WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Personal Data: The Emergence of a New Asset Class

An Initiative of the World Economic Forum
January 2011

In Collaboration with Bain & Company, Inc.

Title picture by frog design inc.

Acknowledgements

This document was prepared by the World Economic Forum, in partnership with the individuals and organisations listed below.

World Economic Forum

Professor Klaus Schwab	Executive Chairman
Alan Marcus	Senior Director, IT & Telecommunications Industries
Justin Rico Oyola	Associate Director and Project Lead, Telecommunications Industry
William Hoffman	Head, Telecommunications Industry

Bain & Company, Inc.

Michele Luzi	Director

The following experts contributed substantial research and interviews throughout the “Rethinking Personal Data” project. We extend our sincere gratitude to all of them.

Julius Akinyemi	MIT
Alberto Calero	France Telecom
Ron Carpinella	Equifax
Chris Conley	ACLU
Douglas Dabérius	Nokia Siemens Networks
Timothy Edgar	Office of the Director of National Intelligence, USA
Jamie Ferguson	Kaiser Permanente
Michael Fertik	ReputationDefender
Tal Givoly	Amdocs
Kaliya Hamlin	Personal Data Ecosystem
William Heath	Mydex
Trevor Hughes	International Association of Privacy Professionals
Betsy Masiello	Google
Mita Mitra	BT Group
Drummond Reed	Information Card Foundation
Nasrin Rezai	Cisco
Natsuhiko Sakimura	OpenID Foundation
Kevin Stanton	MasterCard Advisors
Pamela Warren	McAfee
Von Wright	AT&T

Project Steering Board

This work would also not have been possible without the commitment of:

John Clippinger	Berkman Center for Internet and Society, Harvard University
Scott David	K&L Gates
Marc Davis	Microsoft
Robert Fabricant	frog design
Philip Laidler	STL Partners
Alexander (Sandy) Pentland	MIT
Fabio Sergio	frog design
Simon Torrance	STL Partners

Table of Content

Introduction

We are moving towards a "Web of the world" in which mobile communications, social technologies and sensors are connecting people, the Internet and the physical world into one interconnected network.[1] Data records are collected on who we are, who we know, where we are, where we have been and where we plan to go. Mining and analysing this data give us the ability to understand and even predict where humans focus their attention and activity at the individual, group and global level.

"Personal data is the new oil of the Internet and the new currency of the digital world."

Meglena Kuneva, European Consumer Commissioner, March 2009

This personal data – digital data created by and about people – is generating a new wave of opportunity for economic and societal value creation. The types, quantity and value of personal data being collected are vast: our profiles and demographic data from bank accounts to medical records to employment data. Our Web searches and sites visited, including our likes and dislikes and purchase histories. Our tweets, texts, emails, phone calls, photos and videos as well as the coordinates of our real-world locations. The list continues to grow. Firms collect and use this data to support individualised service-delivery business models that can be monetised. Governments employ personal data to provide critical public services more efficiently and effectively. Researchers accelerate the development of new drugs and treatment protocols. End users benefit from free, personalised consumer experiences such as Internet search, social networking or buying recommendations.

And that is just the beginning. Increasing the control that individuals have over the manner in which their personal data is collected, managed and shared will spur a host of new services and applications. As some put it, personal data will be the new "oil" – a valuable resource of the 21st century. It will emerge as a new asset class touching all aspects of society.

At its core, personal data represents a post-industrial opportunity. It has unprecedented complexity, velocity and global reach. Utilising a ubiquitous communications infrastructure, the personal data opportunity will emerge in a world where nearly everyone and everything are connected in real time. That will require a highly reliable, secure and available infrastructure at its core and robust innovation at the edge. Stakeholders will need to embrace the uncertainty, ambiguity and risk of an emerging ecosystem. In many ways, this opportunity will resemble a living entity and will require new ways of adapting and responding. Most importantly, it will demand a new way of thinking about individuals.

[1] Many of these concepts and background information have been introduced in: Davis, Marc, Ron Martinez and Chris Kalaboukis. "Rethinking Personal Information – Workshop Pre-read." Invention Arts and World Economic Forum, June 2010.

Indeed, rethinking the central importance of the individual is fundamental to the transformational nature of this opportunity because that will spur solutions and insights.

As personal data increasingly becomes a critical source of innovation and value, business boundaries are being redrawn. Profit pools, too, are shifting towards companies that automate and mine the vast amounts of data we continue to generate.[2] Far from certain, however, is how much value will ultimately be created, and who will gain from it. The underlying regulatory, business and technological issues are highly complex, interdependent and ever changing.

But further advances are at risk. The rapid rate of technological change and commercialisation in using personal data is undermining end user confidence and trust. Tensions are rising. Concerns about the misuse of personal data continue to grow. Also mounting is a general public unease about what "they" know about us.[3] Fundamental questions about privacy, property, global governance, human rights – essentially around who should benefit from the products and services built upon personal data – are major uncertainties shaping the opportunity. Yet, we can't just hit the "pause button" and let these issues sort themselves out. Building the legal, cultural, technological and economic infrastructure to enable the development of a balanced personal data ecosystem is vitally important to improving the state of the world.

It is in this context that the World Economic Forum launched a project entitled "Rethinking Personal Data" in 2010. The intent of this multiyear project is to bring together a diverse set of stakeholders – private companies, public sector representatives, end user privacy and rights groups, academics and topic experts. The aim is to deepen the collective understanding of how a principled, collaborative and balanced personal data ecosystem can evolve. In particular, this initiative aims to:

- Establish a user-centric framework for identifying the opportunities, risks and collaborative responses in the use of personal data;

- Foster a rich and collaborative exchange of knowledge in the development of cases and pilot studies;

- Develop a guiding set of global principles to help in the evolution of a balanced personal data ecosystem.

[2] Bain & Company Industry Brief. "Using Data as a Hidden Asset." August 16, 2010.
[3] Angwin, Julia. "The Web's New Gold Mine: Your Secrets." *Wall Street Journal.* July 30, 2010. http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html

Executive Summary

Personal data: untapped opportunities for socioeconomic growth

The rate of increase in the amount of data generated by today's digital society is astounding. According to one estimate, by 2020 the global volume of digital data will increase more than 40-fold.[4] Beyond its sheer volume, data is becoming a new type of raw material that's on par with capital and labour.[5] As this data revolution era begins, the impact on all aspects of society – business, science, government and entertainment – will be profound.

Personal data – a definition

For this report personal data is defined as data (and metadata) created by and about people, encompassing:

- Volunteered data – created and explicitly shared by individuals, e.g., social network profiles.
- Observed data – captured by recording the actions of individuals, e.g., location data when using cell phones.
- Inferred data – data about individuals based on analysis of volunteered or observed information, e.g., credit scores.

Source: World Economic Forum, June 2010.

From a private sector perspective, some of the largest Internet companies such as Google, Facebook and Twitter clearly show the importance of collecting, aggregating, analysing and monetising personal data. These rapidly growing enterprises are built on the economics of personal data.

Governments and public sector institutions are also transforming themselves to use data as a public utility. Many governments have successfully launched e-governance initiatives to improve the efficiency and effectiveness of communication among various public organisations – and with citizens.

But some of the most profound insights are coming from understanding how individuals themselves are creating, sharing and using personal data. On an average day, users globally send around 47 billion (non-spam) emails[6] and submit 95 million "tweets" on Twitter. Each month, users share about 30 billion pieces of content on Facebook.[7] The impact of this "empowered individual" is just beginning to be felt.

However, the potential of personal data goes well beyond these promising beginnings to vast untapped wealth creation opportunities. But unlocking this value depends on several contingencies. The underlying regulatory, business and technological issues are highly complex, interdependent and ever changing.

[4] IDC. "The Digital Universe Decade – Are You Ready?" May 2010.
[5] *The Economist*. "Data, Data Everywhere." February 25, 2010.
[6] The Radicati Group. "Email Statistics Report, 2009–2013." May 2009.
[7] "Twitter + Ping = Discovering More Music." Twitter Blog. November 11, 2010; "Statistics." Facebook Press Room. January 11, 2011. http://www.facebook.com/press/info.php?statistics

The personal data ecosystem – where we stand today

The current personal data ecosystem is fragmented and inefficient. For many participants, the risks and liabilities exceed the economic returns. Personal privacy concerns are inadequately addressed. Regulators, advocates and corporations all grapple with complex and outdated regulations.

Current technologies and laws fall short of providing the legal and technical infrastructure needed to support a well-functioning digital economy. Instead, they represent a patchwork of solutions for collecting and using personal data in support of different institutional aims, and subject to different jurisdictional rules and regulatory contexts (e.g., personal data systems related to banking have different purposes and applicable laws than those developed for the telecom and healthcare sectors).

Consider some of the needs and interests of stakeholders:

Private sector

Private enterprises use personal data to create new efficiencies, stimulate demand, build relationships and generate revenue and profit from their services. But in this drive to develop the "attention economy", enterprises run the risk of violating customer trust. Overstepping the boundary of what users consider fair use can unleash a huge backlash with significant brand implications.

Public sector

Governments and regulators play a vital role in influencing the size and shape of the personal data ecosystem as well as the value created by it. On the one hand, regulators have the mandate to protect the data security and privacy rights of citizens. Therefore, they seek to protect consumers from the potential misuse of their identity. On the other hand, regulators balance this mandate with the need to foster economic growth and promote public well-being. Policy makers around the world are engaged in discussions to enhance legal and regulatory frameworks that will increase disclosure rules, maximise end user control over personal data and penalise non-appropriate usage. Finally, government agencies are using personal data to deliver an array of services for health, education, welfare and law enforcement. The public sector is therefore not just an active player in the personal data universe, but also a stimulator and shaper of the ecosystem – and potentially, the creator of tremendous value for individuals, businesses and economies.

Individuals

Behaviours and attitudes towards personal data are highly fragmented. Demographically, individuals differ in their need for transparency, control and the ability to extract value from the various types of personal data

Common needs for all users

- Reliability
- Predictability
- Interoperability
- Security
- Ease of use
- Cost-effectiveness
- Risk and liability reduction
- Transparency
- Simplicity

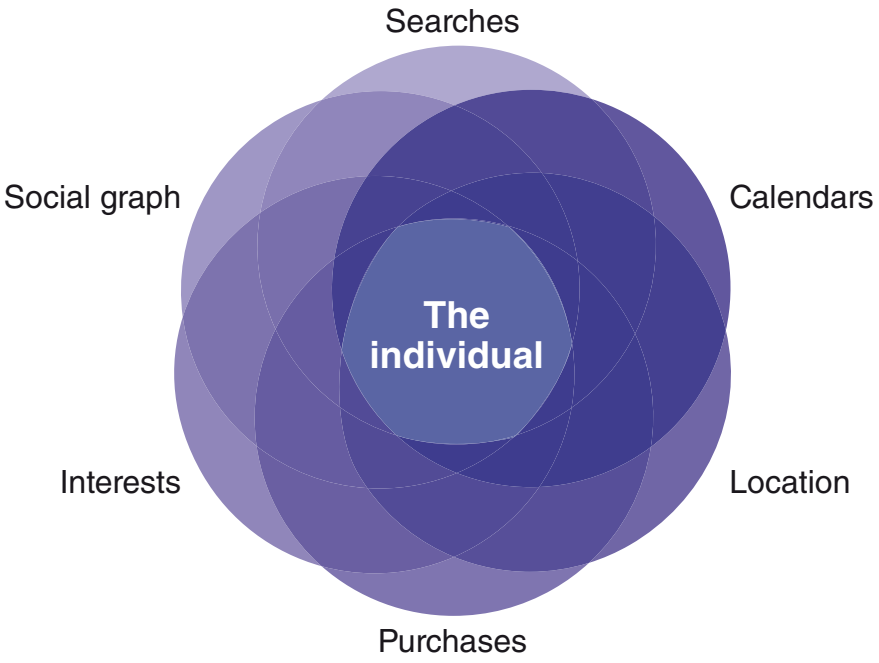
(see Figure 1). According to the research firm International Data Corporation (IDC), individuals' direct or indirect actions generated about 70 per cent of the digital data created in 2010. Activities such as sending an email, taking a digital picture, turning on a mobile phone or posting content online made up this huge volume of data. Younger individuals are more comfortable sharing their data with third parties and social networks – though it remains to be seen whether their behaviours will remain the same or become more risk averse as they age. Older consumers appear to be more sceptical, and demand demonstrably higher security levels from service providers.[8]

Individuals are also becoming more aware of the consequences of not having control over their digital identity and personal data. In 2010 the number of reported incidents of identity theft skyrocketed by 12 per cent.[9]

A way forward: the personal data ecosystem

One viable response to this fragmentation is to align key stakeholders (people, private firms and the public sector) in support of one another. Indeed, "win-win-win" outcomes will come from creating mutually supportive incentives, reducing collective inefficiencies and innovating in such a way that collective risks are reduced.

Figure 1: Individual end users are at the center of diverse types of personal data



Source: Davis, Marc, Ron Martinez and Chris Kalaboukis. "Rethinking Personal Information – Workshop Pre-read." Invention Arts and World Economic Forum, June 2010.

[8] Nokia Siemens Networks. "Digital Safety, Putting Trust into the Customer Experience." *Unite Magazine*. Issue 7. http://www.nokiasiemensnetworks.com/news-events/publications/unite-magazine-february-2010/digital-safety-putting-trust-into-the-customer
[9] Javelin Strategy & Research. "The 2010 Identity Fraud Survey Report." February 10, 2010.

This vision includes a future where:

- Individuals can have greater control over their personal data, digital identity and online privacy, and they would be better compensated for providing others with access to their personal data;

- Disparate silos of personal data held in corporations and government agencies will more easily be exchanged to increase utility and trust among people, private firms and the public sector;

- Government's need to maintain stability, security and individual rights will be met in a more flexible, holistic and adaptive manner.

In practical terms, a person's data would be equivalent to their "money." It would reside in an account where it would be controlled, managed, exchanged and accounted for just like personal banking services operate today. These services would be interoperable so that the data could be exchanged with other institutions and individuals globally. As an essential requirement, the services would operate over a technical and legal infrastructure that is highly trusted. Maintaining confidence in the integrity, confidentiality, transparency and security of the entire system would require high levels of monitoring.

End user-centricity: a critical determinant in building the personal data ecosystem

A key element for aligning stakeholder interests and realising the vision of the personal data ecosystem is the concept of end user-centricity. This is a holistic approach that recognises that end users are vital and independent stakeholders in the co-creation and value exchange of services and experiences. A construct designed for the information economy, it breaks from the industrial-age model of the "consumer" – where relationships are captured, developed and owned.

Instead, end user-centricity represents a transformational opportunity. It seeks to integrate diverse types of personal data in a way that was never possible before. This can only be done by putting the end user at the centre of four key principles:

- Transparency: Individuals expect to know what data is being captured about them, the manner in which such data is captured or inferred, the uses it will be put to and the parties that have access to it;

- Trust: Individuals' confidence that the attributes of availability, reliability, integrity and security are embraced in the applications, systems and providers that have access to their personal data;

- Control: The ability of individuals to effectively manage the extent to which their personal data is shared;

- Value: Individuals' understanding of the value created by the use of their data and the way in which they are compensated for it.

Complex business, policy and technological issues persist and require coordinated leadership from firms and the public sector

A user-centric ecosystem faces challenges almost as big as its promise, however. Firms, policy makers and governments must resolve a series of critical questions.

For private firms, what are the concrete economic incentives to "empower" individuals with greater choice and control over how their data are used? What are the incentives for greater collaboration within and across industry sectors? How can the returns from using personal data begin to outweigh the risks from a technical, legal and brand-trust perspective?

Policy makers are unique in their mandate to collect, manage and store personal data for purposes such as national defence, security and public safety. They face the issue of finding the right balance between competing priorities: How can they ensure the stability and security of government even as they create incentives for economic investment and innovation? How should they define end users' rights and permissions concerning personal data? How can they more effectively clarify the liabilities? How can they scale globally the concepts of accountability and due process?

Five areas of collective action

The issues surrounding personal data – political, technological and commercial alike – are numerous and complex. The choices stakeholders make today will influence the personal data ecosystem for years to come. Five key imperatives require action:

1. Innovate around user-centricity and trust. The personal data ecosystem will be built on the trust and control individuals have in sharing their data. From a technological, policy and sociological sense all stakeholders need to embrace this construct. One particular area of focus is the continued testing and promoting of "trust frameworks" that explore innovative approaches for identity assurance at Internet scale.

2. Define global principles for using and sharing personal data. Given the lack of globally accepted policies governing the use and exchange of personal data, an international community of stakeholders should articulate and advance core principles of a user-centric personal data ecosystem. These pilots should invite real-world input from a diverse group of individuals who can not only articulate the values, needs and desires of end users, but also the complex and contextual nuances involved in revealing one's digital identity.

3. Strengthen the dialog between regulators and the private sector. Building on a collective sense of fundamental principles for creating a balanced ecosystem, public and private stakeholders should actively collaborate as the ecosystem begins to take shape. Those responsible for building and deploying the tools (the technologists) should more closely align with those making the rules (regulators).[10] Establishing the processes to

[10] David, Scott. K&L Gates and Open Identity Exchange ABA Document. October 20, 2010.

enable stakeholders to formulate, adopt and update a standardised set of rules will serve to create a basic legal infrastructure. Additionally, collaborating with policy makers as they update legislation to address key questions related to identity and personal data will be essential.[11]

4. Focus on interoperability and open standards. With the appropriate user controls and legal infrastructure in place, innovations in how personal data moves throughout the value chain will be a key driver for societal and economic value creation. Enabling a secure, trusted, reliable and open infrastructure (both legal and technical) will be vital. Participants should identify best practises and engage with standards bodies, advocacy groups, think tanks and various consortia on the user-centric approaches required to scale the value of personal data.

5. Continually share knowledge. It's a huge challenge for entities to keep up with new research, policies and commercial developments. To stay current, stakeholders should share insights and learnings on their relevant activities, from both successes as well as failures. After all, the ecosystem's promise is about the tremendous value created when individuals share information about who they are and what they know. Clearly, this principle should also apply to practitioners within the development community.

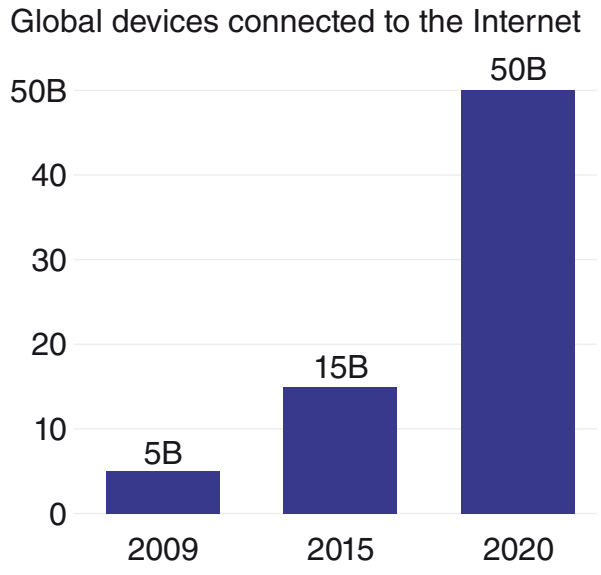
[11] In the US, recent developments emerging from the NSTIC, the Federal Trade Commission and the Department of Commerce warrant attention. In the EU, companies should work with the European Commission's efforts to revise the EU privacy directive and to synchronise legislation across its member states.

Section 1: Personal Data Ecosystem: Overview

Personal data is an evolving and multifaceted opportunity

In the era of "anywhere, anytime" connectivity, more people connect to the Internet now in more ways than ever before. One recent estimate projects that in the next 10 years, more than 50 billion devices may connect to the Internet, many wirelessly (see Figure 2).[12] Global traffic on mobile networks is expected to double each year through 2014.[13]

Figure 2: By 2020, more than 50 billion devices will be connected to the Internet



Sources: Ericsson, Intel

The variety and volume of digital records that can be created, processed and analysed will continue to increase dramatically. By 2020, IDC estimates that the global amount of digital records will increase more than 40-fold (see Figure 3).[14]

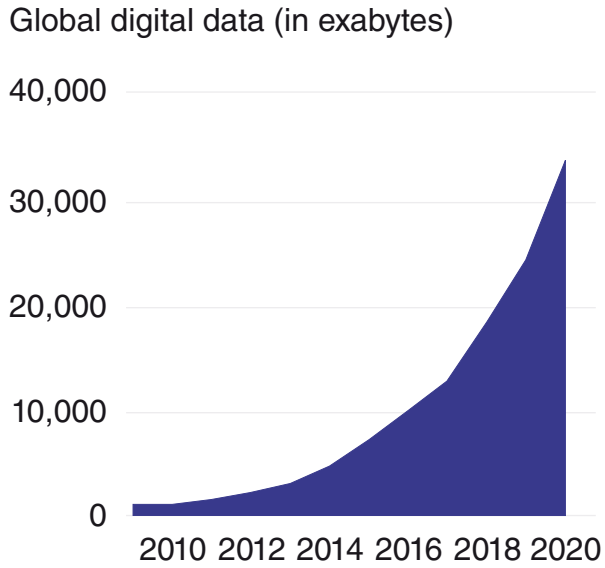
As these devices and software continue to come online, they will generate an increasing amount of personal data. The term personal data has several meanings, but we broadly define it as data relating to an identified or identifiable person or persons.[15]

Think of personal data as the digital record of "everything a person makes and does online and in the world."[16] The wide variety of forms that such data assumes for storage and communication evolves constantly, but an initial list of categories includes:

- Digital identity (for example, names, email addresses, phone numbers, physical addresses, demographic information, social network profile information and the like);

[12] Ericsson [press release]. "CEO to Shareholders: 50 Billion Connections 2020." April 13, 2010.
[13] Cisco. "Cisco Visual Networking Index: Global Mobile Data; Traffic Forecast Update, 2009 – 2014." February 9, 2010.
[14] IDC. "The Digital Universe Decade – Are You Ready?" May 2010.
[15] Definition based on Directive 95/46/EC of the European Parliament and the Council of 24, October 1995.
[16] Davis, Marc, Ron Martinez and Chris Kalaboukis. "Rethinking Personal Information – Workshop Pre-read." Invention Arts and World Economic Forum, June 2010.

FIGURE 3: BY 2020, DIGITAL RECORDS WILL BE 44 TIMES LARGER THAN IN 2009



Source: IDC

- Relationships to other people and organisations (online profiles and contact lists);
- Real-world and online context, activity, interests and behaviour (records of location, time, clicks, searches, browser histories and calendar data);
- Communications data and logs (emails, SMS, phone calls, IM and social network posts);
- Media produced, consumed and shared (in-text, audio, photo, video and other forms of media);
- Financial data (transactions, accounts, credit scores, physical assets and virtual goods);
- Health data (medical history, medical device logs, prescriptions and health insurance coverage);
- Institutional data (governmental, academic and employer data).

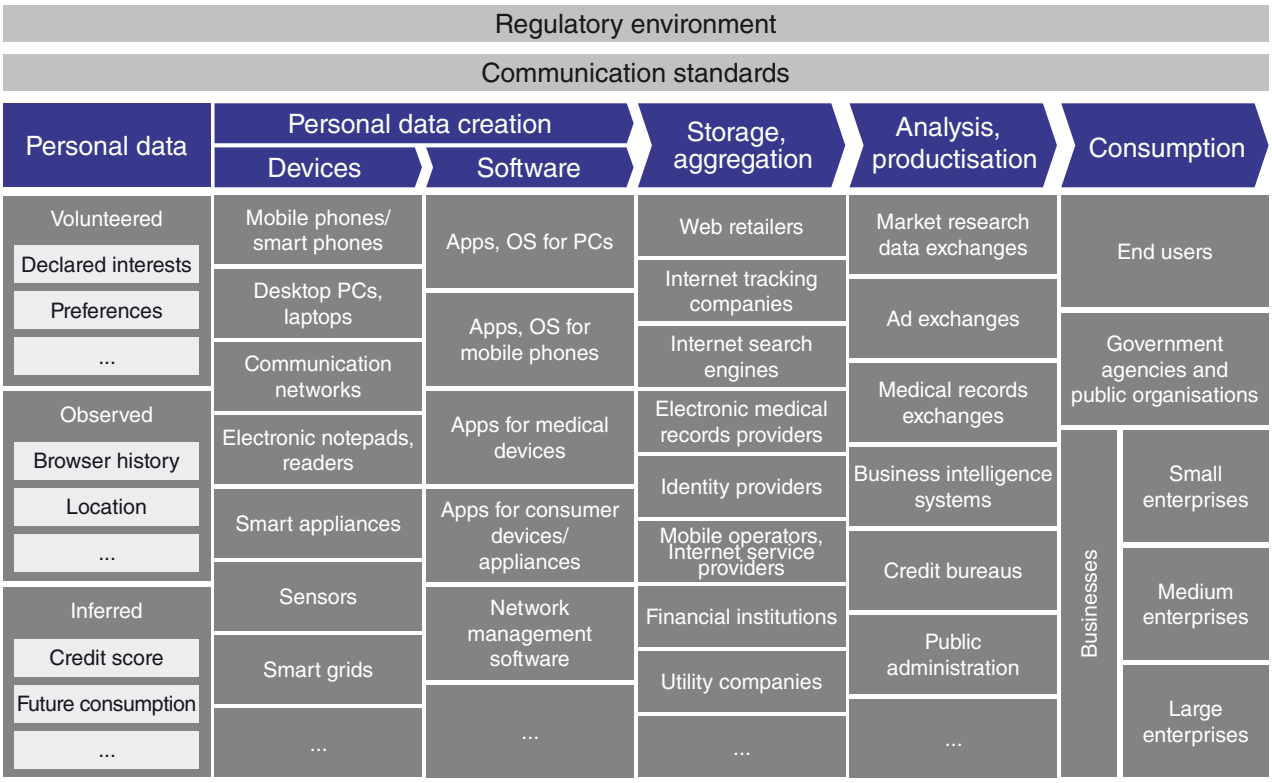
Further, organisations can capture these different personal data in a variety of ways:[17]

- Data can be "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;
- "Observed" data is captured by recording activities of users (in contrast to data they volunteer). Examples include Internet browsing preferences, location data when using cell phones or telephone usage behaviour;
- Organisations can also discern "inferred" data from individuals, based on the analysis of personal data. For instance, credit scores can be calculated based on a number of factors relevant to an individual's financial history.

Each type of personal data (see Figure 4), volunteered, observed or inferred, can be created by multiple sources (devices, software applications), stored and aggregated by various providers (Web retailers, Internet search engines or utility companies) and analysed for a variety of purposes for many different users (end users, businesses, public organisations).

[17] Ibid.

FIGURE 4: THE PERSONAL DATA ECOSYSTEM: A COMPLEX WEB FROM DATA CREATION TO DATA CONSUMPTION



Source: Bain & Company

These stakeholders range from the individual end users, who are the sources and subjects of personal data, to the various entities with which they interact. The latter encompass businesses and corporations in different industries to public sector entities like government bodies, NGOs and academia. Personal data flows through this ecosystem, within the boundaries of regulation, to result ultimately in exchanges of monetary and other value.

POINTS OF TENSION AND UNCERTAINTY

While tremendous value resides in the data generated by different sources, it often remains untapped. Unlocking the full potential of data will require addressing current uncertainties and points of tension:

- Privacy: Individual needs for privacy vary. Policy makers face a complex challenge while developing legislation and regulations;
- Global governance: There is a lack of global legal interoperability, with each country evolving its own legal and regulatory frameworks;
- Personal data ownership: The concept of property rights is not easily extended to data, creating challenges in establishing usage rights;

- Transparency: Too much transparency too soon presents as much a risk to destabilising the personal data ecosystem as too little transparency;

- Value distribution: Even before value can be shared more equitably, much more clarity will be required on what truly constitutes value for each stakeholder.

Privacy

Privacy continues to be a highly publicised, complex and sensitive issue with multiple perspectives. The complexity surrounding how privacy is conceived and defined creates challenges for policy makers as they seek to address a myriad of issues related to context, culture and personal preference.[18] Adding to the complexity is the pace of technological change and a general lack of guidance on how to accommodate and support various perspectives on "privacy" robustly, flexibly and at global scale (for multiple jurisdictions, cultures and commercial and social settings).[19] Given that many governments are drafting laws and regulations to address privacy concerns, the ambiguity and uncertainty on multiple dimensions heighten the risks that could stall investment and innovation.

"We need to arrive at an acceptable reasonable expectation of privacy … a procedural due process that has the flexibility to address any question of privacy and institutionalise learnings into the ecosystem to prevent that grievance from happening again."

Interviewee, "Rethinking Personal Data" project

Global governance

Not only are policies and legislation in flux within national borders, there is wide variation across different countries and regions. Indeed, there is no global consensus on two major questions: Which issues related to personal data should be covered by legal and regulatory frameworks? And how should those issues be addressed? While some cross-national agreements exist, for example, the Safe Harbor agreement between the US and the EU,[20] the development of a globally acceptable view of the personal data ecosystem may be years away. This fragmentation stands in the way of fully realising the global impact of the personal data opportunity.

Personal data ownership

"Who owns the data" and "What rights does ownership imply" are two of the most complex issues related to personal data. At first blush, these questions seem simple. Most people would intuitively assert that they own data about themselves and that therefore, they should control who can access, use, aggregate, edit and share it. However, even a cursory look at the issue quickly reveals that the answers are much less clear. Individuals do not "own" their criminal records or credit history. Medical providers are required to keep certain records about patients, even

[18] "Fair Information Practice Principles (FIPP) Comparison Tool, Draft." Discussion and Development Materials of the OIX Advisory Board and the OIX Legal Policy Group. October 7, 2010.
[19] Ibid.
[20] In 2000, the US and the European Commission agreed upon a framework that would act as a bridge for sharing data between the US and EU, while preserving the basic policy principles of both. See, for example, Thompson, Mozelle W., Peder van Wagonen Magee. "US/EU Safe Harbor Agreement: What It Is and What It Says About the Future of Cross Border Data Protection." Privacy Regulation. Federal Trade Commission, Spring 2003. http://www.ftc.gov/speeches/thompson/thompsonsafeharbor.pdf

as those patients are allowed to access and share that information with others. Do companies such as Google and Amazon, which aggregate search and purchase histories across millions of users, own the proprietary algorithms they've built upon those click streams?

Given the fluid nature of data and the early stages of the personal data ecosystem, many assert that focusing on the issues of rights management, accountability, due process and the formation of "interoperable" legal frameworks is more productive. It is unlikely that there is a one-size-fits-all approach. A more likely scenario is that different classes of information (financial, health, government records, social, etc.) will get varying degrees of protection – as already is the case in the "pre-digital" world. All such solutions will need to balance individuals' rights to privacy with practical concerns about legitimate needs for critical participants (for example, law enforcement and medical personnel) to access key information when necessary. In addition, practical solutions for issues related to data portability, interoperability and easy-to-implement dashboards for consumers to set and monitor access rights will also need to be developed to overcome the growing friction in the current environment.

Transparency

Most end users still remain unaware of just how much they are tagged, tracked and followed on the Internet. Few individuals realise how much data they implicitly give away, how that data might be used or even what is known about them. Some businesses believe the solution lies in "fessing up": simply increasing the transparency on how personal data is used. But that approach not only fails to address the privacy and trust concerns end users have; for many organisations, it often poses a risk to their business model. When customers suddenly find out how their trusted brand of product or service was gathering and using their personal data, they tend to react with outrage, rather than reward the business for its transparency. Similarly, citizens fear Big Brother control and manipulation in the way government uses their personal information. As long as the risk of transparency outweighs the rewards, the personal data ecosystem will remain vulnerable to periodic seismic shocks.

Value distribution

The notion that individuals are producers, creators and owners of their digital activities raises the question: How can value be equitably exchanged? The answer depends on variables like the structure of personal data markets; the amount of public educa-

Personal data and developing economies

As with many innovations related to mobile applications, the development of personal data exchanges could achieve scale in developing economies. The data and analytics from the increasing use of mobile devices – in particular, location data, images from cell phone cameras and mobile finance – can help countries address significant economic and health challenges with greater precision and adaptability. As the mobile platform brings the unbanked into the formal economy, real-time insights into local economies could be gained. Utilising the analytics of m-Health applications could also help improve public health.

tion required; globally governed regulations needed to ensure fair compensation; and the legal frameworks that would ensure accountability and due process.

Uncertainty and tension also exist around the evolution of personal data exchanges and the degree of political empowerment they could create. Some governments can perceive empowered citizens as a disruptive threat to their agenda. Understanding the concept of user-centricity in the context of differing social, cultural and political norms is clearly needed.

Incumbents and disrupters

During the last few decades, a regulatory patchwork has arisen that does not adequately reflect the needs of a competitive global market or the pace of technology. The personal data ecosystem consists of established and new participants; often the regulatory framework covers established business models, but regulation takes time to catch up with emerging, disruptive models. From a regulatory perspective, this can create a fundamentally uneven competitive playing field for creating new personal data services. Companies with established business models – those with large customer bases, legacy investments and trusted brands – typically possess vast amounts of customer data but are legally constrained on its use for commercial purposes. Given those legal constraints, established players are generally conservative in their approach to the market and deeply concerned about unclear liabilities and legal inconsistencies.

On the other hand, many new services and applications are more innovative in their approach and typically use personal data as a central component in their business models. By definition, they tend to fall outside the purview of legacy legal restrictions and typically innovate at the edges of what can be legally done with personal data. A growing concern is the widening chasm between the regulatory oversight on established business models versus new business ideas. Additionally, there are concerns on how current legal and regulatory stakeholders can systemically adapt to the velocity of innovation, the complexity of the ecosystem and the scale of personal impact. Given that a single operational or technical change to a networked communications service can immediately impact hundreds of millions of individuals (if not billions), the capability of policy makers and regulators to understand a given risk and adapt in real time is uncertain. Over time, perceptions of over-regulation and inequity on who can use certain forms of personal data for commercial purposes may create an imbalance among private sector actors.

The risks of an imbalanced ecosystem

The key to unlocking the full potential of data lies in creating equilibrium among the various stakeholders influencing the personal data ecosystem. A lack of balance between stakeholder interests – business, government and individuals – can destabilise the personal data ecosystem in a way that erodes rather than creates value. What follows are just a few possible outcomes that could emerge if any one set of stakeholders gained too strong a role in the ecosystem.

The risk of private sector imbalance

As personal data becomes a primary currency of the digital economy, its use as a

means to create competitive advantage will increase. If little regard is paid to the needs of other stakeholders, businesses searching for innovative ways to collect, aggregate and use data could end up engaging in a "race to the bottom", building out ever more sophisticated "tricks and traps" to capture personal data.[21] This unfettered mining of personal data would alienate end users and possibly create a backlash.[22]

The risk of public sector imbalance

As countries revise their legal frameworks, policies and regulations to catch up with the unprecedented surge in data, they could inadvertently stifle value creation by over-regulating. Additionally, individual countries may seek to act unilaterally to protect their own citizens from potential harm. The resulting lack of clarity and consistency in policy across countries could slow down innovation and investment.

The risk of end user imbalance

In the absence of engagement with both governments and business, end users could self-organise and create non-commercial alternatives for how their personal data is used. While small groups of dedicated individuals could collaborate on non-commercial products that have the same impact as Wikipedia and Linux, the issues of limited funding, security and lack of governance would remain. Over time, the challenges of managing personal data at a global scale could become overwhelming.

Aligning the different interests to create a true "win-win-win" state for all stakeholders represents a challenge – but it can be done. The solution lies in developing policies, incentives and rewards that motivate all stakeholders – private firms, policy makers, end users – to participate in the creation, protection, sharing and value generation from personal data. The private and public sectors can bring their interests closer by creating an infrastructure that enables the secure and efficient sharing of data across organisations and technologies. End users can be gathered into the fold of the private-public partnership by developing mechanisms that safeguard personal data, validate their content and integrity, and protect ownership. When end users begin to get a share of the value created from their personal data, they will gain more confidence in sharing it.

For such a virtuous cycle to evolve, stakeholders in the personal data ecosystem will need to define new roles and opportunities for the private and public sectors. Greater mutual trust can lead to increased information flows, value creation, and reduced litigation and regulatory costs.

Over time, all stakeholders should hopefully recognise that the collective metric of success is the overall growth of the ecosystem rather than the success of one specific participant. A defining characteristic of such a balanced ecosystem would be end user choice. With the ability to switch easily between vendors, competitive pressures would strengthen the control of the end users and help them differentiate between different trust frameworks and service providers.

[21] Clippinger, John. Berkman Center for Internet & Society at Harvard University.
[22] To learn more about how companies are using new and intrusive Internet-tracking technologies, see "What They Know" (series). *Wall Street Journal.* 2010. http://online.wsj.com/public/page/what-they-know-digital-privacy.html

Future Potential: Scenarios of a Balanced Personal Data Ecosystem

What would the personal data ecosystem offer if the needs of government, private industry and individuals were appropriately balanced?

What follows are some possibilities for the year 2018.

Dianne is a mother of two teenage daughters and a remote caregiver for her father. She's not terribly sophisticated with technology but she uses some social networks to keep up with her friends and family. But as the hub of family care, Dianne is tied to several services that keep her family safe, healthy and informed.

Putting a new spring in her step

Dianne recently upgraded her exercise footwear to a wirelessly networked sports shoe, a product that transforms all of her daily walking into valuable data points. Her health insurance provider encourages exercise through a certified, earned credit system. With minimal data breach risk, walking translates directly into discounts on medications, food and other expenses for not only herself but also her father and daughters linked to her health savings account. This lets Dianne take better care of her loved ones, which is a more powerful motivator than her own health and wellness. The initial savings helped convert her children to regular walking as well. What was routine is now a game as the family competes in active walking challenges with one another, all the while providing better healthcare for everyone.

Transparency – data usage disclosure
Control – opt-in participation with immediate feedback in rewards balance
Trust – certified by identity consortium across health, finance and other service providers
Value – discounts powered by data collection that can be applied to many different needs

Source: frog design research, 2010

At ease and secure

Dianne's old anxiety over identity theft has been less of a worry since the Personal Data Protection and Portability Act went into effect, legislation the government passed in 2014 granting citizens greater control and transparency over their digital information. Her employer provides a private, certified Data-Plus Integrity Plan that monitors and ensures the personal data of her whole family and is portable across jobs. Dianne feels more at ease about her daughters' social habits online with the Parent Teachers Association-endorsed TeenSecure. A comprehensive activity summary and alert system means Dianne no longer feels like a spy, monitoring her kids and investigating every new social site. Her daughters' access is managed, tracked and protected by a trusted socially acceptable source. Dianne receives simple, convenient monthly statements that highlight both the activity and stored value of her data. As an added benefit, various retailers offer coupons and discounts during the holidays, in exchange for Dianne allowing them to use some of this activity data as a second currency.

Transparency – single view of all activity
Control – monitoring of dependents
Trust – government and consumer advocacy backed
Value – peace of mind and stored value

Transforming concern into ease

When Dianne's father moved into managed care with early-stage symptoms of Alzheimer's disease, her insurance carrier provided her with control of her father's medications and recommended an online dashboard-like tool adapted to his condition. The service is offered in a partnership with the Alzheimer's Research Foundation, as well as the Department of Public Health, which have connected her father's information and medical health records to her Data-Plus Integrity Plan. This provides Dianne with on-demand monitoring services, medication compliance tracking and feedback on how he is feeling. She is also able to keep tabs on his finances. Dianne hopes that through the sharing of her father's medical condition, they may one day find a cure. In the meantime, her in-person visits are less about evaluating his condition and much more about spending time together.

Transparency – permission of data access
Control – progression of need increases access
Trust – family-centric data safeguards
Value – transferable control

Source: frog design research, 2010

Key enablers of a balanced ecosystem

While building a balanced ecosystem around personal data will require significant commitment from all stakeholders, four critical enablers are apparent:

- An easy-to-understand user-centric approach to the design of systems, tools and policies, with an emphasis on transparency, trust, control and value distribution;
- Mechanisms for enhancing trust among all parties in digital transactions;
- Greater interoperability among existing data silos;
- An expanded role for government, such that governments can use their purchasing power to help shape commercially available products and solutions that the private sector can then leverage.

User-centricity

The concept of user-centricity is the central pivot point of the personal data ecosystem. With greater control placed in the hands of individuals, new efficiencies and capabilities can emerge. Many perceive this shift in power as highly disruptive. It creates a diversity of perspectives on if, how and when the "pivot for the people" might occur. In short, the transition to user-centricity is anything but simple. It's hard collectively to frame and act upon it due to the significant differences in cultural, geopolitical and institutional norms.

Globally, there is a growing consensus that there is an urgent need for greater trust associated with online identities. People find the increasing complexity of managing multiple user names and passwords across different organisations a major inconvenience. Additionally, as online fraud and identity theft continue to skyrocket, people demand greater assurances about who they are interacting with. As secure and trusted online relationships are established with individuals and various institutions, silos of information that were previously unavailable can also become easier to incorporate into personalised solutions.

A market is now taking shape to address these concerns on personal identity. In fact, an ecosystem of interoperable identity service providers offering solutions that are secure, easy to use and market based is in its early stages of development.[23] As more services move online (in particular, health and financial services), the infrastructure costs of ensuring the identity of who can use a given online offering will continue to escalate. The value of paying a third party for trusted digital identities will most likely continue to increase as these services reduce both the cost of fraud as well as the risk of offering additional value-added services[24] (see sidebar, "End user principles").

Trust enablers

Interviews and discussions with leading privacy advocates, regulatory experts and business leaders lead to an overwhelming consensus: trust is another key ingredient required for creating value from today's oceans of disparate personal data. Without

[23] National Strategy for Trusted Identities in Cyberspace. Draft. June 25, 2010.
[24] Reed, Drummond. "Person Data Ecosystem." Podcast Episode 2, December 2010.

End user principles

Transparency

What is a meaningful way to understand transparency, and who provides the lens to the user?

People naturally expect the right to see, and thus know, the data that is being captured about them. If that right is not respected, they feel deceived and exploited. Upon seeing this reflection of themselves through their personal data, people start to feel a sense of personal connection and ownership, leading to the desire for control. However, people struggle to form a mental model of something that is fragmented and abstract in nature. This creates a challenge: what is invisible must be revealed, made tangible and ultimately be connected across different points of access.

Trust

Which investments in building trust will help users feel comfortable allowing others to access their data?

Personal data is difficult, if not impossible, to un-share. Once shared, it gains a life of its own. Given the risk of unintended consequences, people rely heavily on trust to guide their decisions. But how is trust formed? Different thresholds of trust exist for different types of data. While a majority of people accept a certain level of risk, viewing it as an opportunity cost for gaining something, the benefits are often coupled with feelings of anxiety and fear. Such concerns will continue to limit the potential value of personal data until a comprehensible model for creating and certifying trust relationships is adopted on a large scale.

Control

What are the primary parameters that influence how users will want to control their data, and how are they adapted to different contexts?

People naturally want control over data that is both about them and often created by them. Control can be exercised in three ways:

(a) directly through explicit choices;
(b) indirectly by defining rules;
(c) by proxy.

People's perception of a given situation will determine whether they choose to exercise control. The more subtle qualities of an experience (such as feedback, convenience and understanding) will determine how they choose to exercise that control.

Value

What measures must be taken to ensure that data created today is a mutually beneficial asset in the future?

The value of personal data is wildly subjective. Many business models have emerged that encourage and capitalise on the flow of that data. Consumers are becoming increasingly aware of the value of the data they generate even in mundane interactions like a Google search. While direct personal data has an inherent value, secondary inferred data can often be mined and interpreted to produce new information of equal or greater value. The long-term impact of the aggregation and unchecked dissemination of this information is unknown. Digital behaviour today may yield positive distributed value across the ecosystem in the near term, but can have detrimental consequences for the end user in the future.

the establishment of trust, particularly the trust of the end user, a personal data ecosystem that benefits all stakeholders will never coalesce.

To use a metaphor, trust is the lubricant that enables a virtuous cycle for the ecosystem: it engenders stakeholder participation, which, in turn, drives the value creation process. For such a virtuous cycle to evolve, mutual trust needs to be at the foundation of all relationships. Increased trust leads to increased information flows, sharing and value creation and reduces litigation and regulatory costs.

"A collective metric of success could emerge where the overall growth of the ecosystem was the goal – rather than the success of one particular institution."

"Rethinking Personal Data" project

Increasing interoperability and the sharing of personal data

Promoting solutions that drive the exchange and "movement" of personal data in a secure, trusted and authenticated manner is also essential. Today, it is difficult to share personal data across private and public organisations and jurisdictions. This is due to a combination of technological, regulatory and business factors. Decades-old privacy laws and policies could not have foreseen the emergence of digital personal data as a valuable asset. Inadequate legislation has thus made standards surrounding the use of personal data inconsistent.

"We do not have the data-sharing equivalent of SMTP, but as we develop or achieve real data portability we will have a standardised infrastructure for data sharing that does not require centralisation."

Interviewee, "Rethinking Personal Data" project

Furthermore, many organisations employ legacy technology systems and databases that were created in proprietary, closed environments. As a result, personal data today is often isolated in silos – bound by organisational, data type, regional or service borders – each focusing on a limited set of data types and services.

To achieve global scale, technical, semantic and legal infrastructures will need to be established that are both resilient and interoperable. The US National Strategy for Trusted Identities in Cyberspace notes three types of interoperability for identity solutions:[25]

- Technical interoperability – The ability for different technologies to communicate and exchange data based upon well-defined and widely adopted interface standards;
- Semantic interoperability – The ability of each end point to communicate data and have the receiving party understand the message in the sense intended by the sending party;
- Legal interoperability – Common business policies and processes (e.g., identity proofing and vetting) related to the transmission, receipt and acceptance of data between systems, which a legal framework supports.

[25] "National Strategy for Trusted Identities." Draft pages 8–9. June 25, 2010.

US Department of Health & Human Services: "Blue Button" initiative[26]

Personal data also has clear opportunities to create value for the public sector. In October 2010, the US Department of Health's Medicare arm launched its "Blue Button" application. It's a Web-based feature that allows patients easily to download all their historical health information from one secure location and then share it with healthcare providers, caregivers and others they trust – something that wasn't possible before.

The service is innovative in many ways. First, it allows Medicare beneficiaries to access their medical histories from various databases and compile sources into one place (e.g., test results, emergency contact information, family health history, military health history and other health-related information). Second, the service provides the information in a very convenient and transportable format (ASCII text file). That allows it to be shared seamlessly with virtually any healthcare or insurance provider. Finally, Blue Button fully empowers the end user: patients are given control over how their information is shared and distributed. That allows them to be more proactive about – and have more insight into – the medical treatments that they need.

It is important to stress that the call for interoperability does not equate to working exclusively with standards bodies. In many cases standards take too long. By leveraging open protocols, de facto standards, existing pilots and collaboration with industry and advocacy groups, a functional degree of interoperability can be achieved in a shorter time frame.

Despite this "need for speed", the levels of reliability, integrity and security for both the individual and the computing infrastructure cannot be understated. The broad private sector support to cooperate in the sharing of personal data will bring with it extremely high technical, legal and performance requirements.

Government as enabler

Governments have a vital role to play in accelerating the growth of a balanced personal data ecosystem. Their influence manifests itself along three primary dimensions.

First, they play a dominant role in crafting the legal and regulatory environments that shape what is possible in the ecosystem. This is a challenging role in many respects. Within the national context, regulators are being asked to balance consumer protection with the need to create a business environment conducive to innovation, growth and job creation. On top of that, many global industry participants are turning to national and regional regulatory bodies to harmonise guidelines to facilitate global platforms.

Second, governments are active participants in ongoing experiments regarding how the personal data ecosystem can be harnessed to achieve important social goals such as providing more efficient and

[26] "'Blue Button' Provides Access to Downloadable Personal Health Data." Office of Science and Technology Policy, the White House website. http://www.whitehouse.gov/blog/2010/10/07/blue-button-provides-access-downloadable-personal-health-data

"We must have empowered users, but no one is suggesting the user should be able to edit his or her criminal records. We're looking at a collaborative model with users who are as empowered as we can make them."

Interviewee, "Rethinking Personal Data" project

cost-effective services to citizens, stopping epidemics before they become pandemics and using data-mining techniques to enhance national security.

Third, and perhaps most importantly, given their purchasing power, governments are in a position to influence significantly commercially available solutions. In crafting requests for proposals to help modernise service delivery, governments can write specifications for everything from security protocols to end user interfaces and data portability options. Successful projects can serve as proof points and major references for innovative solutions.

Hands-on experience gained in leveraging personal data for government services and objectives, combined with insights gleaned from negotiations with vendors, can give regulatory deliberations a very practical bent, which should be beneficial to all parties.

Section 2: Stakeholder Trust and Trust Frameworks

Achieving a high level of stakeholder trust requires a set of legal and technical structures to govern the interactions of participants within the ecosystem. The concept of trust frameworks is emerging as an increasingly attractive means for the personal data ecosystem to scale in a balanced manner. Trust frameworks consist of documented specifications selected by a particular group (a "trust community"). These govern the laws, contracts and policies undergirding the technologies selected to build the identity system. The specifications ensure the system reliability that is crucial for creating trust within the ecosystem.

The magnitude of data breaches

The Privacy Rights Clearinghouse estimates that in the US alone, more than 2,000 publicly announced data breaches have occurred since 2005. These include instances of unintended disclosure of sensitive information, hacks and payment card fraud, all of which resulted in a staggering 500-million-plus records of data being compromised.

Source: Privacy Rights Clearinghouse

The trust framework model

The Open Identity Trust Framework model (OITF) is a working example. Built to Internet scale, it offers a single sign-on environment for trust between relying parties and end users. The model addresses two problems with the way end users and relying parties interact with the Internet today:

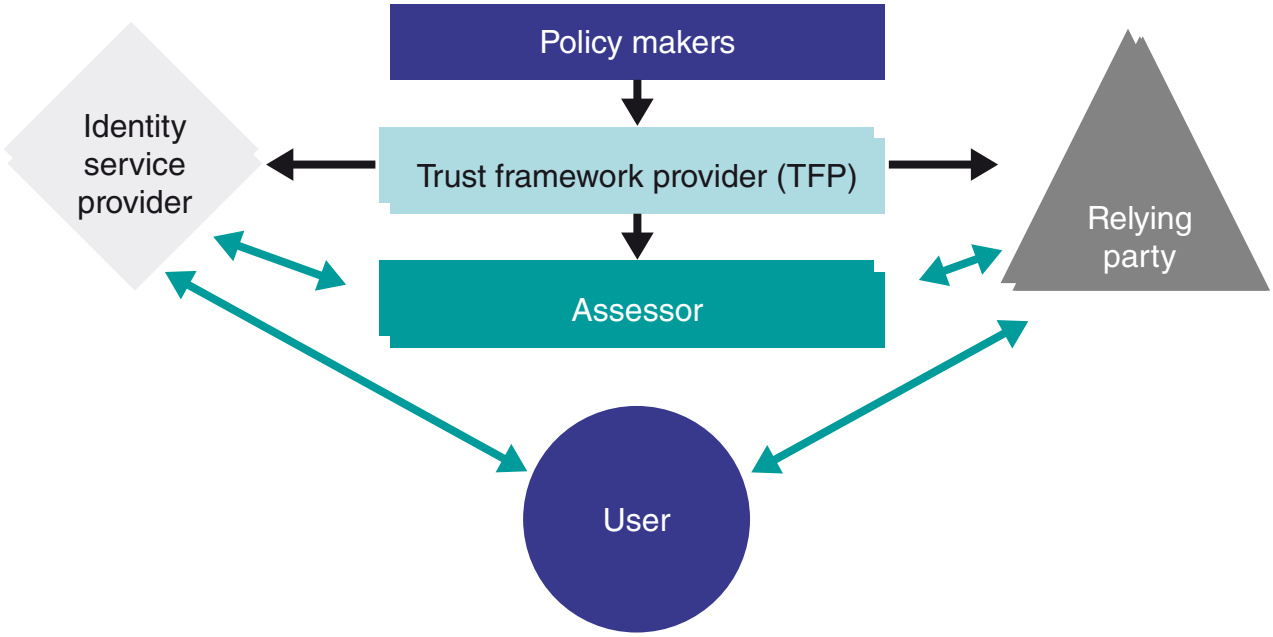
- The proliferation of user names and passwords;
- The inability of relying parties to verify the identity of other entities.

Most people can relate to the first problem. Almost every website requires visitors to establish a user name and password, and invariably requires the sharing of such personal data as name, address and credit card information. Not only is this inconvenient, it's unsafe. It puts our personal data onto every server with which we interact, increasing the odds that our data may be compromised.

The second problem trust frameworks address is the lack of certainty about online identities. In most of today's Internet transactions, neither the user nor the relying party is completely sure of the other's identity. That creates a huge opening for identity theft and fraud. In 2009, more than $3 billion in online revenue was lost due to fraud in North America.[27] Some $550 million of that was money lost by individual US consumers.[28] The hope is that with a richer, scalable and more flexible identity

[27] CyberSource. 11th Annual "Online Fraud Report." 2010.
[28] 2009 "Internet Crime Report." Internet Crime Complaint Center. US Department of Justice, 2010.

FIGURE 5: THE OPEN IDENTITY TRUST FRAMEWORK MODEL



Source: OITF

management system, these losses can be reduced.

The model defines the following roles (see Figure 5) to support Internet-scale identity management:

- Policy makers decide the technical, operational and legal requirements for exchanges of identity information among the group they govern;

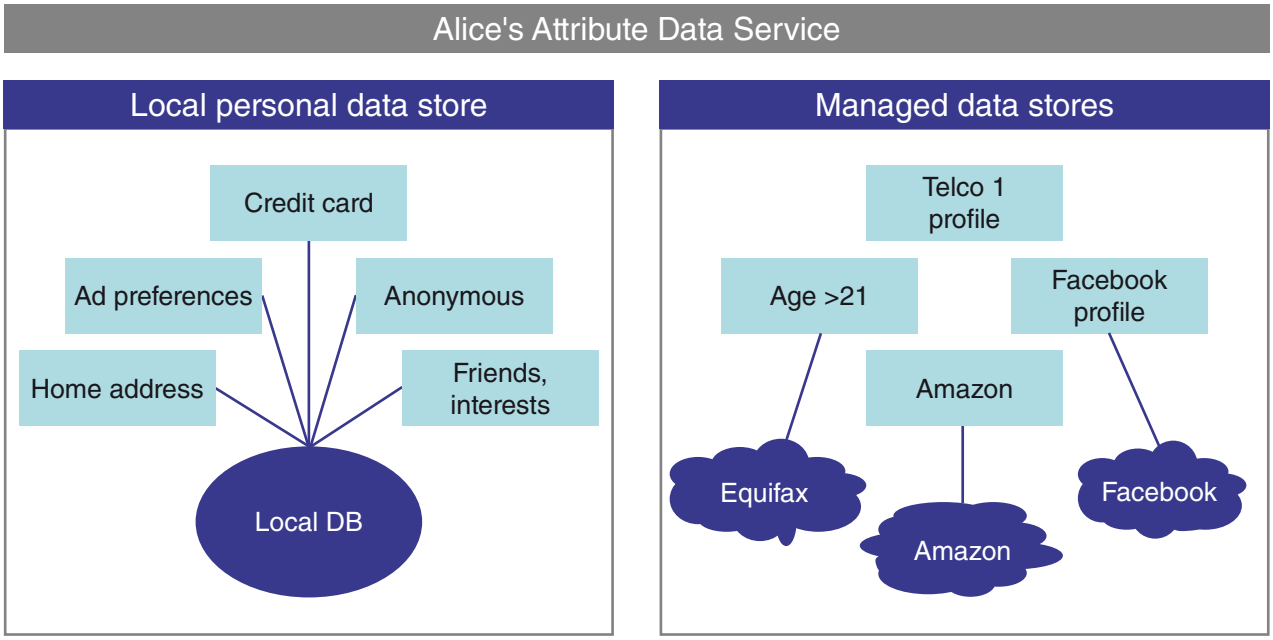
- Trust framework providers translate these requirements into the building blocks of a trust framework. They then certify identity verification providers that provide identity management services in accordance with the specifications of the trust framework. Finally, the trust framework provider recruits assessors responsible for auditing and ensuring that framework participants adhere to the specifications;

- Identity providers (IdPs) issue, verify and maintain online credentials for an individual user. Relying parties accept these credentials and have firm assurances that the IdP has analysed and validated the individual user;

- Assessors evaluate IdPs and relying parties, and certify that they are capable of following the trust framework provider's blueprint.

Within such a trust framework model, end users can access multiple sites (relying

FIGURE 6: PERSONAL DATA SERVICES STORE END USERS' DATA AND PROVIDE APPLICATIONS THAT ENABLE THEM TO MANAGE, SHARE AND GAIN BENEFIT FROM THEIR PERSONAL DATA[29]



Source: The Eclipse Foundation

parties) using a single credential issued by an identity provider. On their part, the sites can rest assured about the identities of the individuals they are doing business with. This screening is similar to how a car rental agent trusts that a driver can legally operate an automobile because he or she has a valid driver's licence.

With such a framework, users would need only to share less sensitive personal data with relying parties. No longer would they have to enter their name, address and credit card information in order to purchase a Web service. Using the trust framework, they would share the minimum amount of data to complete the transaction. In some cases, that may simply amount to verification of the availability of the funds being transmitted to the relying party.

PERSONAL DATA SERVICES

The trust framework model will bring benefits to end users in the form of increased privacy and a more seamless and convenient Web experience. But such advantages can be extended through the related concepts of personal data services and vendor relationship management (VRM).

[29] Higgins Open Source Identity Framework is a project of The Eclipse Foundation. Ottawa, Ontario, Canada. http://www.eclipse.org/higgins/faq.php

Personal data services provide the safe means by which an end user can store, manage, share and gain benefit from his or her personal data. These data can range from such self-asserted attributes as the individual's likes, preferences and interests to such managed and verified attributes as a person's age, credit score or affiliations, and histories with external entities like firms, government agencies and the like (see Figure 6).

Personal data services consolidate end users' digital identity, allowing them to control which third parties are entitled to access – along with how, when and at what price. VRM extends this control to the realm of realising direct value – monetary or in kind – from the personal data stored and managed by personal data services providers.

These emerging concepts will help build stakeholder trust and herald additional benefits for end users and relying parties alike. Indeed, some promising trials are already under way. Yet more testing will be needed to resolve some open questions about the viability of these concepts.

Key uncertainties of trust frameworks

Trust frameworks and personal data services are concepts in their infancy. Despite encouraging pilots in the US and the UK, they need further refinement and testing to fulfil their promise. Implementations thus far have primarily been at websites where the level of assurance required is relatively low, such as those enabling blogging or providing news content. They need to be deployed in environments that encompass more high-risk transactions, such as logging into a bank account. Only then will proponents know if these ideas can achieve Internet scale.

Risks and uncertainties also surround the business models for both identity providers and relying parties. While a large number of private enterprises have begun working in this space (Acxiom, AOL, Citibank, Equifax, Google and PayPal) the economics are unclear.[30]

From the perspective of relying parties, the benefits of transitioning to a user-centric model are still emerging. In this new approach, relying parties will be constrained on collecting data for free and will need to start paying for end user data. While some believe that an aggregated and holistic view of an individual would be more valuable, the balance of trade between what relying parties would be willing to share versus the new insights and efficiencies they would gain from a holistic user-centric view are unclear.

However, the cost of online fraud and risk mitigation could be enough to make relying parties seriously consider participating in a more collaborative model. On average, online fraud represented 1.2 per cent of a Web retailer's revenue in 2009.[31]

Finally, building end user awareness is another uncertainty. How can firms com-

[30] Kreizman, Gregg, Ray Wagner and Earl Perkins. "Open Identity Pilot Advances the Maturity of User-Centric Identity, but Business Models Are Still Needed." Gartner, November 9, 2009. http://www.gartner.com/DisplayDocument?id=1223830
[31] Cybersource. "11th Annual Online Fraud Report." 2010.

municate to individuals the advantages of managing their personal data? For a start, companies must themselves fully understand the convenience, value proposition, contextual nuances and usability of personal data dashboards. Further investigation is therefore needed into applications and services that provide end users with convenient, contextually relevant and simplified control over their data.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Section 3: Conclusions

Personal data will continue to increase dramatically in both quantity and diversity, and has the potential to unlock significant economic and societal value for end users, private firms and public organisations alike.

The business, technology and policy trends shaping the nascent personal ecosystem are complex, interrelated and constantly changing. Yet a future ecosystem that both maximises economic and societal value – and spreads its wealth across all stakeholders – is not only desirable but distinctly possible. To achieve that promise, industries and public bodies must take coordinated actions today. Leaders should consider taking steps in the following five areas:

1. Innovate around user-centricity and trust

Where we stand today

Innovative concepts already exist on how personal data can be shared in a way that allows all stakeholders to trust the integrity and safety of this data. Examples of such trust frameworks include the Open Identity Trust Framework and Kantara's Identity Assurance Framework. However, no truly large-scale application of a trust framework has yet been rolled out. As a consequence, we remain uncertain about how to take advantage of personal data while still aligning stakeholder interests. Also unanswered are questions such as: What are the incentives for stakeholders to participate in trust frameworks? What are the business model mechanics? Who will pay for identity provider services?

What is required and why

Complex blueprints for Internet business models typically come to life in iterative steps. For example, the retail banking sector evolved online through successive phases of change. Trust frameworks need similar pressure testing in large-scale applications to prove these concepts can be instrumental in unlocking economic and societal value. Additionally, end user participation in testing and developing these trust frameworks is crucial. Offering more transparency on how personal data is used and educating end users on the benefits they can extract from such applications – two areas lacking in the ecosystem today – will significantly strengthen trust among all stakeholders.

Recommended next steps

Private firms and policy makers should consider the following next steps:

- Invest in open and collaborative trials orchestrated by end user privacy groups or academics;
- Integrate principles surrounding end user trust and data protection into the development of new services and platforms (the concept of "privacy by design"), particularly when designing new "e-government" platforms;

- Engage with leading innovators and end user advocacy groups to explore the further applications for, and development of, trust frameworks.

2. Define global principles for using and sharing personal data

Where we stand today

Privacy-related laws and police enforcement differ significantly across jurisdictions, often based on cultural, political and historical contexts. Attempts to align such policies have largely failed.[32] But the need is growing. Many Internet services, in particular those based upon cloud computing delivery models, require the cross-jurisdictional exchange of personal data to function at optimal levels.

What is required and why

The downside of the current divergence in regulatory frameworks manifests itself in several ways. First, companies striving to provide products and services based upon personal data see significant complexity costs associated with compliance. As a result of these costs, they may choose not to offer their product and services in certain smaller markets, where the cost of doing business may outweigh incremental profits. That decision to opt out obviously hurts the users who cannot access the services. Less obvious is the fact that users with access are also hurt, as the value of many of these services increases with the number of users.

A truly global and seamless exchange of personal data will not emerge without a set of internationally accepted, user-centric principles. Additionally, a set of commonly accepted terms and definitions – a taxonomy – surrounding personal data concepts must be created to allow unencumbered dialog. Although it is unrealistic to hope to develop globally accepted standards and frameworks while national and regional versions are still in significant flux, establishing a standing, cross-regional dialog will allow for more rapid harmonisation once regulatory environments do begin to stabilise.

"Digital bill of rights have been introduced a half dozen times... If they are introduced in conjunction with a way for them to be actionable by large populations of people then it may have more success."

Interviewee, "Rethinking Personal Data" project

It is imperative for private sector firms to participate in at least some of these dialogs, as they can share real-world perspectives on the cost and challenges of dealing with divergent regulations and can help public sector officials adapt pragmatic and consistent policies.

Recommended next steps

- Policy makers and private firms should launch an international dialog to stay informed about proposed laws and policies that would have a global bearing on their markets. This dialog should encompass governments, international bodies such as the World Trade Organization, end user privacy rights groups and representation from the private sector. It should include not only US and Eu-

[32] See, for example, Connolly, Chris. "The US Safe Harbor – Fact or Fiction?" Galexia, 2008.

ropean Union members, but interested parties from the Asia-Pacific region and emerging countries;

- Among the outputs of this body would be an agreed-upon benchmark measuring the effectiveness of national regulations and their impact on free markets. This could prove vital in unearthing and spreading best practises that could ultimately guide the development of consistent national policies.

3. Strengthen the dialog between regulators and the private sector

Where we stand today

The roots of today's data privacy laws grew from the aspirational principles of the early 1980s, which reflected a consensus about the need for standards to ensure both individual privacy and information flows.[33] But over the last two decades, these principles have been translated very differently into national policies in the US, the European Union and the Asia-Pacific. Although most of these laws aim to maximise data protection and individual control, many experts question their practical effectiveness given technological advances. Some governments, such as in the US and European Union, are therefore revising their policies.

What is required and why

Topic experts and executives involved in the "Rethinking Personal Data" project agree that self-regulation of markets related to personal data is not a desirable outcome for all stakeholders. Instead, national and regional agencies must adopt 21st-century digital policies that promote and accelerate favourable behaviour from all market participants.

Recommended next steps

- In the United States: Private firms should closely watch developments of the National Strategy for Trusted Identities in Cyberspace programme and the privacy bill – and seek ways to contribute to them. Private firms and advocacy groups need to be in constant dialog with the US Department of Commerce, the Federal Trade Commission and other bodies to help shape future legislation and policies;

- In the European Union: Private firms should collaborate with the European Commission in its move to revise the EU privacy directive and to synchronise legislation across its member states. A revised EU privacy directive is scheduled to go into effect in 2011, after a period of public consultation through the European Commission's website during January;[34]

- In other countries: In other regions that differ from the US or the EU in cultural or social norms, very different paths in adopting policy frameworks will be required. However, given the global relevance of many such markets in the future digital economy, private firms and policy makers should not just wait and see. One initial step in making progress

[33] See, for example, Cate, Fred H. "The Failure of Fair Information Practice Principles." Consumer Protection in the Age of the Information Economy, 2006. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972
[34] Ashford, Warwick. "Revised EU Privacy Laws to Demand Greater Transparency on the Web." ComputerWeekly.com., November 5, 2010.

could be to seek ways to harmonise fragmented national privacy policies. For example, a starting point in Asia could be the Asia Pacific Privacy Charter Initiative, which, since 2003, aims to align privacy policies and to promote best practises in regulatory and legislative frameworks in the region.

4. Focus on interoperability and open standards

Where we stand today

A large variety of syntax and semantic standards exist to describe and share personal data. Most of those standards are proprietary and were often invented in an ad hoc manner without broader consultation with industry peers. While some open standards are emerging – for example, in the realm of digital identities, standards include ISO/IEEE, Mozilla and OIX – no standards are in place for many other data types, particularly new ones. The history of the Internet shows that open standards can improve data portability significantly. One example from the 1980s was the advent of the simple mail transfer protocol (SMTP), which superseded various proprietary email standards.[35]

What is required and why

If we posit that the highest potential for economic and societal value creation lies in the aggregation of different personal data types, the implication is clear: To enable the seamless sharing of personal data across organisational borders, private firms and the public sector will require common communication standards, system architectures, accepted personal data terms and definitions, and standard interface design specifications.

Recommended next steps

- Private firms, in particular those from the information communication technologies sector, should participate in initiatives that aim to align today's jumble of standards. The Open Web Foundation is one such example: it has helped companies define commonly accepted standards and avoid competitive deadlocks;[36]

- Private firms and public bodies should use the knowledge gained from ongoing pilot tests of trust frameworks and related services to inform standardisation bodies, such as the IEEE;

- To build momentum, firms and public organisations should monitor the ongoing dialog to identify the most valuable types of personal data and focus standardisation efforts on those first.

5. Continually share knowledge

Where we stand today

Interested sponsors continually hold a large number of conferences, events, websites, private-public discussions and blogs on the different aspects of the personal data ecosystem. Even for active dialog participants, it's challenging to keep up with the latest developments and

[35] Strauser, Kirk. "The History and Future of SMTP." FSM, March 4, 2005.
[36] Taft, Darryl K. "Microsoft Specs Support Open Web Foundation Agreement." eWEEK, November 25, 2009. http://www.eweek.com/c/a/Application-Development/Microsoft-Specs-Support-Open-Web-Foundation-Agreement-632362

research. Some platforms are aiming to synthesise this ongoing dialog, yet none has yet reached a critical mass with private and public stakeholders.

What is required and why

The goal is to aggregate the key insights – from both successful and unsuccessful initiatives – in a timely and unbiased manner. This would enable the sharing of lessons learned, right from the introduction of new personal data services to the development of further research activities.

Recommended next steps

- Private firms should nominate a central gatekeeper in the organisation who actively contributes to the personal data dialog. That person's purview would not only include privacy but also encompass a business development and strategic perspective;

- Private and public sector representatives should invest in a jointly run organisation that facilitates a truly global dialog about personal data – one that stretches across industries and regions. Given private companies' increasing propensity to be multinational, the onus is on them to pressure their respective governments to think on a global scale.

Glossary of Terms

End user
This term refers to individual consumers, citizens or persons about and from whom personal data is created. End users are also able to participate in the use and proliferation of personal data via related services, applications and technology. End users are typically represented on a broad, public scale by consumer advocacy groups, such as the American Civil Liberties Union (ACLU) in the United States.

End user-centricity
End user-centricity refers to the concept of organising the rules and policies of the personal data ecosystem around the key principles that end users value: transparency into what data is captured, control over how it is shared, trust in how others use it and value attributable because of it.

Identity provider
Identity providers (IdPs) issue, verify and maintain online credentials for an individual user. Relying parties accept these credentials and have solid assurances that the IdP has analysed and validated the individual user in accordance with specifications.

Person[37]
A person can be defined as a natural person, a legal person or a digital persona. A natural person refers to a specific human being with an individual physical body (e.g., John Smith). A legal person refers to a body of persons or an entity (as a corporation) considered as having many of the rights and responsibilities of a natural person and in particular the capacity to sue and be sued (e.g., John Smith and Associates, LLC). Legal persons encompass a wide range of legal entities, including corporations, partnerships, limited liability companies, cooperatives, municipalities, sovereign states, intergovernmental organisations and some international organisations. A digital persona (or identity) can be understood as a digital representation of a set of claims made about a person, either by themselves or by another person (e.g., JohnSmith@gmail.com or JohnSmith@facebook.com). Note that a natural person may have multiple digital personae.

Personal data
We broadly define personal data as data and metadata (i.e., data about data) relating to an identified or identifiable person or persons. Our definition is based upon European Union Directive 95/46/EC. Personal data can be created in multiple ways, including: (1) volunteered data, which is created and explicitly shared by individuals (e.g., social network profiles); (2) observed data, which is captured by recording the actions of individuals (e.g.,

[37] Sourced from Davis, Marc, Ron Martinez and Chris Kalaboukis. "Rethinking Personal Information – Workshop Pre-read." Invention Arts and World Economic Forum, June 2010.

location data when using cell phones); and (3) inferred data, which is data about individuals based on analysis of volunteered or observed information (e.g., credit scores).

Privacy[38]

The term privacy has two separate meanings. The public use of the term privacy is very broad, and it is used to reference nearly anything that has to do with personal data and more generally the perceived rights of an individual in relationship to a group. The legal meaning is much narrower. In US domestic law, it refers to a constitutional right (as interpreted by the courts) and several specific tort rights. Privacy tort rights, which are based mostly in common law (i.e., cases as opposed to statutes), are generally categorised to include the protection of solitude and has developed to include protection of "personality." Privacy tort "causes of action" are generally recognised to protect against four kinds of wrongs against the invasion of privacy. That includes (1) the appropriation of a person's picture or name by another for their commercial advantage (generally the promotion of goods), (2) the intrusion on a person's affairs or seclusion (if objectionable to a reasonable person), (3) the publication of facts that place a person in a false light (for example, publicly attributing an action or statement to a person that he or she did not make), and (4) public disclosures of private facts about the person. Both the public and legal meanings have one thing in common; they are both associated with "protection from harm" of the affected person.

Private sector (or companies)

Within the context of the personal data ecosystem, the "private sector" refers to for-profit companies and private organisations involved in the capture, storage, analysis and sharing of personal data for the purposes of developing – and monetising – related services and applications. Private sector participants are not limited by size or industry group: they are any private entity that directly manipulates personal data for explicit financial gain.

Public sector (or agencies)

Within the context of the personal data ecosystem, the public sector refers to governments (and their agencies) and nonprofit public organisations that are involved in the passing of legislation and policies that regulate the capture and use of personal data within their respective jurisdictions. Public sector entities also participate in capturing and storing personal data (e.g., social security information), as well as the development of related services and applications.

Relying party

In the context of trust frameworks, relying parties are typically businesses or organisations that rely on personal data as a means to verify the identities of their customers or partners. Without reliable and verifiable information, these transactions can be fraught with risks, including fraud.

[38] Ibid.

Trust frameworks

Within the context of online and digital transactions, a trust framework is a formalised specification of policies and rules to which a participant (e.g., an end user, relying party or identity provider) must conform in order to be trusted. These policies include requirements around identity, security, privacy, data protection, technical profiles and assessor qualifications. This trust may be subject to different levels of assurance or protection, which are explicitly made clear to all parties.[39]

[39] Ibid.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum is an independent international organisation committed to improving the state of the world by engaging business, political, academic and other leaders of society to shape global, regional and industry agendas.

Incorporated as a foundation in 1971, and based in Geneva, Switzerland, the World Economic Forum is impartial and not-for-profit; it is tied to no political, partisan or national interests.

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

email: contact@weforum.org
www.weforum.org