into the Internet of Things, creates a sea change in how data will be processed. Rather than being based on "interactive" human-machine computing, smart environments rely upon "proactive computing".[51] By design, these proactive environments are one step ahead of individuals. Connected cars need to anticipate accidents before they happen. Alerting systems for public health need to spot the spread of infectious diseases before they reach scale. Evacuating flood prone areas needs to occur before major storms hit.

The emphasis on proactive computing will change the role of human intervention from a governance perspective. Lacking a full understanding of how complex systems work, the ability of humans to understand, make decisions and adapt can be too slow, incomplete and unreliable. In this brave new world, building trust from the "principles up" will be essential and require new forms of governance that are open, inclusive, self-healing and generative.[52]

From a community and societal perspective, as civil "regulation-by-algorithm" begins to scale,[53] incumbent interests and power asymmetries will play an increasing role in establishing who gets access to an array of commercial and governmental services. As such, there is a need to ensure that the algorithms driving proactive and anticipatory decisions will be lawful, fair and can be explained intelligibly. Meaningful responses must be given "when individuals are singled out to receive differentiated treatment by an automated recommendation system".[54]

As Viktor Mayer-Schoenberger and Kenneth Cukier note in their 2013 book *Big Data: A Revolution That Will Transform How We Live, Work and Think*, a new class of professional is needed who can act as reviewers of big-data analysis and predictions. Part mathematician, statistician, computer scientist and data ethicist, these impartial individuals would function much like accountants and evaluate such things as the selection of data sources, the algorithms and the intended impact on identified individuals or communities.

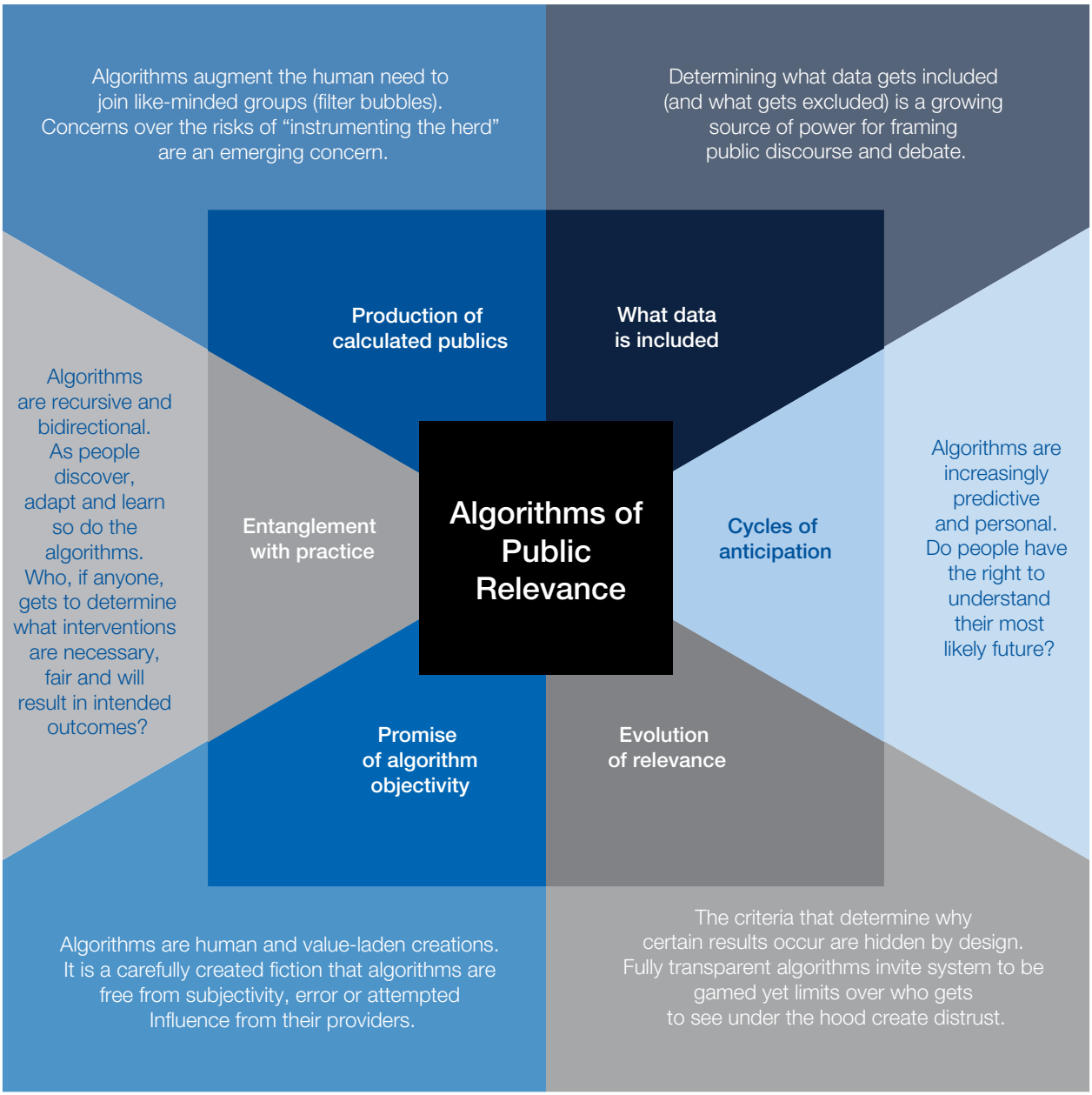
One emerging set of concerns is the institutional ability "to discover and exploit the limits of an individual's ability to pursue their own self-interest."[55] Given that a majority of consumer interactions in the future will be mediated via devices and commercially oriented communications platforms, data-centric institutions will have the means and incentives to trigger "predictable irrationality" from individuals.[56]

With a vast trail of "digital breadcrumbs" accessible for companies to mine and tailor highly personalized experiences, a growing set of concerns is arising on how individuals could be profiled and targeted at moments of key vulnerability (decision fatigue, information overload, etc.) and limit their ability to act with agency and in their own self-interest.[57] With the lives of individuals becoming increasingly mediated by algorithms, a richer understanding is needed for how people adapt their behaviors to empower themselves and gain more control over the manner of how profiles and algorithms shape their lives in areas such as credit scores, retail experiences, differential pricing, reputational currencies, insurance rates, etc. As the New York Times R&D Lab has noted: "As algorithmic systems become more ubiquitous and impactful, what behaviours and strategies emerge to optimize, control, obscure, or otherwise manipulate the data that we emit?"[58]

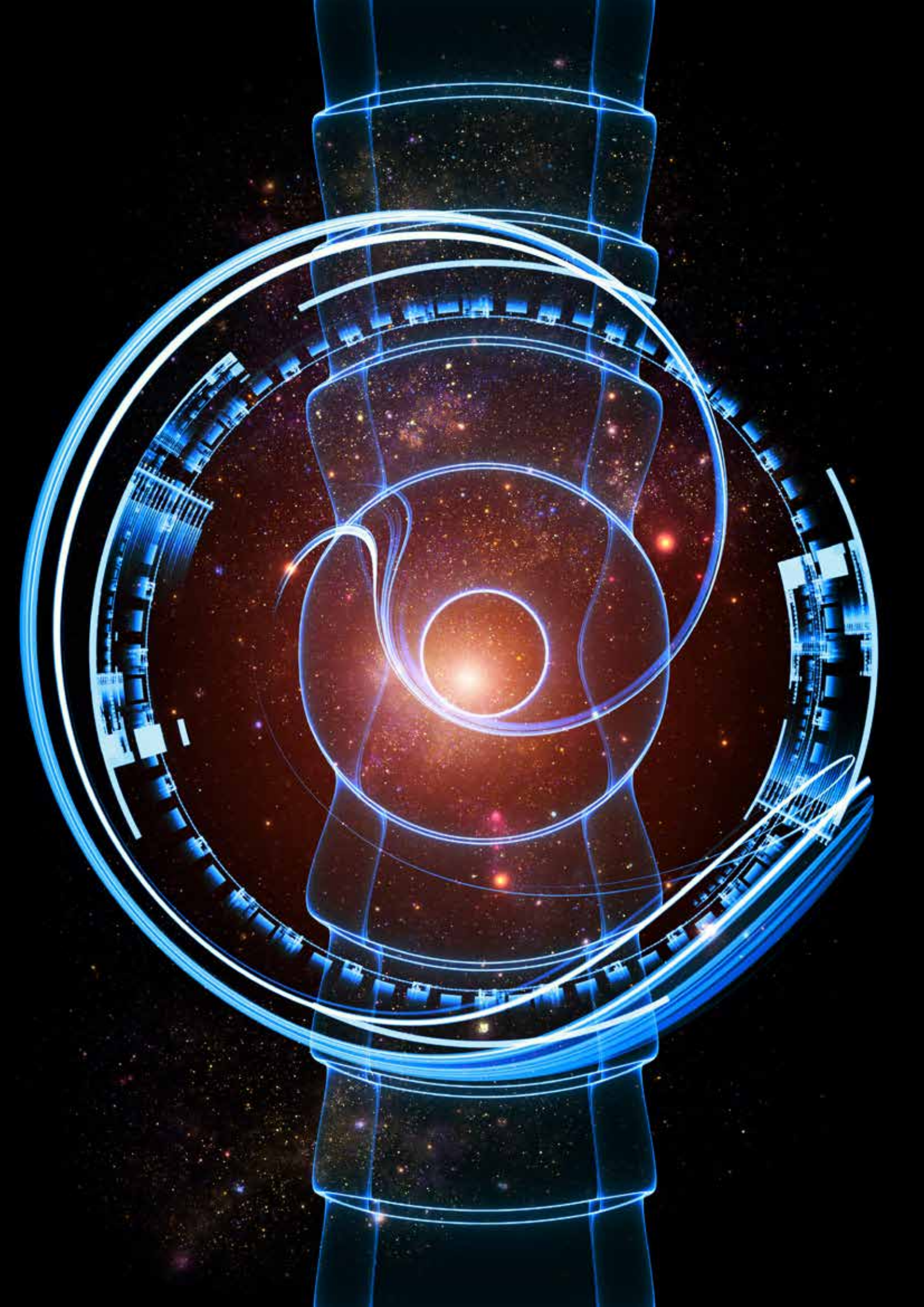
In this light, one of the most provocative and strategic insights on strengthening trust that emerged from the global dialogue was the concept of exploring ways to share intended consequences of data usage to individuals. Participants cited language in the 2012 Draft European Data Protection Act (section 20), which calls for "the obligation for data controllers to provide information about the envisaged effects (emphasis added) of such processing on the data subject".[59]

To address this emerging set of concerns, establishing a cross-disciplinary community of forward-looking experts, complexity scientists, biologists, policy-makers and business leaders with an appreciation of the long-term societal impact was identified as a priority. This group would proactively help design and test systems that balanced the commercial, legal, civil and technological incentives shaping outcomes at the individual and social level. They would need to develop some form of legal protection to limit liabilities and provide a safe space to explore complex issues in a real-world setting. One attribute of this safe space would be for it to be governed by an institutional review board where ethics and the interests of individuals could have a meaningful and relevant voice (similar to how they are used by the biomedical and behavioural science sectors). Institutions concerned about legal uncertainties, regulatory action or civil lawsuits could have a richer means for assessing ethical concerns using these approaches.[60]

Figure 15: Opening the black box: Key dimensions for addressing the impact of algorithms



Gillespie, Tarleton. "The Relevance of Algorithms." In *Media Technologies: Essays on Communication, Materiality, and Society*, edited by Tarleton Gillespie, Pablo Boczkowski, and Kirsten Foot: MIT Press (2014)



Conclusions and Next Steps

A theme consistently stressed throughout the Forum's multi-year engagement on personal data, and reflected within this document, is the inherent dynamism of the personal data economy. Complex and iterative, it needs approaches to governance which operate at the same clock speed and can be applied across the entire data value chain. There is a risk that by moving at such dramatically different speeds, policy frameworks that progressively lag behind innovation will not work.

Also constantly evolving is the position of the individual in the personal data ecosystem. From active participants who "volunteered" data, individuals are increasingly becoming passive data subjects. From providing relatively few details on an occasional basis, individuals in the modern economy are constantly producing data of a variety of types. Their capacity for meaningful influence and control over the disposition and use of data related to them has declined. Perhaps not coincidentally, their perception of the threats posed to them by data use has also grown.

Strengthening the principles of transparency, accountability and individual empowerment will serve as the cornerstones of a trusted and sustainable personal data economy. A central tension is the way that information correlates with power. The personal data environment is founded upon maintaining information differentials between individuals and institutions. One-sided notice and consent agreements, crafted to protect institutional interests and comply with regulatory requirements, are the vehicle for maintaining this gap. The incentives to change this are still limited.

While the growth of data volumes is increasing exponentially, progress is occurring incrementally. One area where this is most evident is the gradual shift away from exclusively focusing on data collection and notice and consent as the exclusive points of data control. Usage-based approaches that complement existing frameworks for governing personal data are gaining wider recognition and support. Similarly, efforts to understand the expectations and explore the rights of individuals regarding personal data are gaining speed.

Overwhelmingly, approaches that start small, "fail fast" and focus on direct input from individuals are the most informative. The complex challenge of personal data must be broken into manageable component parts and progress made in an incremental fashion. "Stop trying to solve the overall problem and start focusing on fixing a problem" was advice heard on multiple occasions during the global dialogue.

The proposals outlined in this report are the first steps towards strengthening trust by regaining transparency, accountability and empowerment. In the near term, data taxonomies can streamline discussions and help establish a common understanding of data policies, providing a foundation for transparent and accountable use. Managing uses by measuring risks and benefits represents a tractable approach to accountability that re-orients data governance around individuals. At the same time, research and innovation into supporting technological and business infrastructure can, over time, drive the necessary scale and efficiencies for sustainability. Finally, thinking through the implications on data governance in the context of smart environments keeps the discussion on the leading edge of emerging issues rather than lagging behind.

However, as has been stressed in this report, many aspects of the personal data economy are inherently unknowable in an a priori sense. The proposed actions listed above must be executed in an applied context rather than an ivory tower. Appendix II of this document outlines three domains where new approaches can be explored for strengthening transparency, accountability and individual empowerment.

In 19th-century Britain, the Locomotive Act of 1865 stipulated that self-propelled vehicles on public highways must be accompanied by a man with a red flag walking 60 yards ahead of the vehicle. The transportation policy sensibilities of one era (in which people principally travelled on foot or horseback) were applied to an emerging technology in a way that seems unthinkable to the modern observer.

Although restrictive, this policy allowed for the use of early automobiles as the sector developed. However, it was only later that policy shifted from a prescriptive restriction (the man with the flag) and adopted a set of principles (traffic signals, speed limits, etc.) that relied on a highly distributed and human-centred coordination. What allowed the ecosystem to truly transform society were flexible approaches and small actions taken by millions of individuals. Red lights by themselves did not make cars stop and intersections safe. It was the shared agreement by everyone to put their foot on the brake that made the system work.

The hope is that data governance policies follow a similar path – from prescriptive restrictions to flexible, accountable and human-centred principles. But this transformation cannot take the decades that were afforded previous generations. All stakeholders in the personal data economy – policy-makers, industry and civil society – need to move forward in ways that are efficacious rather than ideal. Through significant effort, ongoing dialogue and trial-and-error stakeholders can collectively remove the person with the red flag and begin to see personal data through a new lens for strengthening trust.

Near-term priorities

- **Shared data taxonomies:** A shared understanding of the different data types and uses is a foundation for efficient and effective dialogue and policy creation. Data is changing quantitatively and qualitatively. Understanding how the proportions of inferred and observed data are impacting the role of the individual is important to consider in policy formulation. Additionally, interoperable systems to promote transparent and accountable data use require a common frame of reference to enable functionality.

- **Manage usage by measuring risks, benefits and their allocation among stakeholders:** The central necessity is to expand one's understanding of the threats of data use as seen through the eyes of individuals to develop consistent metrics and to build these metrics into accountability frameworks. Individuals' perceptions of risk can vary according to a number of contextual factors, and can change over time. However, a baseline understanding of individuals' needs and expectations can contribute in the near term to more functioning governance.

Long-term needs

- **Technological and business innovations:** Scalable and efficient deployment of tools to enhance transparency, accountability and empowerment will all require enhanced technological capabilities such as smart data. Technology should be seen as a key enabler, especially necessary in a dynamic and distributed ecosystem, of evolving business models and policy frameworks. The focus of these innovations should address ways to prevent, detect and respond to the identified impacts of data usage. Focusing on how the ecosystem can both get it right to ensure the trusted flow of data as well as how to put it right when things go wrong is a top priority.

- **Data governance in smart environments:** As data is generated in an increasingly passive fashion, and analysis and decision-making done increasingly by machines, a new conversation on the ethics of data use will be needed. The potential for computers to co-opt individual preferences, the protocols for human intervention and the capacity for effective transparency are among initial points of discussion.

Appendix I

Trust and context in user-centred data ecosystems

The following is excerpted from the May 2014 World Economic Forum report *Rethinking Personal Data: Trust and Context in User-Centred Data Ecosystems*. To read the full report, visit weforum.org/personaldata.

Despite the growing recognition of the importance for understanding the context of data usage to inform effective policies, little work has been done in this regard. To address this concern, a collaborative global research initiative was established between the World Economic Forum and Microsoft. This appendix is a summarized version of the full report published in May 2014.

The intent of the study was to examine how individuals define context, focusing on the factors that impact their sensitivity regarding the use of data related to them by service providers. The project studied how these factors vary across different countries, how they can aid in the design of context-aware system, and how these systems can be integrated into user-experience designs for interactions that are more meaningful and consistent with complex individual preferences.

The results show that a variety of factors, both objective and subjective, influence the perception that individuals hold regarding the appropriateness of a given scenario. Other demographic characteristics unique to each individual – for example, their age or level of technological sophistication – also play a role.

Framework for analysis

Throughout 2012 and 2013, Microsoft sponsored a series of research studies to address these issues. The research was divided into two stages. The first phase involved qualitative studies in Canada, China, Germany and the United States to develop insights on users' mental models on their personal data. The second phase provided quantitative analysis to validate the initial insights. For this phase, the original list of countries was expanded to include Australia, India, Sweden and the United Kingdom. The research identified seven distinct factors that individuals consider when determining whether a given use of data is acceptable. This is defined as the data context.

The importance of including subjective variables underscores that data use context is very much defined by personal preferences. Note that neither "trust" nor "value exchange" on its own is sufficient to determine acceptability of data use to the individual. They play major roles, but they do not pre-empt other factors.

In addition to these seven variables, factors related to the mental models of individuals are also identified. Some of these individually-based factors included:

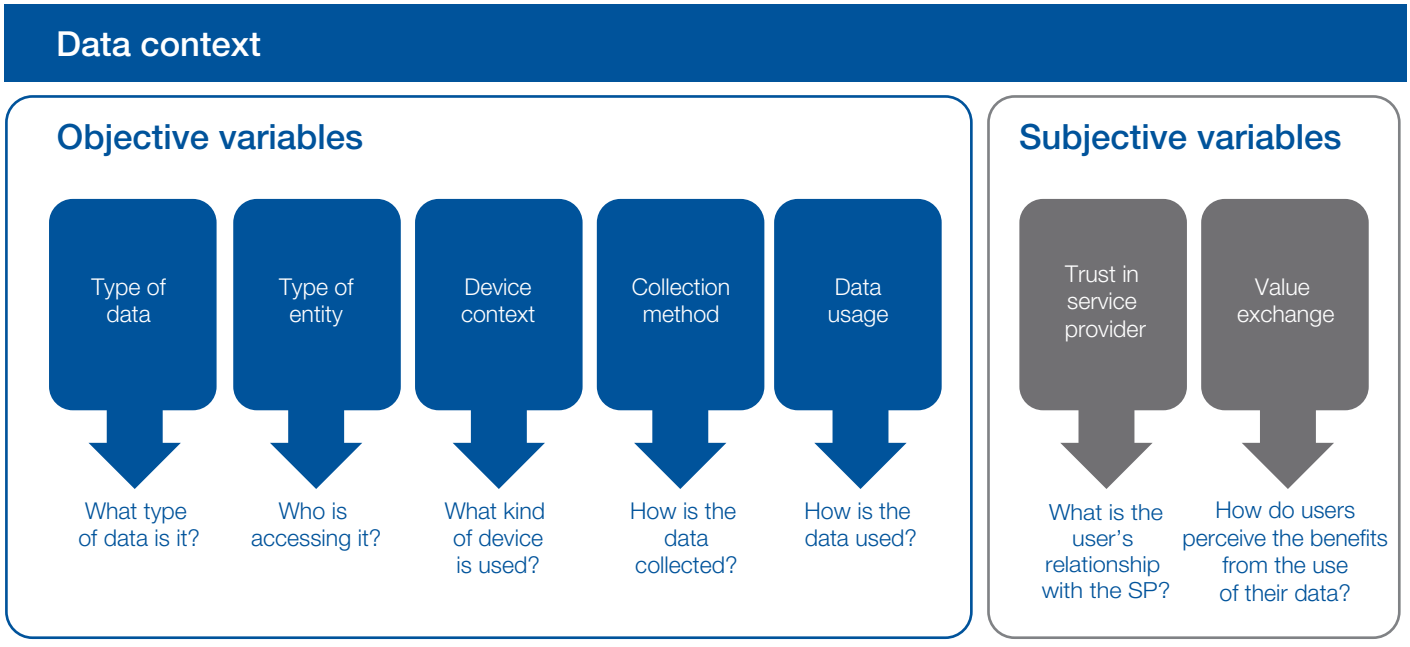
- Attitudes to and adeptness with technology
- Awareness of the relationships and activities within the personal data ecosystem
- Perceptions of government protection

The impact of contextual factors

In most geographies, collection method had the largest impact of all the variables examined. Similar to other research demonstrating that individuals want to have a sense of control over how data is collected, it is interesting to note the strength of this desire despite results that show inconsistent behaviour, perhaps due to the relative lack of available tools for individuals to effectively manage this attribute.

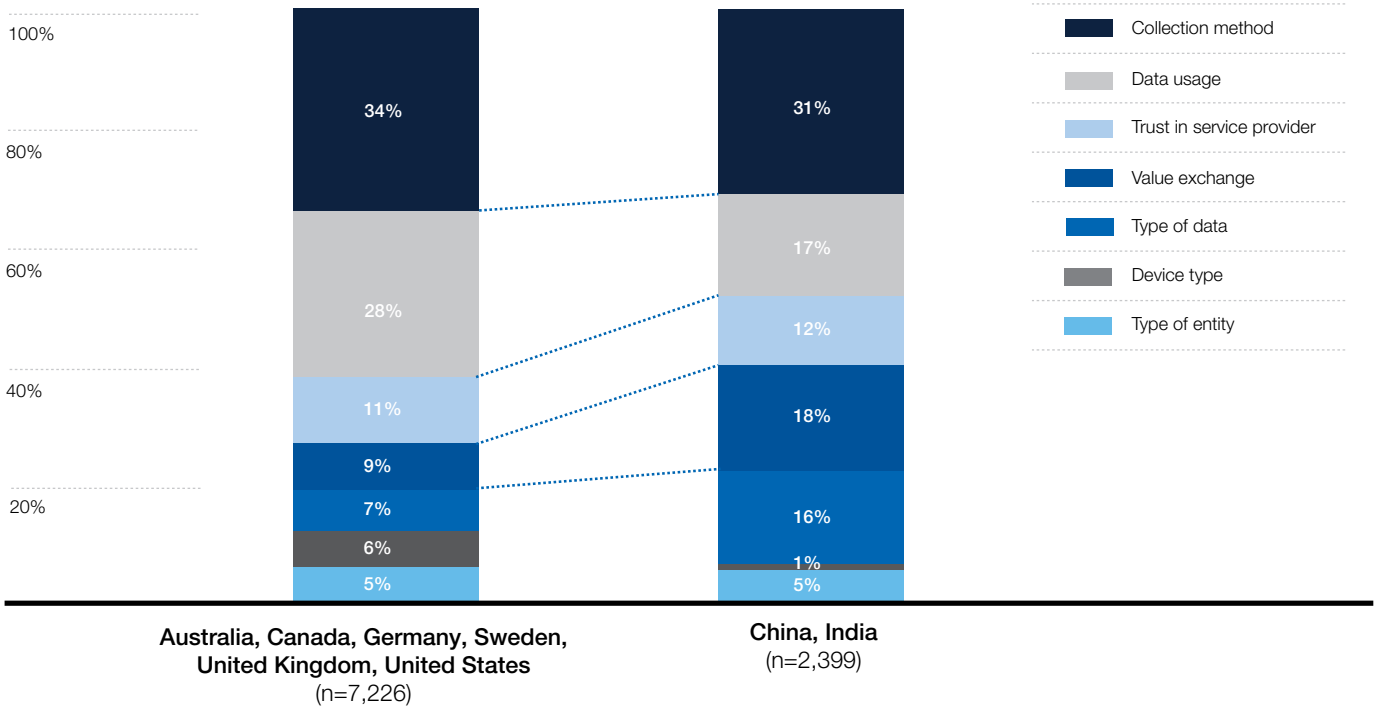
The trust variable was the third most important factor determining acceptable use in the Western countries. For situations involving the passive collection of data and where individuals perceived

Figure 16: Factors impacting individuals' sensitivity to the use of their data



Source: World Economic Forum

Figure 17: The impact of contextual factors



Source: World Economic Forum

no additional benefit (which causes low acceptability), the trust variable had a significant positive impact for all countries.

Although value exchange had a smaller impact in the Western countries, it had the second largest impact in China. In addition, the research uncovers preliminary evidence that individuals tend to frame their interactions from the perspective of a perceived value exchange. When the value exchange is to deliver benefits to users – either in saving time and/or money or to enable something of unique value – the acceptability rate is highest for all countries. However, attitudes towards value exchange when presented in terms of community benefit were more variable, possibly reflecting differences in cultural values between different countries.

The research results discussed here show that individual preferences for data use are nuanced and contextual. With subjective factors such as trust in service provider, perceived value exchange and other attitudinal, demographics and cultural factors all playing a role, what is considered acceptable is clearly personal and will evolve over time.

Binary approaches to data governance that treat all data as equal, and apply universally, are thus neither appropriate nor flexible enough, especially in a world of big data. Incorporating context-related nuances into regulations is difficult. However, technologies similar to those described here may provide an alternative, by facilitating policy frameworks that are principle- and outcome-driven, rather than process- or technology-driven.

Context-based systems and user experiences

A better understanding of individuals' perceptions of context can contribute to the development of systems that incorporate contextual elements into governance and individual engagement functions. Data governance systems that incorporate contextual elements enable more user-centred data ecosystems by respecting individual preferences in data-use scenarios. Where individual preferences are unknown, recommend personalized settings that are based either on individuals' past preferences or prevailing practices.

One approach is a "recommender system" that can be deployed either on behalf of service providers to enable a personalized user experience, or on behalf of individuals as "personal assistants" to help with context-sensitive data settings for different types of applications. In either case, these systems minimize the probability of data uses that are inconsistent with user expectations and empower individuals to engage in more meaningful interactions with service providers, thus increasing the level of trust in the overall ecosystem.

Conceptually, a recommender system that can assess a number of variables can help predict the acceptability of a given data-use scenario, and recommend appropriate data settings, either to an application or a user. If it predicts a negative decision from the user, it can share with the proxy what additional factors would make the scenario more acceptable. A more meaningful user experience can be achieved either by providing additional input or enabling the users to negotiate on the factors that the research found to have the largest impact on increasing acceptability (trust, value exchange, and data usage).

Policy implications

Context is key, even if not well understood. The research presented here shows context as being driven by multiple variables – some objective, but some clearly subjective – and driven by continuously evolving social and cultural norms. However, defining such abstract concepts in regulations is not ideal, and can lead to overly prescriptive and less adaptive laws.

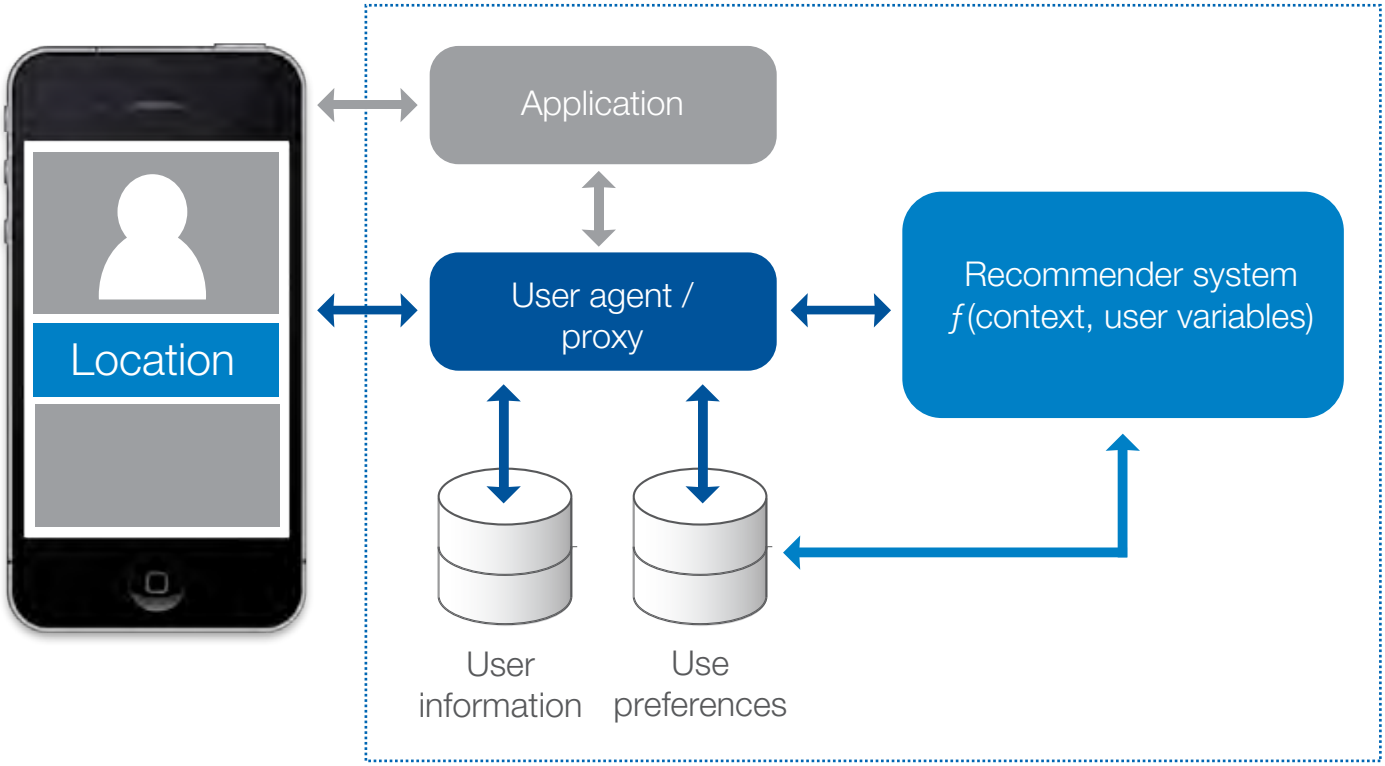
Technologies such as those described here enable the development of context-aware systems, and an alternative approach to policy frameworks that respects individual preferences and needs according to the context of a given data usage. This is different than emphasizing the initial context(s) in which the data was collected. This difference, and the technologies that facilitate it, are crucial for trustworthy data ecosystems.

Importantly, policy development can be informed by evolving technology and research. As the latter advance, new insights into individual behaviours and preferences, and proof of concept on the technology front can influence the scope and flexibility of regulatory frameworks. Policy-makers can base accountability regimes around outcomes rather than a fixed set of rules.

Over time, context-aware systems can be coupled with other technologies such as a metadata-based architectures – where data is logically accompanied by interoperable "metadata tags". These tags can contain use policies associated with the data and related provenance information. Combined, these preferences and permissions can inform any entity that touches the data on how it can be used. Providing automated mechanisms that can facilitate contextually appropriate data use can also be leveraged for its enforcement. What is considered acceptable context would be reflected in the data-use policies – examining these policies would reveal contextually inconsistent uses. With these, innovations, it would be easier to uphold principles in a constantly changing world of big data.

More research is needed on how context can be defined more clearly and simply, and how it can be practically integrated into systems and interface designs that engender meaningful user engagements. This research is needed at the global level to provide an evidence base that can be used to develop an interoperable global framework, or simply a framework that would allow individuals from one region to access services in another – a basic enabler for today's internet commerce.

Figure 18: Illustrative example of a recommender system



Appendix II

Contexts of usage – Applying the insights

The global dialogue on personal data had extensive conversations with practitioners from an array of communities throughout the year. The following profiles outline the challenges, opportunities and immediate next steps for activating real-world learning environments in three contexts: health and wellness, international development, humanitarian aid and human rights.

Health and Wellness

Opportunities and potential value

The global health and wellness community is using personal data to improve care outcomes and drive efficiencies along a number of fronts. Managed care providers are combining behavioural data with traditional medical records to suggest treatment and prevention regimens. In the precision and personalized medicine space, researchers are combining large genomic data sets to develop advanced medicines. Digital health uses information technology to promote collaboration and personalization in healthcare, while reducing costs, by combining many applications of data and technology, including mHealth, eHealth, connected health, big data, wearable computing and gamification.

However, much of this data remains fragmented across industries and organizations. Ownership, interoperability and transfer issues remain unresolved. Much of this data – for example, location data from a mobile phone – is viewed by individuals as highly sensitive. Further, individuals may fear that greater access to personal data could adversely affect their health premiums or treatment options.

Opportunities for building trust

Transparency

- Determination of a coarse-grained set of uses that are understandable to individuals
- Assessment of the risks to individuals created when different data types are applied to each use, as well as mitigating actions that can be taken
- Based on sensitivity and risk assessments, determination of what levels of preference and control individuals should possess

Accountability

- Establishment of common codes of conduct within communities of care providers and research institutions
- Procedures for transferring data to researchers or care providers outside established trust boundaries that evaluate the appropriateness of a transfer based on individual preference and risk potential
- Revision of risk management practices that integrate data risk assessments with other clinical and research risk control procedures

Empowerment

- Establish clear and easy-to-understand preference types that individuals can express when entering a care environment, as well as an articulation of what data uses will not be subject to their preferences, and why
- Communication to individuals of the specific risks that have been taken into account, and the measures that are in place to mitigate these outcomes
- Enabling online patient communities to interact and share treatment experiences to support one another

Stakeholder considerations

Policy-makers

- Can new uses be covered by existing privacy regulations (e.g. HIPPA)? Can existing health-focused policies cover new data types?
- How can policies be coordinated globally, particularly in the context of multi-national research efforts?
- How can accountability be determined across trust boundaries and geographies?
- How can policies evolve in concert with technological progress on accountability and individual empowerment tools (e.g. recommender systems that adaptively interpret preferences)?

Industry

- How can data taxonomies be constructed that reflect the complexity of clinical and research environments while also facilitating clear communication and seamless interoperability?
- How can trust networks be established in a highly fragmented industry, and encompass both clinical and research functions?

Next steps

- Engagement of individuals through “patient empowerment” tools such as patient portals to strengthen engagement and transparency
- Further articulation of the impact of data use on individuals, moving beyond traditional medical privacy guidelines to include individuals’ perceived risks
- Development of interoperable codes of conduct that can be deployed to support trust networks between the health space and other industries

International Development

Opportunities and potential value

The increase in available public data sets provides international development and humanitarian organizations with access to effective baseline data and helps drive innovative solutions at the local level and provides citizens with more ways to be involved in their government. There is a growing consensus that data about people's actions, when coupled with advanced analytical tools and used responsibly, can contribute to social progress. Additionally, the growing trend towards open civic data provides transparency in an unprecedented manner.

Large personal data sets can provide a fine-grained representation of reality that can help development organizations understand the impact and efficacy of programmes as well as emerging needs. For example, using mobile phone data to analyse the spread of a malaria outbreak or using communications records as a proxy for levels of sub-regional development.

Opportunities for building trust

Transparency

- Articulation of the core data types that are used in a development context (e.g. mobile location, gross financial transactions, traffic mapping) to coordinate and communicate with data holders about specific needs and the safeguards for sharing data in a trusted manner
- Identification of the potential risk factors that are specific to the development context, such as corruption, ethnic tensions and displacement, and how they can be addressed to achieve social benefits
- Raising awareness to the general public on the impact and benefits of using data in innovative ways that fundamentally protect the rights and privacy of individuals

Accountability

- Coordination between data holders (e.g. mobile operators) and international development agencies on standard codes of conduct for data use that transcend local laws in jurisdictions where data protection regulation is lacking
- Development of trust marks and reputation indicators so that individuals can strengthen their trust with entities that use data about them
- Promote awareness of leading privacy and data protection best practices in the arena of international development
- Establishment of trust networks among multiple development agencies and the private sector to facilitate data exchange but also to ensure that risk management is held to the highest standard

Empowerment

- Provide individuals with applications and services that deliver genuine utility at the local level
- Tap into the "bottom up" flow of data to enrich applications which are "top down" oriented in their use of data
- Advocate for access and ethical use of real-time data sources, advanced and affordable analytics, and localized data science expertise

Stakeholder considerations

Policy-makers

- Explore how a contextual and usage-based approach in the use of personal data can be applied applied for issues related to national security
- Work to find new ways and approaches to gain the support of individuals for broad social impacts (education, logistics, weather information, market information services)
- Strengthen the engagement of national statistics experts who can leverage the insights of big data to build more adaptive and evidence-based policies

Industry

- Identify the incentive structures for industry to create APIs, which access select sets of data that address defined challenges
- Identify key business risks and the measurements that would help to reduce them so that capital could flow more effectively
- Identify data partnership opportunities where the combined sharing of data could unlock new market segments (logistics, alerting systems, reputation systems, etc.) either with other private sector actors, donors, governments or civil society actors

Next steps

- Establish linkages between core actors in the development space (including civil society, NGOs, international organizations, governments and the private sector) to engage in a structured dialogue on data usage in a development context
- Articulate the ethical and social impacts of data usage in development
- Identify target projects where collaborative approaches to managing risks can be tested, and the value of data in development demonstrated

Humanitarian Aid and Human Rights

Opportunities and potential value

Leaders within the human rights community are working to better understand the nature in which human rights, civil rights and property rights are transitioning into the digital domain. Among the issues under consideration are the role of data systems in supporting human rights work, the role of providers of data system services in settings where state and individual interests are adverse, and the nature of emerging digital-related rights as potential sources of human rights and other related topics.

One applied space where personal data has been deployed for humanitarian activities is in disaster preparedness and response. For example, mobile location data has been used to plan evacuations and to locate populations for targeted relief in natural disaster such as hurricanes and tsunamis.

Opportunities for building trust

Transparency

- Articulation of humanitarian-specific context elements (e.g. crisis levels, immediate life-threatening situations) and the impact that these have on expressed preferences and controls for particular data types and uses
- Construction of a framework for balancing the risk factors that individuals can be exposed to through personal data use with the risks faced during a humanitarian crisis
- Mapping of dynamic permissions levels so that data access levels correspond with the stages of a humanitarian intervention (e.g. access levels are highest in the immediate aftermath of a disaster, but decline as the situation becomes less fluid)

Accountability

- Creating frameworks for accountability that rebalance risk and responsibility for disaster-specific contexts
- Establishment of codes of conduct that can be adopted by major multinational players (e.g. UNHCR, IFRC) as well as institutional capabilities to support those codes that are structured to flexibly incorporate smaller human rights responders
- Risk-management procedures that are adaptive to humanitarian-specific risks, and include post-crisis closures to ensure that data leveraged for humanitarian purposes is not inappropriately transferred or used post-crisis

Empowerment

- Clear communication of data use and benefits during crisis situations, as well as post-crisis closure tools and accountability mechanisms

Stakeholder considerations

Policy-makers

- What policy frameworks can increase the coordination and interoperability of multiple private and public sector actors across geographies, and what are the implications for privacy?
- Should involvement in humanitarian initiatives by industry and individuals be voluntary or mandatory?
- How can evolving understanding of individuals' perceptions of context facilitate more rapid decision-making in humanitarian and disaster situations?

Industry

- How can participation in humanitarian initiatives be made systematic rather than ad hoc?
- Can disaster programmes be integrated with existing business continuity programmes?
- What liabilities are industry players exposed to for inappropriate data use during or after humanitarian circumstances, and how can these be managed?

Next steps

- Identification of core data types and uses to serve as a foundational taxonomy
- Exploration of the potential impacts of these uses on individuals
- Integration of taxonomies and impact assessments with existing disaster preparedness and response programs

Endnotes

[1] Nguyen, Carolyn and Haynes, Peter. "Rebalancing Socioeconomic Asymmetry in a Data-Driven Economy". *World Economic Forum Global Information Technology Report* 2013.

[2] Nissenbaum, Helen. A Contextual Approach to Privacy, *Journal of the American Academy of Arts & Sciences*, 2011.

[3] Rothenberg, Randall. "IAB Head: The Digital Advertising Industry Must Stop Having Unprotected Sex". *Business Insider*, 2014, http://www.businessinsider.com/iab-randall-rothenberg-supply-chain-2014-2.

[4] Cavoukian, Ann, *A Primer on Metadata: Separating Fact from Fiction 2013*: www.privacybydesign.ca/index.php/paper/.

[5] Cate, Fred, Cullen, Peter and Mayer-Schonberger, Viktor. "Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines". OECD Expert Roundtable Discussion, March 2014.

[6] Article 29 Working Party, The Principle of Accountability, 2010: ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf2010.

[7] *Mapping the Market for Personal Data Management Services*, Ctrl-Shift, 2014.

[8] Ibid.

[9] Mundie, Craig, *Foreign Affairs*, April 2014.

[10] Calo, Ryan. "Digital Market Manipulation". *George Washington Law Review* (forthcoming 2014).

[11] *Mapping the Market for Personal Data Management Services*, Ctrl-Shift, 2014.

[12] Lanier, Jaron, "Who Owns The Future?" Simon and Schuster, 2013.

[13] *Mapping the Market for Personal Data Management Services*, Ctrl-Shift, 2014.

[14] "Rethinking Personal Data: From Collection to Usage". World Economic Forum, 2013.

[15] "Creating a Data Ecosystem Centred on the Individual: Context and Policy". International Institute of Communications, October 2013.

[16] Rethinking Personal Data Workshop at the World Economic Forum Annual Meeting 2014 in Davos, Switzerland.

[17] Taylor, Linnet. "Hacking a Path through the Personal Data Ecosystem". December 2013, http://linnettaylor.wordpress.com/2013/12/12/hacking-a-path-through-the-personal-data-ecosystem.

[18] "More Than 50 Billion Connected Devices". Ericsson White Paper, 284 23-3149, February 2011. As cited in Nguyen, Haynes, Maguire and Friedberg, "A User-Centered Approach to the Data Dilemma: Context, Architecture, and Policy". DEF Proceedings, 2013.

[19] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012-2017, 2013. As cited in Nguyen, Haynes, Maguire and Friedberg, "A User-Centered Approach to the Data Dilemma: Context, Architecture, and Policy". DEF Proceedings 2013.

[20] Abrams, Martin. "Protecting Privacy in a Data-Driven Economy". OECD Expert Roundtable Discussion, 2014.

[21] Ibid.

[22] Ibid.

[23] Expert Interview, Ctrl-Shift, April 2014.

[24] Crompton, Malcolm. Comments made at the International Institute of Communications, October 2013.

[25] Botsman, Rachel. *The Currency of the New Economy is Trust*. TED Talks. September, 2012 https://www.youtube.com/watch?v=kTqgiF4HmgQ.

[26] Pillay, Navi. Comments made by the UN High Commissioner on Human Rights. *Guardian*. December 2013 www.theguardian.com/world/2013/dec/26/un-navi-pillay-internet-privacy.

[27] Centre for Information Policy Leadership, 2014. Insights from the Centre's Privacy Risk Framework Project and its white papers, expert interviews and conferences.

[28] Ibid.

[29] Ibid.

[30] Technology is often subject to "dread control" regulations of this phenomenon; it is not understood, so the worst thing that could go horribly wrong needs to be prevented.

[31] Recent work from Microsoft Research points to differences that can be seen in the impact of how value exchange is perceived by users in different regions of the world. For individuals from developed OECD countries that were presented scenarios of data usage, "providing a benefit to the community" was less acceptable to users than those from emerging markets where the same value renders scenarios more acceptable.

[32] Brill, Julie. "The Internet of Things: Building Trust and Maximizing Benefits through Consumer Control". March, 2014.

[33] Cate, Fred and Mayer-Schoenberger, Viktor. Proceedings from the Data Use and Impact Global Workshop, 2014.

[34] Bus, Jacques and Carolyn M-H Nguyen. "Personal Data Management – A Structured Discussion". Digital Enlightenment Forum 2013 Yearbook.

[35] Cavoukian, Ann, Time to Get Smart About Data: 2012 www.mri.gov.on.ca/blog/index.php/2012/05/cavoukian-3/.

[36] Cavoukian, Ann and Reed, Drummond: "Big Privacy: Bridging Big Data and the Personal Data Ecosystem through Privacy by Design", 2013.

[37] Ibid.

[38] "Creating a Data Ecosystem Centred on the Individual: Context and Policy". International Institute of Communications, October 2013.

[39] Clippinger,John The Social Stack and Data Privacy: ID Cubed: idcubed.org/personal-data-ecosystem/social-stack-and-data-privacy/.

[40] Crompton, Malcolm. Comments made at the International Institute of Communications, October 2013.

[41] David, Scott. University of Washington, World Economic Forum Privacy Meetings, June 2013.

[42] Acquisti, A Nudging Privacy. "The Behavioral Economics of Personal Information". IEEE Computer and Reliability Societies, 2009.

[43] Nguyen, Haynes, Maguire and Friedberg. "A User-Centred Approach to the Data Dilemma: Context, Architecture, and Policy". DEF Proceedings, 2013.

[44] Labaco, Ron. Out of Hand, Materializing the Postdigital. Museum of Arts and Design, February 2014

[45] Diakopoulos, Nicholas. Algorithmic Accountability Reporting on the Investigation of Black Boxes, 2013.

[46] Lohr, Steve. The Promise and Peril of the 'Data-Driven Society, New York Times, February 2013.

[47] Ibid.

[48] Nguyen, Haynes, Maguire and Friedberg. "A User-Centred Approach to the Data Dilemma: Context, Architecture, and Policy". DEF Proceedings, 2013.

[49] Hildebrandt, Mireille. "Profiling into the future: An assessment of profiling technologies in the context of ambient intelligence". Digital Enlightenment Yearbook 2012, J. Bus et al. (Eds.). IOS Press, 2012.

[50] Pentland, Alexander, Social Physics, How Good Ideas Spread.The Lessons from a New Science". Penguin Press, 2014.

[51] Tennenhouse, David. "Proactive Computing". Communications of the ACM, May 2000.

[52] Clippinger, John Henry. The Windhover Accords, September 2013.

[53] O'Reilly, Tim. September 19, 2011, https://plus.google.com/+TimOReilly/posts/CPi-AX9YiVUB.

[54] Morozov, Evgeny. "The Real Privacy Problem". MIT Technology Review, 22 October 2013. The need for meaningful responses when individuals are treated differentially by automated recommendation systems has had wide support in the literature for a number years. See Danielle Citron (2008), Eli Pariser (2011), Cynthia Dwork (2013) and Deirdre Mulligan (2013) for additional insights.

[55] Calo, Ryan. "Digital Market Manipulation". *George Washington Law Review* (forthcoming 2014).

[56] Ibid.

[57] Ibid.

[58] Social Media Week 2014. Impulse Response, A Strategic Approach to Algorithmic Encounters. Hosted by the *New York Times* R&D Lab.

[59] Hildebrandt, Mireille. "Profiling into the future: An assessment of profiling technologies in the context of ambient intelligence". Digital Enlightenment Yearbook 2012, J. Bus et al. (Eds.). IOS Press, 2012.

[60] Calo, Ryan. "Consumer Subject Review Boards: A Thought Experiment". *Stanford Law Review*, September 2013.

Acknowledgments

The World Economic Forum would like to acknowledge the support of all those who contributed to this initiative in 2013 and 2014. The global dialogue series included sessions in New York, USA; Dublin, Ireland; London, United Kingdom; Dalian, People's Republic of China; Brussels, Belgium; Abu Dhabi, United Arab Emirates; and Davos, Switzerland.

The project engaged a multistakeholder community across government, the private sector, civil society, academia and others throughout the dialogue series and through its Working Group.

Special thanks are extended to all those who supported these events and joined regular Working Group calls with their insights and collaborative spirit including: AT Kearney, AT&T, Axciom, BT Group, Centre for Information Policy Leadership, Cisco, Ctrl-Shift, Digital Enlightenment Forum, European Commission, Future of Privacy Forum, Google, GSMA, HP, ID3, Intel, Kaiser Permanente, Microsoft, MIT, Mydex CIC, Orange, Personal, Personal Data Ecosystem Consortium, Planetary Skin Institute, Qualcomm, Reputation.com, Respect Network, Rhode Island School of Design (RISD), STL Partners, Telecom Italia, Telefonica, UN Global Pulse, University of Washington, US Federal Trade Commission, Ushahidi, US National Institute of Standards and Technology, Vimpelcom and Visa.

Editorial input for this report was provided by the Steering Board members and their respective teams. Members of the Steering Board are as follows:

Robert Quinn, Senior Vice-President, Federal Regulatory and Chief Privacy Officer, AT&T, USA

Ray Baxter, Senior Vice-President for Community Benefit, Research and Health Policy, Kaiser Permanente, USA

Anoop Gupta, Distinguished Scientist, Technology Policy Group, Microsoft, USA

Augie K. Fabela II, Co-Founder and Chairman Emeritus, VimpelCom, Netherlands

Ellen Richey, Executive Vice President and Chief Legal Officer, Visa Inc., USA

At the World Economic Forum, William Hoffman leads the Rethinking Personal Data initiative and was the principle author of the report. A.T. Kearney served as the project adviser in 2013 under the leadership of Naveen Menon, Reuben Chaudhury and Justin Shepherd, who was seconded to the World Economic Forum. Ryan Murphy of the Rhode Island School of Design served as the chief design consultant. Special thanks to the Center for Information Policy Leadership and the Information Accountability Foundation for their support and guidance. Additionally, Carolyn Nguyen of Microsoft and Jamie Ferguson of Kaiser Permanente played an invaluable role in guiding this report and the overall initiative. Thanks also to the Global Agenda Council on Data-Driven Development, especially John Clippinger, ID3; Scott David, University of Washington; Marc Davis, Marcdavis.me; Sandy Pentland, MIT Media Lab; and Simon Torrance STL Partners for their ongoing advice and guidance.

For more information, contact William Hoffman, Associate Director, by email at william.hoffman@weforum.org

Visit http://www.weforum.org/personaldata

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum is an international institution committed to improving the state of the world through public-private cooperation in the spirit of global citizenship. It engages with business, political, academic and other leaders of society to shape global, regional and industry agendas.

Incorporated as a not-for-profit foundation in 1971 and headquartered in Geneva, Switzerland, the Forum is independent, impartial and not tied to any interests. It cooperates closely with all leading international organizations.

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel +41 (0) 22 869 1212
Fax +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org