# *Chapter 5*

# Building trust for data-driven innovation

*This chapter provides an overview of emerging trust issues raised by the increasing use of data-intensive applications that impact individuals in their commercial, social and citizen interactions. Security issues are addressed first, with an examination of the traditional approach and its inherent limitations. Comparisons are then made with current digital security risk management, which views risks as the possible detrimental* consequences *for the objectives of, or benefits expected from, the data value cycle. The point is made that a certain level of risk has always to be accepted for the value cycle to provide some benefit – raising the question of who decides that level. The discussion then takes up privacy protection. Practical means for preventing information discovery are enumerated, and the dangers of information asymmetry, data-driven discrimination, and unanticipated uses of consumer data addressed. Attention then turns to potential policy approaches to help in addressing the issues raised.*

*It takes years to build up trust, and only seconds to destroy it (unknown author).*

*"Ginny!" said Mr. Weasley, flabbergasted. "Haven't I taught you anything? What have I always told you? Never trust anything that can think for itself if you can't see where it keeps its brain?"* (Rowling, 1998, *Harry Potter and the Chamber of Secrets*)

Critical to reaping the substantial economic benefits of data-driven innovation (DDI) – as well as to realising the full social and cultural potential of that innovation – is the key element of trust. Trust is a complex issue, and yet there is consensus that it plays a central if not vital role in social and economic interactions and institutions (Putnam et al., 1993; Morrone, et al., 2009; OECD, 2011a). In reducing transaction costs and frictions, trust generates efficiency gains, and is considered by some to be a determinant of economic growth, development, and well-being. The OECD (2011a) provides quantitative evidence that high country trust is strongly associated with high household income levels.

In relation to the digital economy, the main components of trust are security and privacy protection for individual citizens and consumers. DDI relies on an intricate, hyper-connected information and communication technology (ICT) environment in which security threats have changed in both scale and kind. Security measures aim to address these challenges to establish the trust needed for economic activities to take place. But they can also inhibit economic and social development, by reducing innovation and productivity. The digital security risk management approach described below is a way forward: it helps address security-related uncertainties in a manner that fosters DDI. Tackling the issues raised by the second dimension of trust – the protection of personal data – is less straightforward than addressing security, as will be seen below. In the context of DDI, the consumer protection issues relate primarily to the collection and use of consumer data and are treated in common with the more general analysis of privacy.

## 5.1. Security for data-driven innovation

Given that decision making is becoming increasingly data-driven and automated, and the expected benefits of such decision making and of data-driven knowledge creation are growing, it has become essential to address digital security The digital assets of businesses, individuals and governments face various types of threats from a growing number of sources. These include organised crime groups, "hacktivists", foreign governments, terrorists, individual "hackers" – and sometimes, business competitors. A range of techniques are deployed – some basic, others extremely sophisticated – to target valuable digital assets. There are in addition the non-intentional digital threats, such as hardware failure and natural disasters. Whether intentional or not, digital threats can disrupt the functioning of systems and networks and damage the economic and social activities that rely on the confidentiality, integrity and availability of data and information.

Analysis of a new generation of national cybersecurity strategies in OECD countries shows that cybersecurity policy making has reached a "turning point" and has "become a national policy priority" (OECD, 2012a). Yet many stakeholders continue to adopt a traditional security approach that not only falls short of appropriately protecting assets in the current digital environment, but also is likely to stifle innovation and growth. This traditional approach is introduced below, prior to a discussion of the digital security risk management approach promoted by the OECD.[1]

### *The traditional security approach*

The traditional security approach, as conveyed by the dictionary definition of the term "security" (Online Etymology Dictionary, 2014), aims to create a secure environment that is "free from danger or risk of loss". Knowing that any threat will be eliminated or neutralised by security measures, users of the digital environment can then trust it and carry out their economic and social activities without being concerned.

In more precise terms, this approach aims to create a digital environment secure from threats that can undermine the availability, integrity and/or confidentiality of information or information systems – the AIC triad.[2] Availability is the accessibility and usability of data upon demand by an authorised entity. Integrity is the protection of data quality in terms of accuracy and completeness. Confidentiality refers to the prevention of data disclosure to unauthorised individuals, entities or processes.

To preserve each of these dimensions, security experts put in place security measures, sometimes also called security "controls", "mechanisms" or "safeguards". They are generally based on technologies (e.g. firewalls, anti-virus protection, encryption), people (e.g. training, assigning responsibilities) and processes (e.g. backup procedures, password policies). Thus it is possible for many security measures to be selected and implemented; however, since resources are limited, security experts often have to decide which measures to place where in a system for security to be the most effective. These choices are based on analysis of the likelihood of threats exploiting vulnerabilities and undermining one or more dimensions of the AIC triad.

Under this traditional model, once security measures are in place, the system and the valuable data it contains (i.e. the environment) are deemed protected. Security measures form a perimeter around the protected assets to secure them. As economic and social activities require limited protection within the walled perimeter, the effort is focused on the height of the walls, as well as the number of gates and guards controlling entry and exit. Finally, since security focuses on the protection of the digital environment, a key characteristic of the traditional security approach is that the primary responsibility for security generally rests with the party responsible for the provision of that environment: the IT department.

### *Limitations of the traditional security approach in a data-intensive environment*

Data-driven innovation (or data-intensive economic and social activities) relies greatly on the digital environment. However, this environment must have certain characteristics to be conducive to DDI: it must be open and interconnected, as well as flexible. It must also host a massive volume of data of considerable diversity. Unfortunately, these interrelated characteristics increase the complexity of security management to a point where the traditional security approach cannot scale up.

#### *Openness is essential and interconnectedness is blurring the perimeter*

First, data-driven innovation leverages the fundamentally open and interconnected nature of information systems and networks, qualities enabled by the generalisation of Internet technologies in the second half of the 1990s. It depends on the capacity to exchange data flows easily, flexibly and cheaply with a potentially unlimited number of partners outside the perimeter.

The traditional closed security perimeter approach is thus an obstacle to the development of data-driven innovation. The idea that, for security reasons, a system should be kept closed by default and open only by exception belongs to the past, when information technologies were not designed for interoperability and when their contribution to economic and social progress depended less on the free flow of data. In the pre-Internet era, information systems were inherently isolated, designed and operated with a clear and closed perimeter by default. Interconnecting them required an expensive add-on to be developed on a case-by-case basis. However, since the mid-1990s, this "siloed" world has progressively disappeared. Information systems are now designed to

be open and interconnected by default, without additional cost, and this characteristic has become the main driver for using ICTs to drive productivity, innovation and growth. It has in fact become complicated and expensive to close information systems, both in terms of the security measures needed to reduce interconnectedness and – most importantly – because limiting interconnectedness also inhibits ICT from enabling any of those gains. Closing these systems will moreover provide only an illusion of security.

The very concept of a perimeter in any case becomes blurred in an environment where the number of gateways to the outside digital world increases exponentially, making systematic and comprehensive control of inputs and outputs equally illusory. It is challenging to define a perimeter whose length may cross the boundaries of the organisation and national jurisdictions, and perhaps even extend to the whole of the Internet. Trends such as cloud computing, mobility, "bring your own device", machine-to-machine communication (M2M) and the "Internet of Things" (i.e. the interconnection of physical objects over the Internet) are firm evidence of the dissolution of boundaries for information systems and networks. Future trends unknown now will likely continue to expand this landscape. Thus, although a system's perimeter remains a potential location to deploy local security measures, relying on its robustness while limiting its openness would be both ineffective from a security perspective, and economically counterproductive.

### *The traditional approach reduces the flexibility of the environment*

Second, DDI relies on the capacity to exploit the dynamic nature of the digital environment – rapidly connecting, matching and analysing what was previously not related in order to create new assets. In contrast, the traditional security approach is meant to protect clearly defined tangible and intangible assets, including information systems, networks, data and information. Changes in the digital environment or its use are likely to require the reorganisation of security measures and are therefore not welcome from a traditional security perspective. Traditional security is static in nature and fails to address rapid change in the system and its use. If the economic benefits of DDI result from the dynamic nature of the digital environment and its usage, traditional security is likely to become an obstacle to change and therefore an inhibitor for realising the full benefits.[3]

### *The volume and diversity of data increases complexity*

Third, the growing volume and diversity of digitised data, DDI's key enablers, raise another challenge to traditional security. Traditional security can deal with increased volumes and diversity if the data are located within a defined perimeter and their processing is not subject to continuously unpredictible uses and flows. However, the uncertainty already introduced by the open and dynamic nature of data-driven innovation grows, sometimes exponentially, with these increases. Malicious elements are ubiquitous in complex systems – just as the natural environment is rife with viruses, bacteria and parasites (Forrest, Hofmeyr and Edwards, 2013) – and the complexity of the security equation is now multiplied by the scale, volume and diversity of the data stored and processed. This can be seen as an aggravation either of the potential threat (i.e. more data are likely to attract more malicious players and generate more errors) or of the potential vulnerabilities – or both.

These characteristics underline the main weakness of the traditional security approach, which is both binary (there is no middle ground between secure and insecure) and monolithic (the entire digital environment has to be secured for the approach to be effective). By adding an ever growing number of fast-changing variables, the potentially unlimited extension and openness of the perimeter and the ever growing and

unpredictible (i.e. innovative) usage of the environment for legitimate economic and social objectives put stress on the security paradigm. The approach can only operate at the cost of reducing the complexity and increasing stability, which will inevitably slow innovative usage and, ultimately, undermine the economic and social benefits of interoperable ICTs.

One may argue that to address these challenges, traditional security could be implemented in a more flexible way by focusing on those parts of the digital environment that are of more value to the organisation, and placing less emphasis elsewhere. However, the value is not really in the digital environment itself, or in the data, or in the information, but rather in the whole data value cycle (see Chapter 1 of this volume); that is what can generate economic and social benefits. More precisely, even when focusing on the data rather than on the information systems and networks, the fact that "information is context-dependent" (Chapter 4) makes it difficult to tailor the traditional security approach to the value of the data, because they are impossible to assess before their use.

### *From traditional security to digital security risk management*

As noted above, the challenges to digital security are not new; they result from the mid-1990s shift of ICTs towards openness and interconnectedness by default, a trend that fed two decades of flourishing Internet-related innovation. In the early 2000s, application to ICT-related economic and social activities of risk management concepts and frameworks experienced in other areas such as industrial, health and environmental risks offered an alternative to the traditional digital security approach. The risk-based approach – which has been referred to with different terms and sometimes misleading but widespread expressions such as information security, information assurance and cybersecurity – requires a different culture, mindset and framework from traditional security. It redefines what should be protected, for what purpose, how it should be protected, and who should be responsible, with far-reaching consequences in terms of corporate governance applied to ICTs, and business management more generally. Surprisingly, however, while its application to ICTs is relatively recent, risk management is a common management and decision-making tool in business and industry.

The methodology of application is actually the same used by decision makers to address other risks. Nevertheless, it represents a significant paradigm shift in the way economic and social (or "business") decision makers,[4] security experts and ICT professionals often approach digital security threats. This section focuses on the two main changes required by digital security risk management: a different culture, and a different framework. The application of digital security risk management to digital activities was initially promoted in the 2002 *OECD Recommendation concerning Guidelines for the Security of Information Systems and Networks,* and is at the core of an ongoing process to revise this Recommendation.

#### *From a culture of security to a culture of risk management*

As explained in Chapter 1 of this volume, the value of data-intensive activities is not limited to the digital storage and processing of a large quantity of data ("big data"), but rather to the capacity to manage a data value cycle (see Figure 1.7 in Chapter 1). This cycle can transform the data into information and knowledge to feed more effective decision making and generate economic and social benefits through DDI. The objective of digital security risk management is therefore to *increase the likelihood of economic*

*and social benefits from the data value cycle by minimising potential adverse effects of uncertainty related to the availability, integrity and confidentiality of the cycle (AIC triad).* Unlike the traditional security approach, digital security risk management does not aim to create a secure digital environment to eliminate risk. Instead, it creates a framework to select proportionate and efficient AIC security measures in light of the benefits expected from the cycle. Therefore, it should be an integral part of the establishment and business use of the data value cycle, rather than merely a technical framework or a process separated from the business cycle.

The application of risk management to the use of ICT throughout the data value cycle requires decision makers and other key actors to understand the following fundamentals:

- Digital security risks are the possible detrimental *consequences* for the objectives of or benefits expected from the data value cycle that could result from uncertain events.[5] Such events are generally incidents resulting from the nexus of threats and vulnerabilities. In simple terms, risks are not the causes of problems but their economic and social consequences. Although it is important to understand the causes, digital security risk management focuses primarily on their potential economic and social consequences.
- To generate benefits, the data value cycle relies on *open, interconnected, dynamic and flexible ICTs*. In most contexts, these characteristics are essential to realising the benefits of data-driven innovation (must-have features). They are not optional add-ons (nice-to-have features) that can be simply dismissed or limited. Limiting them will directly impact the expected economic and social benefits of data-intensive activities.
- Because of this indispensable openness and interconnectedness, a degree of uncertainty is inevitable and must be accepted. The digital environment cannot be secured or made completely safe. Despite all the security measures that may be put into place, risk related to the use of ICTs cannot be completely eliminated. Thus *a certain level of risk has always to be accepted (i.e. taken)* for the value cycle to provide some benefit. This is often called "residual risk". The ability to manage risk is a critical success factor in DDI.

The risk management framework helps determine which security measures can reduce risk to an acceptable level[6] in light of the potential benefits, while recognising that the same measures impose constraints on the economic and social activities at stake. These interferences should be understood and balanced with the benefits before the measures are agreed upon and implemented. They can affect performance, cost, complexity and usability, in turn impacting on profitability and time to market. They can also impact on privacy. Thus digital security risk management is a disciplined systematic approach to achieve the right balance between insufficient security measures – i.e. where the benefits are undermined by an unacceptable level of risk – and too many security measures – i.e. where the benefits are inhibited by too much security.

That raises the key question of responsibility. Traditional security focuses on securing the digital environment. Therefore, in most cases, the party responsible for the provision of the environment takes responsibility for its security, and users of the environment do not have to be concerned with it. In contrast, from a digital security risk management perspective, responsibility cannot be delegated to a separate party. Instead, the allocation of responsibility follows three principles, all of which stem from management being an integral part of economic and social (i.e. "business") decision making.

First, as noted above, managing risk means accepting a certain level of risk – or, deciding not to accept it, and therefore not to realise the benefits. The primary responsibility for managing risk should mirror the responsibility for achieving the objectives and realising the benefits. Digital security risk is not an exception to this general management principle.

Second, in complex data-driven innovation activities, it is likely that only one or a very limited number of actors will be responsible for realisation of the overarching expected benefits from the data value cycle; many other actors will each have a role to contribute, at their level, to achievement of these objectives. Among them, some will ensure that the content of the data value cycle generates the expected benefits ("business" or economic actors); others will provide the optimal digital environment to support the operation of the cycle (IT actors).[7] The distribution of responsibility for digital security risk management should therefore reflect this distribution of roles, and appropriate delegations of responsibility and authority to act should be established. Since benefits and risks are two sides of the same coin, the ultimate owner of the benefits should also ultimately own the risk. One consequence is that the primary responsibility should not be fully delegated to an IT actor who could jeopardise the economic performance of the data value cycle.

Third, DDI relies on a chain of interdependent links; to some degree, each part of the value cycle is dependent on and impacts the others. In the cycle's operation, the responsible actors cannot be isolated from one another: they form a holistic data ecosystem. The complexity of interdependencies within this ecosystem can be very high, considering for example that some elements or sub-elements of the cycle can operate across different organisations, and even across jurisdictions. Therefore, a clear mapping of roles and responsibilities is necessary. Further, digital threats can propagate extremely rapidly from one link to the other, quickly contaminating the entire cycle. The consequences of threats exploiting vulnerabilities can escalate both within the cycle and beyond, to affect other economic and social activities that depend on the cycle. For that reason, it is indispensable to establish a robust collaboration and co-operation culture supporting good communications among the business actors and the IT actors, and between the two groups. Thus to manage risk in the part of the cycle where Party A has a responsibility, a security measure may be more effective in a part under the responsibility of Party B. Similarly, security measures protecting the part of the cycle under one's responsibility may create risk in or undermine the effectiveness of another part. Considering this degree of complexity, it could be good practice to assign responsibility to someone for ensuring co-operation and collaboration among all the cycle's actors.

Possible good practices include the following examples (see also Box 5.1):

- There could be a clear rule whereby if a risk management decision made at a particular stage in the cycle would affect another stage, then it should be made collectively among the group of decision makers with responsibility in the areas of possible impact.
- Digital security risk management decisions affecting the performance of the cycle as a whole should be made at the highest level of responsibility by the actor who is responsible for the benefits from the cycle and, as such, can understand the effect of such decisions on the cycle's objectives; assess the tolerance to risk (or "risk appetite") in light of the expected benefits; and set the appropriate acceptable level of risk.

### Box 5.1. **An illustration of digital security risks**

Consider a large national or international discount supermarket chain selling mass products at a low margin and aiming to optimise its profits through high-volume sales. Data and analytics may support that objective by enabling the company to optimise its supply chain in respect to the expected demand of its customers. The company would establish a data value cycle to optimise the decision-making processes related to the chain's purchase, logistics, and marketing activities including (e.g.) price and discounts, product placement and advertising. However, the supermarket chain would not control all the data sources, as it would rely on many third parties outside its control (e.g. data brokers) to feed the cycle or even to operate some parts of it (e.g. cloud computing providers).

In this context, the AIC triad is key to data-driven innovation for the company. A breach of availability at one stage could stop or slow the ability of the company to maximise its profit margins, leading to economic losses or lost opportunities. Integrity is also a key factor. Accurate economic decisions from the cycle rely on accurate data and information flowing through the cycle and accurate analytics. Wrong decision making directly affecting the company's profitability and competitiveness could result from illegitimately modified data and information at any stage of the cycle, or from corrupted analytics. Finally, confidentiality relates to protecting the company's market position. For example, a competitor could greatly benefit from disclosure of the underlying analytic algorithms or from obtaining access to the company knowledge base, which is essential to key economic decisions and part of the company's competitive advantage. A breach of confidentiality at the value cycle's "big data" stage, i.e. data storage, could result in legal privacy challenges damaging the company's reputation and consumer trust, in addition to potential financial loss from lawsuits.

In assigning decisions, one should also clearly distinguish between those relating to provision of the digital environment (i.e. IT), which do not have a negative impact on the performance of the data value cycle (such as updates and upgrades), from those that can impact its performance and deliverables. The former should be left to the IT professionals; the latter should be first reviewed by the actors responsible for realising the objective of the value cycle, since they are best placed to understand the potential consequences for these objectives. All responsible actors should, however, take advantage of the essential role played by IT professionals in managing technical security measures and informing other decision makers about threats and vulnerabilities. Good co-operation and dialogue are essential.

Since the cycle may bring together professionals with different skills, cultures and perspectives, ensuring a high degree of collaboration will likely prove a management challenge. Establishment from the outset of a common culture of risk management would help transcend differences across various groups of actors and increase team spirit and project coherence. The creation of such a culture is a critical success factor. The multiplication of stakeholders involved in operating the data value cycle from outside the boundaries of the organisation, such as cloud providers and other outsourced services, further increases the challenge.

As noted above, many different actors with different roles will operate the data value chain and reflect different background and styles of management which need to be respected. With regard to these many different actors, digital security risk management should respect fundamental rights and values, such as privacy, as well as the legitimate interests of others. Privacy is a case where the ethics and interests of those who establish, use and benefit from the data value cycle may not be fully aligned with those whose personal data are processed. Mechanisms to reconcile conflicting interests are needed.

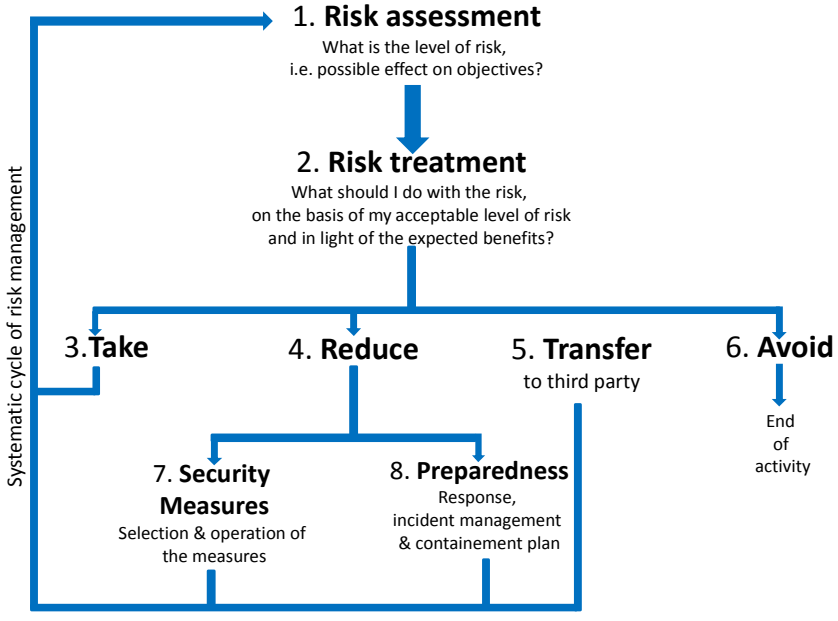
The owner of the cycle should be responsible to ensure that across each of its stages, digital security risk management is accomplished in accordance with the rights and values, regulation and culture of all parties, including parties considered "external" to the cycle but affected by it.

In summary, a culture of digital security risk management is essential to increase the likelihood of success of data-driven innovation projects. It relies on a solid understanding of risk management; the alignment of responsibility for managing risk with the responsibility to realise the objective; a robust collaboration and co-operation framework; and respect for the fundamental values and legitimate interests of others.

### *From static perimeter security to risk management cycle*

While the data value cycle in Figure 1.7 (Chapter 1 of this volume) is a valid general representation of most data-intensive innovation activities, its complexity can vary considerably depending on the size of the organisation, the number of people and entities involved (stakeholders), and many other factors. In some cases, as noted above, such a value cycle can cross multiple organisations and regulatory jurisdictions, and consequently involve a multiplicity of different professional cultures and perspectives. The complexity of the efforts to generate benefits will be mirrored in the complexity of managing digital security risk. The response to a higher degree of complexity is to establish a systematic framework for digital security risk management processes and weld it together with the data value cycle. Doing so is essential to enable risk management to scale up, as well as for auditing and accountability reasons. Figure 5.1 represents the digital security risk management cycle.

Figure 5.1. **Digital security risk management cycle**




As with the traditional security approach, security here is related to the likelihood of threats exploiting vulnerabilities to undermine the AIC triad, and the security measures available are the same in both approaches. However, their selection and application results from a completely different process that starts with the assessment of risk (Step 1 in Figure 5.1) and its treatment (Step 2), i.e. the determination of whether to take it as it is

(Step 3), reduce it (Step 4), transfer it to someone else (e.g. through contract, insurance or other legal agreement) (Step 5) or avoid it by not carrying out the activity (Step 6). If one decides to reduce the risk, the risk assessment helps determine which security measures should be selected and applied where and when, in light of the consequences of uncertain events on the economic and social objectives (Step 7). The primary criterion determining selection and application is the acceptable level of risk to the economic and social activities at stake – not just the likelihood of a threat that can exploit a vulnerability to create harm. This process provides shades of grey that enable the systematic protection of assets in proportion to their value, and therefore enable the protection to scale to the size and complexity of the value cycle. Finally, residual risk cannot be ignored. A preparedness plan (Step 8) should also be established to limit and manage the consequences of incidents when they occur and reduce the potential of escalation. Finally, since the dynamic nature of the cycle is key to DDI, the risk assessment and treatment, selection of security measures and incident management plan should likewise be operated as an ongoing cycle.

In the complex context of DDI, risk should be assessed at several levels: the level of the data value cycle as a whole; the level of each stage of the data value cycle (as represented in Figure 1.7); the level of each sub-process within each of these stages, and so on until the degree of uncertainty is considered sufficiently understood by the owner of the benefits and risk. In reality, it is the aggregation of risk assessments at the lower level that will feed the risk assessment at higher levels up to the highest one. This will produce an overarching decision-making tool in the form of a risk matrix surrounding the data value cycle and encompassing the whole data ecosystem.

## 5.2. Privacy protection for data-driven innovation

Unlike the analysis of digital security risks, which are tied to the economic and social objectives of the data-driven activity in question, analysis of privacy issues is oriented around the impact on individuals and society, whose interests may not always fall directly within those objectives. There are clear areas of overlap between security and privacy, including the security safeguards principle of the OECD (2013a) *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD Privacy Guidelines) and the utility of the risk-based approach. But there are also important differences in considering privacy issues, some of which touch on fundamental values for individuals and society. After identifying certain privacy-related impacts, the discussion turns to a number of policy approaches that could offer more effective privacy protection.

### *Possible privacy-related impacts of data-driven innovation*

Trends in data collection, analysis and use described in other chapters of this volume are transforming organisational practice across a number of business and government sectors, and could extend to many more. At the same time, these trends are raising questions about whether policies, laws and norms are able to protect privacy and other social values, such as individual liberties, that are essential for user trust in the digital economy. The issues described below may not be truly novel, but taken in combination they pose important and fresh questions about how to ensure that DDI will be deployed to the benefit of individuals, whether as consumers, social actors or citizens.

Each step of the data value cycle (Figure 1.7) on which DDI relies can raise privacy concerns. Step 1 is the initial data collection, which is becoming increasingly

comprehensive, diminishing an individual's private space. Step 2 is the massive storage of data, which increases the potential of data theft or misuse by malicious actors and other consequences of a data security breach, the risks of which may not be easy to ascertain. Steps 3 and 4 involve inferences of information and knowledge[8] enabled by data analytics, a tool that extracts information from data by revealing the context in which the data are embedded and their organisation and structure.[9] Analytics often goes well beyond the data knowingly provided by a data subject, diminishing an individual's control and creating information asymmetry. Finally, data-driven decision making (Step 5) can lead to a real-world discriminatory impact on individuals and other harms.

### *Comprehensive data collection and the loss of private space*

Many commercial and social activities, whether conducted in public or in private, leave behind some form of digital trace. A growing number of entities, such as online retailers, Internet service providers (ISPs), operating systems, browsers, social media and search engines, financial service providers (i.e. banks, credit card companies, etc.) and mobile operators have the capability to collect vast amounts of this data. Such data collection may be limited to a specific context or transaction, but usually spans a wide range of economic social activities.

Some of the data collected are knowingly and willingly provided by the consumer, and are often essential to the completion of an online commercial transaction. Behavioural advertising, by contrast, relies on the online tracking of consumers and the collection and analysis of related personal information in order to provide them with advertising tailored to their expected needs and interests. Another example is geolocation data from mobile devices, which on the one hand can be used to improve the location-based services on which many rely today, but at the same time leaves a trail of an individual's daily routines and movements, which are increasingly used for other services including for process improvements. According to a recent survey, two-thirds of device owners in the United States have no idea who has access to data from their devices or how it is used (Intel, 2014).

Other types of data are not collected directly from the consumer. Data brokers, for example, collect and aggregate personal data regarding individuals with whom they have no direct interaction, in order to offer a variety of services to third parties, such as employment background checks, localisation services and identity verification (FTC, 2014). Government and private sector researchers are increasingly using health data to evaluate outcomes, identify drug interactions, and push the boundaries of predictive medicine (OECD, 2013d). In education, as technological tools become commonplace in schools, data collection, retention, and analysis are becoming increasingly systematic, revealing greater insights into student and teacher performances (*New York Times*, 2014). The possibility of improving educational performance is evident, but so too is the challenge of introducing policies and processes for protecting sensitive student data.

While the use of data collected about individuals can benefit organisations, individuals and society, the breadth and scale of current data collection practices has given rise to concerns on the part of data subjects, and these have both social and economic ramifications. First, if citizens believe that they are being watched or monitored with respect to their online activities in ways they consider inappropriate or unfair, they may feel less free to participate in the discussion of controversial subjects; this can lead to a type of self-censorship that may undermine civil discourse and engagement. Indeed, one study indicates that citizens in several OECD countries have begun to self-censor with

respect to search terms entered into search engines, based on a widespread public belief that their use of search terms is being inappropriately monitored (Marthews and Tucker, 2014). Second, individuals may feel that certain forms of commercial data collection are inappropriate or unfair, particularly when they are being carried out without their knowledge or consent. Concerned that storage of a massive aggregation of personal data is more vulnerable to privacy violation, including through inappropriate reuse, individuals may simply forego certain online activities.

### *Inference and the loss of control*

There are a number of means that individuals use to protect their own privacy (see Box 5.2). Intuitively, the most obvious way is to withhold or conceal information relating to them. However, the ubiquitous nature of ICTs, coupled with technological advances in data analytics, makes it increasingly easy to generate inferences about individuals from data collected in commercial or social contexts, even if these individuals never directly shared this information with anyone.

#### Box 5.2. **Practical means for preventing information discovery**

Data analytics extracts information from data by revealing the context in which the data are embedded, its organisation and structure (see Chapter 3 of this volume). There exist a number of practical means for preventing or significantly increasing the cost of extracting the information embedded in the data through data analytics, though these may adversely affect data utility. Examples follow.

*Reduced collection* – A reduction in data collection can be considered the strongest means for preventing information extraction, because where no data are collected, no information can be extracted. Data subjects can withhold or decline to provide data. Data controllers can practice data minimisation. As Pfitzmann and Hansen (2010) have highlighted, data minimisation "is the only generic strategy [misinformation or disinformation aside] to enable unlinkability, since all correct personal data provide some linkability".

*Cryptography* – Cryptography is a practice that "embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorised use" (OECD, 1977). It is a key technological means to provide security for data in information and communications systems. Cryptography can be used to protect the confidentiality of data, such as financial or personal data, whether that data is in storage or in transit. Cryptography can also be used to verify the integrity of data by revealing whether data have been altered and identifying the person or device that sent it.

*De-identification* – This term covers a range of practices ranging from anonymisation to pseudonymisation. These practices share a common aim of preventing the extraction of identifying attributes (i.e. re-identification), or at least significantly increasing the costs of re-identification. *Anonymisation* is a process in which an entity's identifying information is excluded or masked so that the entity's identity cannot be, or becomes too costly to be, reconstructed (Pfitzmann and Hansen, 2010; Mivule, 2013). Some research suggests that when linked with other data, most anonymised data can be de-anonymised – that is, the identifying information can be reconstructed (Narayanan and Shmatikov, 2006; Ohm, 2009).[1] For many applications, however, some kind of identifier is needed, and having complete anonymity would prevent any useful two-way communication and transaction. *Pseudonymisation* is therefore used, whereby the most identifying attributes (i.e. identifiers) within a data record are replaced by unique artificial identifiers (i.e. pseudonyms).

Box 5.2. **Practical means for preventing information discovery (cont.)**

*Unlinkability and functional separation* – Unlinkability results from processes to ensure that data processors cannot distinguish whether items of interest are related or not (Pfitzmann and Hansen, 2010). According to ISO (Pfitzmann and Hansen, 2010), unlinkability "ensures that a user may make multiple uses of resources or services without others being able to link these uses together". De-identification is a means to enable unlinkability, but cannot guarantee it. Other technical means include functional separation and distribution (decentralisation).

*Noise addition and disinformation* – The addition of "noise" to a data set allows analysis based on the complete data set to remain significant while masking sensitive data attributes. Finding the right balance that protects privacy while minimising the costs to data utility is a challenge (Mivule, 2013). Disinformation is false or inaccurate information spread intentionally to mislead. Noise addition techniques are considered promising means to help protect privacy and confidentiality in databases, while keeping all data sets statistically close to the original data sets. Work on "differential privacy" is one example (Dwork and Roth, 2014).

1. Narayanan and Shmatikov (2007), for example, have used the "anonymous" data set released as part of the first Netflix prize to demonstrate how the authors could correlate Netflix's list of movie rentals with reviews posted on the Internet Movie Database (IMDb). This let them identify individual renters, and gave the authors access to their complete rental histories (Warden, 2011). The view that de-identification does not work has been challenged, however – see for example Cavoukian and Castro, 2014.

As highlighted in Chapter 3 of this volume, data analytics extracts information from data by revealing the context in which the data are embedded, including patterns, correlations among facts, interactions among entities, and relations among concepts (Merelli and Rasetti, 2013). Thus, data analytics enables the "discovery" of information even if there was no prior record of such information. Data analytics is not a new phenomenon. However, as the volume and variety of available data sets increase, as well as the capacity to link different data sets, so does the ability to derive further information from these data. Advances in analytics now make it possible to infer sensitive information from data that may appear trivial at first, such as past purchase behaviour or electricity consumption. The IoT will likely accelerate this trend, generating a large number of diverse but interlinkable data sets that relate to economic and social activities.

Traditionally, many privacy violations have involved disclosure of personal information beyond the envisaged recipients or beyond the purposes set out for the collection and processing of the data. However, active disclosure or new secondary uses are not a prerequisite for the inference of personal characteristics. Once linked with sufficient other information, data analysts can predict, with varying degrees of certainty, the likelihood that an individual will possess certain characteristics, building a profile. This knowledge can be used for legitimate purposes, but it can also be used in ways that individuals do not desire or expect, or which adversely affect them – for example, when it results in unfair discrimination. There is a risk that the inferences may not be accurate, but even where correct, the inferences produce possibilities for tactless, harmful or discriminatory use of data outside the individual's control (see Chapter 3 on the limits of data analytics).

### *Creation of the knowledge base and information asymmetry*

In spite of the wealth of information now available to consumers via the Internet, businesses in many respects retain more information than consumers about the features and quality of the products they sell, the contract terms and conditions, the associated production and distribution costs, the availability of competing alternatives, and so forth. Data analytics can indeed lead to valuable insights for those parties employing them. In

the credit-reporting context, for example, the very purpose of data analytics is to reduce information asymmetries by making a debtor's credit history available to potential creditors (World Bank, 2011). Certain forms of data analytics, however, entail a risk of exacerbating the information imbalance – in certain cases dramatically (Schermer, 2011) – and in ways potentially incompatible with broader societal values.

For example, the use of data analytics may increase the ability of governments and businesses to influence and persuade individual citizens and consumers. As described earlier, companies are often capable of targeting a particular consumer with advertisements across a range of websites and apps. This capacity has also been used for political campaigns (Hurwitz, 2012; Rutenberg, 2013; Nickerson and Rogers, 2014). Tailoring advertisements to the interests of consumers may benefit both the company and the consumer. However, concerns have been raised that the information inferred through data analytics may also facilitate aggressive or predatory marketing practices, whereby a company exploits the vulnerabilities of consumers in a way that induces them to purchase goods or services that they would not otherwise have bought. In the context of government-citizen relationships in areas such as health and education, the same data-driven approaches that bring improved government delivery of services to citizens can also expand government power (EOP, 2014, p. 22).

Behavioural factors (e.g. the tendency of individuals to focus on short-term benefits and costs, their tendency to automatically accept defaults set by organisations, and their overconfidence) can lead individuals to make poor and sometimes costly decisions (OECD, 2010). The issue of information asymmetry can be further exacerbated by the limited transparency of data analytics, particularly with respect to data controllers who have no direct interaction with consumers. Many individuals may either be unaware that data analytics are affecting the marketing and delivery of goods and services they are being offered, or have considerable difficulty ascertaining how exactly analytics are being used to influence them or to determine the offers they see online. Individuals are becoming more transparent to organisations, but it is not clear that there is a parallel advance in the transparency of the data-processing practices of organisations to individuals.

### *Data-driven decision making, discrimination and other societal values*

Data analytics can be used to provide new insights into human behaviour and societal and macroeconomic trends. In their search for competitive advantage, private actors increasingly rely on the predictive capabilities of data analytics. While these predictive analyses may result in greater efficiencies, they may also perpetuate existing stereotypes, limiting an individual's ability to escape the impact of pre-existing socio-economic indicators.

Classification based on attributes is at the heart of many forms of data analytics associated with profiling, an activity defined in the section "The pervasive power of data analytics" in Chapter 3 of this volume. Through data mining techniques that extract information patterns from data sets, a data analyst can discover patterns and relationships among different data objects, which in turn allow for increased differentiation. A well-known example in this regard is consumer segmentation: individual consumers are categorised among different behavioural or socio-economic profiles on the basis of observed or inferred attributes.

One form of differentiation among consumers that has recently been gaining attention is known as "price discrimination" (also referred to as "differential", "personalised" or "dynamic" pricing). Price discrimination is traditionally defined as firms' sale of the same good to different customers at different prices, even though the cost of producing for the

two customers is the same (OECD, 2002). This can occur directly, where each consumer is charged based on his or her willingness to pay, or indirectly, through volume discounts or discounts for groups such as students or the elderly (OFT, 2013).

Price discrimination is facilitated by data analytics in a number of ways. For example, by analysing a consumer's behaviour over a certain period, vendors can obtain a strong indication of future purchasing habits, which allows them to set their prices accordingly. Similarly, data analytics can allow vendors to differentiate among customers with different degrees of willingness to pay, by steering them towards different sets of products when they search within a product category (Valentino-Devries, 2012).

Proponents defend price discrimination practices on the grounds of efficiency and an ability to increase aggregate economic welfare. Opponents argue that such practices are unfair, violating notions of equality among consumers and exacerbating existing information asymmetries (see Box 5.3). Detailed consumer profiles enable vendors to obtain a strong indication of a consumer's demand curve and reserve price. The consumer, however, typically has no idea of a vendor's reserve value, and is disadvantaged as a result. While a consumer may retain the ability to shop elsewhere, the transactional costs can add up. There are also transparency issues, as consumers may be unaware that the prices they see are determined in part by their personal data collected in the past.

Box 5.3. **Consumer reaction to price discrimination**

- According to a survey carried out from January 2004 to May 2005, 87% of Americans surveyed strongly object to or would be bothered by the practice of online stores charging people different prices for the same products based on information collected about their shopping habits (Turow, Feldman and Meltzer, 2005).
- A number of studies suggest that consumers perceive personalised pricing as unfair (Garbarino and Lee, 2003; Levine, 2002; Hillman and Rachlinski, 2001; Odlyzko, 2003).
- Others suggest that consumers can accept price discrimination as long as all consumers have equal access to better prices and benefit from product choices (Cox, 2001; Dickson and Kalapurakal, 1994).
- Consumers tend to believe that coupons, rewards and discounts are fair practices (Narayanan, 2013).

Price discrimination is not new and, as a legal matter, is not generally considered to be an unfair commercial practice.[10] There is a long history of prices negotiated directly between businesses and consumers, or consumers being placed in different categories and charged accordingly. What is new is the potential that analytics creates to systematise personalised pricing. Anecdotal evidence suggests that the practice is not yet widespread (EOP, 2015). But if it were to become a more commonplace activity, how would consumers react?

While differentiating on the basis of price may be the most overt type of discrimination, analytics can also enable personalised treatment in other dimensions of the customer-business relationship. Customer service calls, complaint handling and many other interactions can be tailored to the specific customer. Consideration may be called for as to whether there are limits beyond which differential treatment of consumers should be considered a form of discrimination and discouraged.

Certain uses of data analytics may have additional and more serious implications for individuals, for example by affecting their ability to secure employment, insurance or credit. Indeed, this is the precise purpose of data analytics in credit reporting systems, to

support "unbiased credit decision-making … based on objective and correct data" and to "discipline debtor behaviour" by rewarding good credit history (World Bank, 2011, p. 23). Historically, credit has been granted on the basis of a credit officer's personal knowledge of the debtor. Ideally, advanced data analytics in credit reporting systems can empower consumers, enabling credit to those denied in the past due to some form of prejudice (e.g. assuming automatically that a low-income individual is always a bad debtor). At the same time, they also "raise the potential of encoding discrimination in automated decisions," in ways not fully transparent (EOP, 2014).

Segmentation and differentiation among individuals can yield important benefits to both organisations and individuals, ranging from well-targeted offers to credit to underserved communities, personalised medicine and improved fraud detection. Some forms of discrimination, however, are generally considered unethical or even illegal, such as differentiation on the basis of race, gender, ethnicity or disability (EOP, 2014, p. 64). Even when discrimination is based on less contentious characteristics (such as income level), there is still a risk of discrimination against certain social groups that might otherwise be protected. This may be the case, for example, where the characteristics used to differentiate are shared by a majority of individuals who belong to a particular social or racial group (Sweeney, 2013). Similarly, characteristics such as geographic location or postal code may serve as effective proxies to disguise what would otherwise be unlawful discrimination. In other words, even when the categories of differentiation that result from data analytics do not derive from prejudicial sources, they may nonetheless have a discriminatory effect against certain social groups in practice.

Discrimination may take other forms that run counter to societal values. To take an example related to fairness, consider a scenario in which an increasing number of people choose to collect and track data about their health, lifestyle, diet or even driving habits, and disclose them to their insurance company in exchange for discounted rates. Such an exchange may well serve their individual interests. But such practices may have social costs for others who choose not to share their data, for whatever reason. These individuals could eventually be charged higher rates than those who do share, or even be denied coverage – not because they represent a higher risk, but rather because they do not agree to participate in the profiling. Such scenarios may have policy implications with regard to fairness.

The links to freedom of speech and association are more difficult to discern, but of significant potential consequence. An environment where digital activity is systematically tracked and aggregated may create a "chilling effect" in which an individual curtails communications and activities in fear of uncertain but possibly adverse consequences (IWGDPT, 2014, p. 9). The widespread exchange of views with those whose opinions may differ may be undermined by what has been called the "filter bubble" effect when efforts to personalise news and other content narrow the range of views exposed to an individual (Pariser, 2012). More generally, data analytics can affect human decision making by shaping the behaviour of individuals, but it may also (unintentionally) alter individuals' preferences and, where the use of analytics undermines the values of those being influenced, set society on an irreversible transformative path (see Lessig, 1999; Frischmann, 2014).

### *Policy approaches for more effective privacy protection*

Several responses can be identified for improving the effectiveness of privacy protections in the context of data-driven innovation. One set of initiatives is grouped under a heading of improving transparency, access and empowerment for individuals. A second area of focus is the promotion of responsible usage of personal data by

organisations. The promise of technologies used in the service of privacy protection has been long noted. Finally, the application of risk management to privacy protection is highlighted as providing another possible avenue.

These initiatives are not, of course, mutually exclusive and may best be deployed in combination with each other. Likewise, their implementation fits within the broader policy framework of an instrument such as the OECD Privacy Guidelines and the applicable legislation. A number of challenges have been noted in attempts to apply elements of the broader framework in terms of the scale of data use today. For example, the Report from the Expert Group that helped prepare revisions to the OECD Privacy Guidelines identified the role of consent, the role of the individual, the roles of purpose specification and use limitation, and the definition of personal data as raising issues for further study (OECD, 2013b).

Those challenges may not be surprising, given the historical context that shaped the elaboration of the principles. The predominant data processing model in the 1970s involved the direct provision of personal data from a data subject to a data controller. Although some examples of observed or inferred data can be found from that period, the basic model assumed an active role for the individual as a participant in the data collection process.

Today that assumption is challenged. The growth of the Internet, including the Internet of Things, has led to an explosion in observable data, with sensor-equipped smart devices poised to expand that category further. And the capacity to run analytics over unstructured data sets – which may be related to identified or identifiable individuals – is significantly expanding the category of inferred data and probability-based determinations. The context of processing addressed in this volume is focused to a much greater extent on data that are observed or inferred though sensors and analytics, which are growing at a much faster rate than user-contributed data (Abrams, 2014)

It should not be surprising, then, that the principles formulated for an active, engaged data subject are more challenging to apply where the personal data in question are generated at a distance from the subject. Nevertheless, attention to the areas identified below can help improve the effectiveness of privacy protection in a dynamic environment, where there is such flux in the scale, scope and value of personal data uses.

### *Transparency, access and empowerment*

Promoting transparency and the rights to access and correction have been part of the OECD Privacy Guidelines since their initial adoption in 1980, and are incorporated into national laws around the world. Transparency and access have long been recognised as powerful tools against discrimination, as they help enable data subjects to ascertain the basis on which decisions are taken. The Council of Europe recommends that in some circumstances the transparency extend to include the logic underpinning the processing in the context of profiling (Council of Europe, 2010). However, many individuals today find it difficult to exercise these rights. There are a number of new initiatives aimed at rebalancing information asymmetries between individuals and organisations, and better enabling individuals to reap the benefit and value of their data. Governments are partnering with businesses to provide consumers with access to their personal data (including their own consumption and transaction data) in portable, electronic formats.

One element in a number of these initiatives is data portability, which allows users to more easily change data controllers by reducing switching costs, and enables them to analyse their own data for their own benefit by receiving it in a usable format. Data

portability not only promises to give individuals a key role in promoting the free flow of their personal data across organisations, thereby strengthening their participation in data-driven innovation processes; it is also seen as a means of increasing competition among providers of data-driven products.

In the United States for example, in 2011 the US National Science and Technology Council launched Smart Disclosure, an initiative aimed at providing consumers with access to data about products and companies as well as to their own data, in a secure, user-friendly and portable electronic format (NSTC, 2013). Other projects include the *Green Button* initiative, aimed at providing electricity customers with easy access to their energy usage data in a consumer-friendly and computer-friendly format. Recent efforts in the United States have focused on enhancing the transparency around the practices of data brokers (FTC, 2014) who have begun to respond with initiatives of their own.[11] In 2011, a government-backed initiative called *Midata* was launched in the United Kingdom to help individuals access their transaction and consumption data in the energy, finance, telecommunications and retail sectors. Under the programme, businesses are encouraged to provide their customers with their consumption and transaction data in a portable, preferably machine readable format. A similar initiative has been launched in France by Fing (Fondation Internet Nouvelle Génération), which provides a web-based platform MesInfos,[12] for consumers to access their financial, communication, health, insurance and energy data that are being held by businesses. Last, but not least, the right to data portability proposed by the EC in the current proposal for reform of their data protection legislation aims at stimulating innovation through more efficient and diversified use of personal data by allowing users "to give their data to third parties offering different value-added services" (EDPS, 2014).

These initiatives (discussed further in Chapter 4 of this volume), promise greater control to individuals wishing to make informed decisions and increase their trust in the data-intensive services that organisations seek to deliver. But such programmes may also bring significant costs, in terms of both developing and maintaining the mechanisms for enhanced data access and compliance with relevant regulations (Field Fisher Waterhouse, 2012). That raises the question about who should bear the costs for developing and maintaining these mechanisms.

Other initiatives aiming to address transparency issues for individuals include efforts to develop "multi-layered privacy notices": simplified notices providing basic information supplemented by more complete privacy statements (OECD, 2006). Another example is "just in time" notices that aim to deliver messages to an individual at the moment when they are most likely to be of use. Developing privacy icons is another proposal to simplify and improve the communication of information about privacy practices (LIBE, 2013). Increasingly, feedback and awareness tools are being made available to show individuals the possible related consequences of activities that they and others may perform within a particular system. Continued development of new ways of effectively presenting information to individuals can help address the complexity of DDI.

The transparency called for in the "Openness" principle of the OECD Guidelines serves a broader purpose than its direct value to individuals in exercising their access rights; it enables enforcement authorities, privacy advocates, journalists and the general public to better understand and evaluate privacy practices.

### *Responsible usage and effective enforcement*

Focusing more explicitly on promoting responsible usage by organisations could be a useful complement to efforts to improve transparency, access and empowerment. Further efforts are needed to find ways to express boundaries outside of which responsible organisations should not use the fruits of data analytics.

One way to make organisations and individuals aware of the limits to responsible uses – as well as common mistakes and the potentially adverse effects of data analytics – is through education and awareness, which are specifically identified in the revised OECD Privacy Guidelines' call for "complementary measures". Privacy frameworks are articulated in terms of high-level principles that need to be applied in order to ensure effective implementation in practice.

Policy makers and enforcement authorities would need to play a role in helping organisations to identify appropriate substantive limits. Examples can be drawn from guides to credit scoring, policies against the use of genetic information by insurers, and prohibitions on the use of social networking data by employers.

The new provisions in the OECD Privacy Guidelines on implementing accountability respond directly to these new concepts and emerging business practices. Greater emphasis within organisations on internal processes to assign responsibility and to assess (and reassess) risks and controls should improve decisions about responsible usage in those organisations. Some have suggested that one way to treat these issues is through an ethical lens, subjecting data-driven decision making to oversight by experts in data ethics (Mayer-Schönberger and Cukier, 2013), an approach that is gaining momentum (see for example Richards and King, 2014; Johnson and Henderson-Ross, 2012).

Strengthening the enforcement tools of privacy authorities is also needed if these bodies are to play a greater role in monitoring responsible uses. The revised OECD Privacy Guidelines already provide that governments should equip authorities with the resources and technical expertise to exercise their powers effectively; the need for resources and expertise will be all the greater if they are given greater responsibilities to monitor use.

### *Privacy-enhancing technologies*

There are a number of technologies that aim to preserve both privacy and functionality (see Box 5.2). Examples may include privacy-preserving analytics, differential privacy and anonymous credentials. De-identification is often a practical method for obtaining the benefits from data analytics while minimising privacy risks. These risks cannot be completely eliminated, however, and where a sufficient number of different sources of de-identified data are combined, patterns can be revealed that may eventually be traceable back to an individual (EU WP29, 2014a). Some in fact doubt that such tools can withstand progress in re-identification methods, questioning their efficacy as a dependable policy response (PCAST, 2014, p. 39).

Actual risks with regard to re-identification will depend on the context in which the analytics are to be carried out, as well as on the resources and motivation of those who might re-identify. Risk assessment should also consider the likely consequences to the data subject in the event that re-identification occurred. Approaches that combine technical de-identification measures with administrative and legal measures (e.g. enforceable commitments not to re-identify) can help minimise linkability risks (FTC, 2012).

Other types of technical tools can record and describe the life cycle of personal data collected by an organisation (such as provenance) and may assist organisations in managing personal data, and as well as facilitate accountability. For example, advanced data-tagging schemes may be able to attach context and preference information to the data, to help govern future uses (EOP, 2014, p. 56).

Safeguards such as functional separation may also have a useful role to play in ensuring that data used for statistical or other research purposes cannot be used to take decisions with respect to a particular individual (EU WP29, 2013, p. 30). At the same time, functional separation can also support uses related to gaining appropriate insights and knowledge. Policy makers could consider stimulating further research and development in this area, and promote adoption via private-public partnerships, certification schemes and similar initiatives.

Finally, it should be noted that it is possible that the same techniques of data analytics that create discriminatory impacts can likewise be deployed to help individuals and groups identify and assess discriminatory practices, and thereby aid in the enforcement of their rights (EOP, 2014, p. 65).

### *Privacy risk management*

The revised OECD Privacy Guidelines introduce risk management as a key theme for privacy protection, especially in the context of developing privacy management programmes to implement accountability. Risk assessment can consider data sources and quality as well as the sensitivity of the intended uses. In addition to mitigating against the risks of misuse, the assessment can also examine the process by which the data have been analysed; this can help identify where errors or mistakes may have been introduced into the analytical process itself. To be effective, the scope of any privacy risk assessment must be sufficiently broad to take into account the wide range of harms and benefits, yet sufficiently simple to be applied routinely and consistently. It is a challenging task, involving the identification of relevant risks, which may be subjective, and then determining their possible severity and likelihood of impact. As noted above, mitigation measures involving technical tools to de-identify data – particularly when combined with public commitments not to re-identify – may have considerable value, even if they cannot serve as a full guarantee of protection.

Risk-based approaches are not entirely new to privacy frameworks. Risk assessment is implicit, for example, in the OECD Guideline's security safeguards principle[13] and there are close links to privacy impact assessments. Nevertheless, the extent to which a comprehensive risk management approach can strengthen application of the privacy principles is a topic for continued work. As explained in the above section on digital security, successful risk management requires both understanding the risk culture and establishing a risk management framework. The culture of risk management requires a shift from the protection of an asset or an environment from threats, to the optimisation of benefits by recognising that a certain level of risk has to be accepted. How would this translate to privacy protection, where the risks to the individual need to be treated independently of the risks to the organisation?

Risk management also requires one to set the acceptable level of risk, and to treat the risk accordingly on the basis of a full risk assessment. Complex questions remain to be explored further to apply this to privacy protection, such as how to allocate responsibility and how to define the acceptable level of risk. Further, the risk management framework requires establishing a full and ongoing risk management cycle, where awareness, skills,

responsibility and co-operation play key roles, and where risk assessment and treatment are continuous in order to take into account the dynamic nature of the activities and the environment. Finally, the risks to the organisation need to be separated from the risks to the individual. There may be a useful role for third party accreditation in some situations, to validate internal processes for implementing risk-based approaches. Further work is needed to understand how such a framework would best be translated to support the existing privacy protection principles.

## 5.3. Key findings and policy conclusions

The current and potential benefits of data-driven innovation – building on the expanding availability of data, improved tools to link, process and store them, and algorithms for deriving insights – are amply discussed in other chapters, and have not been addressed here. The focus here has instead been on the importance of addressing the trust issues, the challenges of doing so, and possible ways forward.

Addressing security in the context of data-driven innovation raises a double challenge: first, shifting the culture and mindset of decision makers and other parties involved in DDI, from traditional to risk-based digital security; second, systematically implementing an ongoing risk management process in the overall data value cycle and within each of its parts. The complexity of applying digital security risk management to activities such as data-driven innovation should not be underestimated. It requires a high degree of systematisation and significant management efforts, bundled with operation of the data value cycle itself. Notably however, this is the same risk management approach routinely applied by many businesses in other spheres of their activities to increase their likelihood of success. Revision of the OECD Security Guidelines offers an opportunity to elevate the need for attention to digital security risks to the highest levels in organisations – a key to progress in this area.

The privacy challenges described are not really new. Risks of discrimination are at the heart of privacy laws dating back to the 1970s. As early as 1980, the OECD called for measures to prevent unfair discrimination in its Privacy Guidelines. But the data-intensive developments described in this book do bring the privacy challenges into greater focus.

Several particular points also emerge as showing promise to improve user trust in data-driven innovation. Privacy risk management has been identified as important, but considerable work is still needed to understand how to implement a risk approach for privacy. The experience of the security risk management community may be usefully brought to bear in helping privacy professionals make progress in this area, and this is a topic for future work at the OECD.

Privacy-enhancing technologies continue to offer promise, both in reducing the identifiability of individuals, and in improving the traceability and accountability of policies to protect privacy. Transparency, access and empowerment remain essential to any effective privacy framework, and efforts to improve these dimensions are important. Data access and portability measures can help minimise the information asymmetries and power imbalances that favour data-intensive organisations.

Perhaps the most difficult policy prescription advanced in this chapter is a need for greater effort to articulate substantive boundaries within which responsible uses would be limited. Determining where these boundaries lie – and who should make this determination – will become an increasingly necessary task for organisations making good on the promise of data-driven innovation.

# Notes

1 The 2002 OECD *Recommendation concerning Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* ("Security Guidelines") is being revised at the time of writing.

2 Various alternative models coexist, but the AICIC triad is the most universally recognised.

3 An analogy may be useful here: research shows that biological systems use diversity as a powerful strategy to remain open while successfully responding to the multitudes of evolving threats constantly attacking them. See Forrest, Hofmeyr and Edwards, 2013.

4 For example, those in public and private organisations, who are ultimately responsible for the realisation of economic and social objectives related of data-driven innovation.

5 There are many definitions of risk in various standards. The concept of risk as the effect of consequences on objectives is borrowed from ISO risk standards: ISO 31000 and ISO Guide 73, as well as ISO 27000:2012.

6 Instead of being reduced, risk can also be taken; transferred to someone else; or avoided by not carrying out the activity.

7 This is a simplification: some actors may have a dual role and other categories of actors could also be considered.

8 Data, information and knowledge are seen as different but interrelated concepts. Information is often conveyed through data, while knowledge is typically gained through the assimilation of information. The boundaries between data, information and knowledge may not always be clear, and these concepts are often used as synonyms in media and literature. However, separating the concepts is important to gain a better understanding of data-driven value creation. One can have a lot of data, but not be able to extract value from them when not equipped with the appropriate analytic capacities (see Chapter 3 of this volume). Similarly, one can have a lot of information, but not be able to gain knowledge from it, a phenomenon nowadays better known as "information overload." As observed by Herbert Simon, "a wealth of information creates a poverty of attention" (Shapiro and Varian, 1999).

9 The term is more fully defined and discussed in Chapter 3 of this volume.

10 For example, discrimination in access to fares among passengers on the basis of their place of residence or nationality can infringe EC Regulation No. 1008/2008 of the European Parliament and Council on common rules for the operation of air services in the European Union: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008R1008. More generally, the European Union's Article 29 Data Protection Working Party gives the example of price discrimination based on the computer type used for online purchases as a problematic example of an incompatible use of data (EU WP29, 2013, p 23).

11 For example, the commercial data broker Acxiom has created a website for consumers to gain access to data held about them – www.aboutthedata.com -- in response to the "Reclaim Your Name" initiative by a Commissioner of the Federal Trade Commission (Brill, 2013).

12 See: http://fing.org/?-MesInfos-les-donnees-personnelles-&lang=fr.

13 The EU Article 29 Working Party notes a number of areas in the EU framework (EU Art. 29, 2014c). Risk assessment is required by Korea's certification system (Personal Information Management System).

# *References*

Abrams, Martin (2014), "The origins of personal data and its implications for governance", OECD Expert Roundtable Discussion, Background Paper A – Session I, 21 March 2014 http://informationaccountability.org/wp-content/uploads/Data-Origins-Abrams.pdf.

Brill, Julie (2013), "Reclaim Your Name", 26 June, www.ftc.gov/speeches/brill/130626computersfreedom.pdf (accessed 24 April 2015).

Cavoukian, A. and D. Castro (2014), "Big data and innovation, setting the record straight: De-identification does work", Office of the Information and Privacy Commissioner, Ontario, 16 June, www.privacybydesign.ca/index.php/paper/big-data-innovation-setting-record-straight-de-identification-work.

Council of Europe (2010), "Recommendation on the protection of individuals with regard to the automatic processing of personal data in the context of profiling", CM/REC(2010)13, 23 November, https://wcd.coe.int/ViewDoc.jsp?id=1710949.

Cox, J. (2001), "Can differential prices be fair?", *Journal of Product and Brand Management*, Vol. 10, pp. 264-76, www.emeraldinsight.com/journals.htm?articleid=857764.

Dickson, P. and R. Kalapurakal (1994), "The use and perceived fairness of price-setting rules in the bulk electricity market", *Journal of Economic Psychology*, Vol. 15, pp. 427-48, www.sciencedirect.com/science/article/pii/016748709490023X.

Dwork C. and A. Roth (2014), "The Algorythmic Foundations of Differential Privacy", *Foundations and Trends in Theoretical Computer Science*, Vol. 9, Nos. 2-4, pp. 211-407, http://dx.doi.org/10.1561/0400000042.

EDPS (European Data protection Supervisor) (2014), "Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the digital economy", March, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf.

EOP (Executive Office of the President, United States) (2015), "Big data and differential pricing", February, www.whitehouse.gov/sites/default/files/docs/Big_Data_Report_Nonembargo_v2.pdf, accessed 24 April 2015.

EOP (2014), "Big data: Seizing opportunities, preserving values", www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf, accessed 24 April 2015.

EU WP29 (Article 29 Data Protection Working Party, European Union) (2014a), "Opinion 05/2014 on Anonymisation Techniques" adopted 10 April 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

EU WP29 (2014b), "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC", adopted 9 April, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

EU WP29 (2014c), "Statement on the role of a risk-based approach in date protection legal frameworks", adopted 30 May 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

EU WP29 (2013), "Opinion 03/2013 on purpose limitation", adopted 2 April, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

Field Fisher Waterhouse (2012), "Will access to midata work?", 19 November, http://privacylawblog.ffw.com/2012/will-access-to-midata-work, accessed 24 April 2015.

Forrest, S., S. Hofmeyr and B. Edwards (2013), "The complex science of cyber defense", *Harvard Business Review*, 24 June, http://blogs.hbr.org/2013/06/embrace-the-complexity-of-cybe/.

Frischmann, B.M. (2014), "Human-focused turing tests: A framework for judging nudging and techno-social engineering of human beings", draft paper, 22 September, http://dx.doi.org/10.2139/ssrn.2499760, accessed 23 April 2015.

FTC (Federal Trade Commission, United States) (2014) "Data brokers: A call for transparency and accountability", May, www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014, accessed 24 April 2015.

FTC (2012) "Protecting privacy in an era of rapid change: Recommendations for businesses and policy makers", www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf, accessed 24 April 2015.

Garbarino, E. and O.F. Lee (2003), "Dynamic pricing in Internet retail: Effects on consumer trust", *Psychology and Marketing*, Vol. 20, pp. 495-98, http://onlinelibrary.wiley.com/doi/10.1002/mar.10084/abstract.

Hurwitz, J. (2012), "The making of a (big data) president", *Bloomberg Businessweek*, Management Blog, 14 November, www.businessweek.com/articles/2012-11-14/the-making-of-a-big-data-president.

Intel (2014), "Survey: Distrust and lack of understanding in data privacy fact sheet", www.intel.com/newsroom/kits/bigdata/pdfs/Privacy_Survey_Factsheet.pdf, accessed 24 April 2015.

IWGDPT (International Working Group on Data Protection in Telecommunications) (2014), "Big data and privacy: Privacy principles under pressure in the age of big data analytics", www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf, accessed 24 April 2015.

Johnson, D. and J. Henderson-Ross (2012), "The new data values", *Aim*, www.aimia.com/content/dam/aimiawebsite/CaseStudiesWhitepapersResearch/english/WhitepaperUKDataValuesFINAL.pdf, accessed 24 April 2015.

Levine, M.E. (2002), "Price discrimination without market power", Discussion Paper No. 276, 2/2000, Harvard Law School, Cambridge, MA, www.law.harvard.edu/programs/olin_center/papers/pdf/276.pdf.

Lessig, L. (1999), *Code and Other Laws of Cyberspace*, 30 November, Basic Books.

LIBE (Committee on Civil Liberties, Justice and Home Affairs, European Parliament) (2013) "Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data", 22 November, www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BREPORT%2BA7-2013-0402%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN.

Mayer-Schönberger, V. and K. Cukier (2013), *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, Eamon Dolan/Houghton Mifflin Harcourt.

Merelli, E. and M. Rasetti (2013), "Non locality, topology, formal languages: New global tools to handle large data sets", International Conference on Computational Science, ICCS 2013, *Procedia Computer Science 18,* pp. 90-99, http://dx.doi.org/10.1016/j.procs.2013.05.172.

Mivule, K. (2013), "Utilizing Noise Addition for Data Privacy, an Overview", Proceedings of the International Conference on Information and Knowledge Engineering (IKE 2012), pp. 65-71, http://arxiv.org/pdf/1309.3958.pdf, accessed 22 April 2015.

Morrone, A., N. Tontoranelli and G. Ranuzzi (2009), "How good is trust? Measuring trust and its role for the progress of societies", *OECD Statistics Working Paper*, Paris.

Narayanan, A. (2013), "Personalized coupons as a vehicle for perfect price discrimination", 25 June, http://33bits.org/2013/06/25/personalized-coupons-price-discrimination, accessed 24 April 2015.

Narayanan, A. and V. Shmatikov (2006), "How To Break Anonymity of the Netflix Prize Dataset", CoRR, abs/cs/0610105, 05 December, http://arxiv.org/abs/cs/0610105.

New York Times (2014), "Protecting student privacy in online learning", 24 September, www.nytimes.com/roomfordebate/2014/09/24/protecting-student-privacy-in-online-learning (accessed 24 April 2015).

Nickerson, D.W. and T. Rogers (2014), "Political campaigns and big data", *Journal of Economic Perspectives*, Vol. 28, No. 2, pp. 51-74, http://dx.doi.org/10.1257/jep.28.2.51.

NSTC (National Science and Technology Council, Executive Office of the President, United States) (2013), "Smart disclosure and consumer decision making: Report of the task force on smart disclosure", 30 May, www.whitehouse.gov/sites/default/files/microsites/ostp/report_of_the_task_force_on_smart_disclosure.pdf.

Odlyzko, A. (2003), "Privacy, economics, and price discrimination on the Internet", Working Paper Series of the University of Minnesota, 27 July, http://ssrn.com/abstract=429762.

OECD (2014a), "Summary of the OECD privacy expert roundtable: Protecting privacy in a data-driven economy: Taking stock of current thinking", OECD Publishing, Paris, http://dx.doi.org/10.1787/5k3xz5zmj2mx-en.

OECD (2014b), *Society at a Glance 2014*, OECD Publishing, Paris.

OECD (2013a), Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 11 July, C(2013)79, www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

OECD (2013b), "Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines", OECD Publishing, Paris, http://dx.doi.org/10.1787/5k3xz5zmj2mx-en.

OECD (2012a), Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies, OECD Publishing, Paris, http://dx.doi.org/10.1787/5k8zq92vdgtl-en.

OECD (2011a), *Society at a Glance 2011: OECD Social Indicators*, OECD Publishing, http://dx.doi.org/10.1787/soc_glance-2011-en.

OECD (2010), *Consumer Policy Toolkit*, Paris, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264079663-en, www.oecd-ilibrary.org/governance/consumer-policy-toolkit_9789264079663-en.

OECD (2006), "Making Privacy Notices Simple: An OECD Report and Recommendations", OECD Publishing, Paris, http://dx.doi.org/10.1787/231428216052.

OECD (2002), "Price Discrimination", *Glossary of Statistical Terms*, OECD, Paris, http://stats.oecd.org/glossary/detail.asp?ID=3283, accessed 24 April 2015.

OECD (1997), Recommendation of the Council concerning Guidelines for Cryptography Policy, C(97)62/FINAL, 27 March, http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=115.

OFT (Office of Fair Trading, United Kingdom) (2013) "The economics of online personalised pricing", May, http://webarchive.nationalarchives.gov.uk/20140402142426/http://www.oft.gov.uk/shared_oft/research/oft1488.pdf, accessed 24 April 2015.

Ohm, P. (2009), "The rise and fall of invasive ISP surveillance", *University of Illinois Law Review* 1417.

Online etymology dictionary (2014), "Security", etymonline.com, www.etymonline.com/index.php?term=security, accessed 23 October 2014.

Pariser, Eli (2012), The Filter Bubble: How the New Personalised Web is Changing What We Read and How We Think, Penguin Books, April.

PCAST (President's Council of Advisors on Science and Technology, United States) (2014), "Big data and privacy: A technological perspective", www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf, accessed 23 April 2015.

Pfitzmann, A. and M. Hansen (2010), "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management", v0.34, 10 August, http://dud.inf.tu-dresden.de/Anon_Terminology.shtml, accessed 23 April 2015.

Putnam, R., R. Leonardi, and R. Y. Nanetti (1993), *Making Democracy Work: Civic Traditions in Modern Italy*, Princeton University Press, Princeton, NJ.

Richards, N.M. and J.H. King (2014), "Big data ethics", *Wake Forest Law Review*, 19 May, http://ssrn.com/abstract=2384174.

Rowling, J. K. (1998), *Harry Potter and the Chamber of Secrets*, Bloomsbury.

Rutenberg, J. (2013), "Data you can believe in", New York Times, 20 June, www.nytimes.com/2013/06/23/magazine/the-obama-campaigns-digital-masterminds-cash-in.html.

Schermer, B.W. (2011), "The limits of privacy in automated profiling and data mining", *Computer, Law & Security Review*, Vol. 27, p. 45-52.

Sweeney, L. (2013), "Discrimination in online ad delivery", 28 January http://dx.doi.org/10.2139/ssrn.2208240

Turow, J., L. Feldman and K. Meltzer (2005), "Open to exploitation: American shoppers online and offline", Annenberg Public Policy Center of the University of Pennsylvania, http://repository.upenn.edu/cgi/viewcontent.cgi?article=1035&context=asc_papers.

Valentino-Devries, J. (2012), "Websites vary prices, deals based on users' information", *Wall Street Journal*, 24 December, http://online.wsj.com/news/articles/SB10001424127887323777204578189391813881534.

Warden, P. (2011), "Why you can't really anonymize your data", *O'Reilly Strata*, 17 May, http://strata.oreilly.com/2011/05/anonymize-data-limits.html.

World Bank (2011), "General principles for credit reporting", *World Bank Consultative Report*, March, para. 20, http://siteresources.worldbank.org/FINANAICLSECTOR/Resources/GeneralPrinciplesforCreditReporting(final).pdf.

# *Further reading*

Cleveland, H. (1982), "Information As a Resource", *The Futurist*, December, http://hbswk.hbs.edu/pdf/20000905cleveland.pdf.

Cooper, J.C. (2013), "Privacy and antitrust: Underpants gnomes, the First Amendment, and subjectivity", George Mason Law & Economics Research Paper No. 13-39, 21 June, http://ssrn.com/abstract=2283390.

Foundation Internet Nouvelle Génération website, http://fing.org/?-MesInfos-les-donnees-personnelles-&lang=fr, accessed 23 October 2014.

FTC (2007), "Federal trade commission closes google/doubleclick investigation", 20 December, www.ftc.gov/news-events/press-releases/2007/12/federal-trade-commission-closes-googledoubleclick-investigation (accessed 24 April 2015).

Gugeshashvili, G. (2009), "Is goodwill synonymous with reputation", *Juridica International* XVI, p. 126-34, www.juridicainternational.eu/public/pdf/ji_2009_1_126.pdf.

Hillman, R.A. and J.J. Rachlinski (2001), "Standard-form contracting in the electronic age", Working Paper Series of the Cornell Law School, http://ssrn.com/abstract=287819.

Marthews, A. and C. Tucker (2014), "Government surveillance and internet search behavior", 24 March, http://ssrn.com/abstract=2412564 or http://dx.doi.org/10.2139/ssrn.2412564.

Obama (President Barack Obama, United States) (2012), Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy", www.whitehouse.gov/sites/default/files/privacy-final.pdf, accessed 23 April 2015.

OECD (2013b), "Supplemental Explanatory Memorandum to the Revised Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data", OECD, Paris, www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

OECD (2013d), *Strengthening Health Information Infrastructure for Health Care Quality Governance: Good Practices, New Opportunities and Data Privacy Protection Challenges*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264193505-en

OECD (2013e), *The Internet Economy on the Rise: Progress since the Seoul Declaration*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264201545-en.

OECD (2012c), *Improving the Evidence Base for Information Security and Privacy Policies*, OECD Publishing, Paris, http://dx.doi.org/10.1787/5k4dq3rkb19n-en.

OECD (2011b), *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, OECD Publishing, Paris, http://dx.doi.org/10.1787/5kgf09z90c31-en.

OECD (1997), *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris, www.oecd.org/internet/ieconomy/guidelinesforcryptographypolicy.htm.

Project VRM (2014), Project VRM website, http://cyber.law.harvard.edu/projectvrm/Main_Page, accessed 23 October 20014.

Shapiro, C. and H.R. Varian (1999), *Information Rules: A Strategic Guide to the Network Economy*, Harvard Business Press, Boston, MA.

Thaler, R. H. and C. R. Sunstein (2009), *Nudge: Improving decisions about health, wealth, and happiness*, 24 February, Penguin Books.

World Economic Forum [WEF] (2014), "Rethinking personal data: A new lens for strengthening trust", www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf, accessed 24 April 2015.


**From:**
# Data-Driven Innovation
## Big Data for Growth and Well-Being

**Access the complete publication at:**
https://doi.org/10.1787/9789264229358-en

**Please cite this chapter as:**

OECD (2015), "Building trust for data-driven innovation", in *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris.

DOI: https://doi.org/10.1787/9789264229358-9-en