Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development

20-May-2014

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE ON DIGITAL ECONOMY POLICY

DSTI/ICCP/REG(2014)3
Unclassified

Working Party on Security and Privacy in the Digital Economy

SUMMARY OF THE OECD PRIVACY EXPERT ROUNDTABLE

Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking

21 March 2014

JT03357584

English - Or. English

NOTE BY THE SECRETARIAT

This document provides a summary report on an informal Roundtable discussion that brought together a wide-cross section of privacy experts to the OECD on 21 March 2014. Participants exchanged views about how to apply or reshape current privacy frameworks within a data-driven economy. The Roundtable was organised in the context of ongoing OECD work on "*Data as a Source of Knowledge-Based Capital*" and in particular to inform the preparation of a report on trust in a data-driven economy.

The Roundtable was conducted under the "Chatham House Rule," so in this summary no viewpoints are attributed to any individual expert. Nor should the opinions and arguments reproduced in this summary be reported as representing the official views of the OECD or of its member countries.

The Roundtable agenda and document list are included as annexes. The summary has been prepared with the assistance of Brendan Van Alsenoy, working as a consultant to the Secretariat. It will be presented to the Working Party on Security and Privacy in the Digital Economy at its meeting on 18 June 2014.

SUMMARY OF THE OECD EXPERT ROUNDTABLE DISCUSSION

'PROTECTING PRIVACY IN A DATA-DRIVEN ECONOMY: TAKING STOCK OF CURRENT THINKING'

Introduction

On 21 March 2014, the OECD organised an Expert Roundtable entitled "*Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking*". The objective of this Roundtable was to discuss emerging challenges to the protection of privacy in light of the increasing use of data-intensive applications. To this end, a wide cross-section of privacy experts were invited to exchange views on possible innovative approaches to the protection of privacy and how the effectiveness of established approaches might be enhanced.

The Roundtable was attended by approximately 65 privacy experts from around the world. Participants included experts from governments, privacy enforcement authorities, academics, business and the Internet technical community. The experts participated in their individual capacity, rather than as representatives of the viewpoints of their organisation.

The Roundtable was organised in the context of an ongoing OECD project entitled "*Data as a Source of Knowledge-Based Capital*".[1] This project aims to study how the collection, analysis and use of increasingly large streams of digital data can generate productivity gains, boost innovation and improve efficiency, particularly in areas such as health care, science and public service delivery. In addition, this project also aims analyse policy implications in areas such as privacy and consumer protection, skills development, employment and competition.

Starting points for the Roundtable were the recently revised OECD Privacy Guidelines[2], as well as the Report of the Privacy Expert Group on the review of the Guidelines.[3] The latter document had highlighted a number of issues for possible further study and the Roundtable provided a forum to further explore some of these issues.

The Roundtable agenda (Annex 1) consisted of four sessions: (1) personal data taxonomies and governance; (2) the implementation of privacy risk management; (3) the implementation of access rights; and (4) the basic principles of national application in the OECD Privacy Guidelines. The first and last session were intended to explore possible innovative approaches to the protection of privacy and data protection. The middle two sessions invited participants to reflect on how established approaches might be enhanced or improved to work more effectively in the context of a data-driven economy.

This paper offers a discussion summary of the Roundtable. It does not attempt to offer a comprehensive account, but rather to extract of number of key points and themes from the Roundtable. The

---

1 For more information see OECD (2013), *Supporting Investment in Knowledge Capital, Growth and Innovation*, OECD Publishing. http://dx.doi.org/10.1787/9789264193307-en.

2 OECD (2013), *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 23 September 1980 - C(80)58/FINAL. Amended on 11 July 2013 - C(2013)79, accessible at http://webnet.oecd.org/oecdacts. See also OECD (2013), *The OECD Privacy Framework*, OECD Publishing. http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

3 OECD (2013), "Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines", *OECD Digital Economy Papers*, No. 229, OECD Publishing. http://dx.doi.org/10.1787/5k3xz5zmj2mx-en.

discussion was conducted under the "Chatham House Rule," so no viewpoints are attributed to any individual participant in this summary. In preparation for the Roundtable, six background documents were circulated as a basis for discussion. These documents are noted in the Documents List (Annex 2) and in places the discussion summary below has been supplemented by points from those papers.

Session I. Personal data taxonomies and governance

The objective of the first session was to reflect upon the utility of *data categorisations* ("personal data taxonomies") as a means to promote good data governance. Paragraph 3(a) of the OECD Privacy Guidelines recognises that countries may provide for

> "*[…] the application of different protective measures to different categories of personal data, depending upon their nature and the context in which they are collected, stored, processed or disseminated*"

This paragraph signals that countries have some discretion in deciding which measures should be applied to which types of data.[4] Against this backdrop, the first session set out to consider the possible utility of new forms of data categorisation. Questions raised at the beginning of this session included:

- What are the key existing data categories?
- Should we consider new types of data categorisation?
- Can new data categorisations inform the implementation of privacy principles in a practical way?

Existing data categories

During the introductory remarks, it was pointed out that one can already find a number of data categorisations, both implicit and explicit in current privacy frameworks. For instance, data might be treated differently in light of

- the *sensitivity of the data* at issue (e.g., data concerning health, data revealing racial or ethnic origin, political opinions, genetic data, biometrics);
- the *subject* to whom the data refers (e.g., data relating to minors, employees, non-citizens);
- the *purposes* for which the data are being used (e.g., personal use, business use, law enforcement purposes, scientific purposes);
- the *context* in which the data are being processed (e.g., in the context of electronic communications, credit reporting, archival, social security administration);
- the *degree of identifiability* (e.g. "identifying", "de-identified", "anonymous", "pseudonymous"); and
- whether the data has been collected *directly or indirectly* (e.g., in relation to notice obligations).

4 OECD (1980), *Explanatory Memorandum to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, paragraph 45. OECD Publishing (2001), http://dx.doi.org/10.1787/9789264196391-en.

A taxonomy based on origin

After these introductory remarks, the Roundtable turned to consider a proposal for a new data taxonomy. Rather than categorising data according to its sensitivity or use model, this taxonomy categorises data according to the manner in which they originated. The proposed taxonomy makes a distinction between four main categories of data: (1) provided data; (2) observed data; (3) derived data; and (4) inferred data.

Provided data are data which originate from direct actions taken by an individual, whereby he or she is fully aware of the actions that lead to data origination. Examples include: data disclosed by individuals in the context of a loan application ("initiated data"), data created when buying a product with a credit card ("transactional data"), or data shared (actively) via an online social network ("posted data"). While the individuals concerned may be unaware of the implications of providing these data, the fact that these data are being created should be obvious – or at least intuitive.

Observed data are data which have been observed by others and recorded in a digital format. These data can be recorded either at the moment of their creation, or transmitted to a digital carrier after observation. Examples include: data originating from online cookies, data generated by sensors, and passively created observational data (e.g., data captured by CCTV cameras combined with facial recognition). While individuals may be made aware of the creation of observed data (e.g., due to active engagement), much of the creation of observed data may go unnoticed.

Derived data are data generated from other data, after which they become new data elements related to a particular individual. Derived data are said to be created in a fairly "mechanical" fashion using simple reasoning and basic mathematics to detect patterns within a data set and create classifications. While these classifications may later be used for predictive purposes, they are not themselves based on probabilistic reasoning. Examples include: computational data (e.g. a calculation of customer profitability based on the ratio between number of visits and the items bought) and notational data (e.g. the detection of common attributes among "profitable" customers which are then used to classify potential customers).

Inferred data are the product of probability-based analytic processes. They are a result of the detection of correlations which are used to create predictions of behaviour. These predictions are then used to categorise individuals. Examples of include: statistical data (e.g., credit risk scores, life expectancy scores) and advanced analytical data (e.g., likelihood of future health outcomes based on an analysis of large and diverse medical data sets). Typically, the individuals to whom these data relate are not involved in their creation and may remain unaware of any inferences made.

From a historical perspective, it was pointed out that most of the data categories noted above have been in existence for a long time. "Inferred data", however, was said to have more recent origins, situated in the early 1980s (when companies first began to develop credit risk scores). There has, however, been a remarkable increase in both the volume and variety of available data sets.[5] In particular, there has been substantial growth in the amount of "observed", "derived" and "inferred" data. This development has been attributed to a number of factors. One is the continuous decrease in data storage and communication costs. A second is the Internet, which has led to a significant expansion in the types and amount of data being created since the mid-1990s. Finally, a third important development has been the proliferation, particularly

[5] See also OECD (2011), "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", *OECD Digital Economy Papers*, No. 176, OECD Publishing. http://dx.doi.org/10.1787/5kgf09z90c31-en and OECD (2013), "Exploring Data-Driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by "Big Data"", *OECD Digital Economy Papers*, No. 222, OECD Publishing. http://dx.doi.org/10.1787/5k47zw3fcp43-en.

in the 21st century, of new sensor technologies, which allow for detailed observations in both physical and digital environments.

Policy implications

It was argued that the developments described in the previous paragraph challenge traditional models of privacy protection. Specifically, it was asserted that the OECD Privacy Guidelines reflect a presumption that data are being collected primarily from the individuals concerned, with some degree of involvement or awareness. In other words, the argument was made that the Guidelines were developed primarily with "provided data" in mind, which may pose challenges where data are increasingly created "at a distance" from the individual (i.e., without the individual's involvement or awareness).

It was also noted that the basic values underlying the OECD Privacy Guidelines, lawfulness and fairness for example, remain crucial no matter how data originates. Other principles, such as openness, accountability and security may require greater emphasis. The principle of individual participation principle was highlighted as being particularly challenged, therefore necessitating greater consideration as to how to ensure its effectiveness in practice – a topic discussed in the third session.

Discussion

Participants first considered the use of different data categories within the *credit industry*. It was observed that many credit processes (e.g., a loan application) involve not only "provided" and "derived" data, but also "inferred data". While policymakers can learn from the experience acquired in this sector, it was argued that there is also a need to look across sectors. More general reflections might then be supplemented by additional measures at the level of individual sectors (e.g., in the form of codes of conduct) in order to address specific risks.

The discussion then turned to the *question of practical utility* of the proposed taxonomy. One participant asked whether the proposed classification would not introduce unnecessary complexity, underlining that the potential harm to individuals is determined by the use of the data rather than its origins. Others pointed out that the taxonomy could benefit education and awareness raising efforts, particularly within organisations. By illustrating the complexity of data sets and data usage, the taxonomy could also help shed light on issues of practical implementation (e.g., how might a right to correction be exercised in relation to "inferred data"?). Finally, the taxonomy was also viewed as helpful for policymakers and regulators, in particular when identifying areas requiring greater scrutiny and accountability.

A third discussion topic focused on the *principle of data quality*. Participants generally agreed that "derived" and "inferred" data are only as good as the processes which create these data. A first area of concern was therefore the quality of the underlying data sets ("garbage in, garbage out"). Participants then reflected upon the probabilistic nature of inferred data. Use of probabilistic reasoning may be considered inappropriate in contexts where the likelihood of adverse impact was high (e.g., in a law enforcement context). Considerations of fairness and equality were also highlighted as being particularly important (e.g., a very high probability ratio might still lead to an unfair outcome). Finally, one participant also noted that traditional mechanisms for individual participation (such as the right to access and correction) may not be sufficient in relation to "derived" and "inferred" data, even in situations where individuals are made aware of their impact.

Other points raised during the discussion include:

- the importance of focusing on *outcome* and potential *impact* on individuals;

- the importance of providing *clear and simple guidance* to practitioners;
- the need for increased *transparency to individuals*, particularly in relation to inferred data;
- the need for stronger *mechanisms to object* to inappropriate use, in particular with respect to uses of inferred data;
- the importance of *functional separation* between, on the on hand, processes aimed at creating insights and, on the other hand, processes which apply acquired insights; and
- the need to look at *discriminatory effects in practice*, rather than focusing (only) on the overt use of restricted ("sensitive") categories of data.

Session II. Implementing Privacy Risk Management

The revised OECD Privacy Guidelines introduced "risk management" as a key theme across the Guidelines. One of the areas where "risk" was given particular attention was in the context of privacy management programmes. Paragraph 15(a)(iii) stipulates that a data controller should have in place a privacy management programme that "provides for appropriate safeguards based on privacy risk assessment."

To date, the concept of risk management has not yet been widely applied in the privacy context. Against this background, the second session set out to consider various aspects of privacy risk management, including the role of technical measures. Questions raised at the beginning of this session included:

- How should organisations assess the relevant risks, which may be subjective?
- How can organisations assess the severity and likelihood of impact?
- What are promising approaches and methodologies for risk management?
- How can technical tools help reduce privacy risks?
- What challenges does risk management raise for privacy enforcement authorities with oversight responsibilities?

A risk-based approach to privacy

The second session began by recalling the main rationale for the use of "risk-based approaches" in the area of privacy and data protection. Two motivating factors were identified, namely the desire to *simplify* privacy and data protection regulations and to make these regulations *more effective* in practice. Several potential benefits of a risk-based approach were highlighted as well. For instance, the adoption of a risk-based approach was viewed as having the potential to:

- stimulate organisations to *assess the impact* of their activities upon *individuals and society*;
- assist both data controllers and privacy enforcement authorities in *priority setting*;
- promote *global interoperability*, provided a common approach can be identified; and

- leverage *insights gained in other areas* where risk management methodologies have been established for a longer period of time (e.g., security, environment, food safety).

A risk matrix

Having set forth these preliminary observations, the Roundtable then explored the possibility of using a matrix as a tool to identify and classify risks. A risk matrix was presented, which combined the following two elements:

- potential threats arising out of the handling of personal information taking into account the full lifecycle of information; and

- negative impacts, which might occur if the threat were realised.

Examples of potential threats included: unanticipated usage of information, use of inaccurate or outdated information, unusual use beyond societal norms, or disclosure to unauthorized entities. Potential negative impacts could include *tangible damage*, such as bodily harm, loss of liberty, damage and to earning power. Other types of impact include *intangible distress*, with examples such as detriment from monitoring, exposure of identity, the chilling of free speech, reputational harms, intrusion into private life and discrimination or stigmatisation. A third category includes *societal impact*, such as damage to democratic institutions or loss of social trust.

The objective of the proposed risk matrix is to line up threats and impacts against each other. For each intersection (between threat and impact), the user of the matrix is invited to consider two factors: *likelihood* and *severity*. By combining these two factors, the proposed matrix mainly aims to facilitate *prioritisation*: in areas of threat with a high likelihood of significant negative impact, additional safeguards and/or greater scrutiny are likely to be necessary.

Potential use cases

It was suggested that the risk matrix might be useful to a number of stakeholders. For data controllers, the matrix could provide a framework which helps them to identify issues and to prioritise allocation of resources. The matrix could also help regulators to set priorities, this time in terms of oversight and enforcement. In addition, the matrix might also assist them in the determination of appropriate sanctions and remedies. Finally, the matrix might also be useful for policymakers, when contemplating areas where further regulatory intervention might be necessary.

Open issues

While the potential of risk-based approaches was widely accepted, it was also recognised that further clarification was necessary in a number of areas, such as *scope*. Should risk assessments only focus on risks to privacy? Or should one also consider the potential impact on other fundamental rights and freedoms? And which assessments should be made by data controllers and which assessments should be made by lawmakers? To what extent can (or should) private entities be asked to evaluate societal risks?

Another key area of work regards the *criteria* for risk assessment. Should they be subjective or objective? Should a distinction be made between actual and potential harm? How can one balance the interests of commercial or governmental entities with the interests of the individual? Similarly, questions exist regarding classification. What is an appropriate method of risk classification? Should one distinguish between risks for individuals and risks for companies? A final area highlighted is the *role* of risk assessment. Once the assessment has been made, how should one deal with its results? Should risk

assessment lead to modulation of the basic principles? Or is it only the implementation of these principles which should be modulated? Before discussing these questions, the Roundtable turned to consider the role of privacy enhancing technologies in mitigating privacy risks.

Privacy Enhancing Technologies (PETs)

It was pointed out as a preliminary matter that engineers of PETs conceptualise risk in a distinctive manner. An implicit design assumption of many PETs is that the mere disclosure of personal data creates a risk. As a result, these PETs are designed to *reduce risk by minimising disclosure*, rather than to mitigate risks related to data handling.

PETs can strive for data minimization in different ways. For instance, many PETs seek to curb "default" data disclosures. These PETs are designed to prevent any disclosure of data which is not strictly necessary to provide the envisaged functionality. Very often, these PETs do not attempt to minimize disclosures by individuals, but instead focus on inadvertent disclosures (i.e., disclosures which otherwise occur simply because the system operates in a certain way). In other words: these PETs do not aim to reduce the amount of "provided" data, but rather the amount of "observed" data.

Other PETs do not focus on data minimization, but rather on *obfuscation*. The goal of these PETs is to introduce "noise" into the system, with the aim of disrupting the integrity and reliability of data collection (particularly of "observed", "derived" or "inferred" data). While acknowledging that the legitimacy or desirability of such "protest" technologies may be questioned, it was also pointed out that such tools are very often a "weapon of the weak": individuals may have little other options to counter or disrupt the continuous surveillance of their activities.

The Roundtable then considered *three design principles* for PETs, which might also be taken into account when assessing the risks of a particular technological design. These design principles were:

- Eliminate single points of failure. Privacy should not depend on a single "trusted party" behaving correctly. Instead, trust should be distributed so that multiple components/entities need to be compromised before a breach can occur.

- Minimise default information disclosure. Minimising the amount of information available automatically reduces any risk relating to potential compromise of this information. Data which is not strictly necessary to the proper functioning of the system should not be disclosed or collected. Certain PETs can help minimise disclosure beyond collection limitation (e.g., the use of certain cryptographic techniques can allow inputs to be taken into account without actually revealing those inputs).

- Ensure transparency and community-based review. Algorithms, protocols, designs and implementations should be open for review. This is particularly the case if individuals are expected to trust a particular technology. Some form of "open audit" can enable verification that the technology in fact has all claimed properties.

The presentation of these principles was followed by a discussion of policy implications related to PETs. It was pointed out that different policy responses may be appropriate depending on the technology and context in question. For example, it might be appropriate to incentivise (or even mandate) the use of PETs in situations where these technologies need to be implemented by the service providers themselves. For other PETs, it might be sufficient that they are "tolerated" and that policy makers refrain from adopting measures that limit an individual's ability to make use of such PETs (e.g. email encryption tools).

Discussion

The discussion began with participants reflecting upon the *scope* of risk assessment processes. It was argued that risk assessments should take into account not only privacy, but also other societal values (e.g., freedom of speech). Others pointed out that risk assessment processes should not be limited to compliance aspects. While compliance may be an important aspect, risk assessment tools should involve a much broader assessment of the impact of an organisation's activities. Finally, it was also argued that risk assessment methodologies should not only factor risks, but also benefits to individuals, groups of individuals or society as a whole.

The Roundtable then considered the *nature* of risk assessment criteria. Several participants stressed the need to approach risk management objectively. In addition, the importance of context was also emphasized: a risk assessment should incorporate factors such as nature, volume, type and usage of data. Finally, it was also suggested that more efforts should be made to improve the evidence base for risk assessments (e.g., through surveys). However, it was also recognised that much will remain dependent on practical judgement and common sense.

A third discussion topic concerned the *transparency* of risk assessment procedures. While recognizing the potential benefits of transparency, one participant argued that not every impact assessment should be made transparent towards individuals or regulators. Rather, the appropriate level of transparency should also be the outcome of a prior risk analysis. Another participant argued that greater public involvement in risk assessment processes would be beneficial. Specifically, it was argued that public disclosure may be necessary in order to bring in the right level of scrutiny. There was also consideration of the appropriate degree of *transparency of algorithms*. Several participants considered that disclosure of algorithms may not be appropriate (either due to proprietary interests or risks of "gaming"). At the same time, it was also recognised that more could be done to increase the transparency of algorithmic effects.

A fourth element of discussion focused on the *role* of risk assessment tools. It was underlined that risk-based approaches should not detract from established data protection principles. Instead, risk assessment tools should serve as vehicles to elaborate these principles in a more practical way. For example, the development of risk assessment methodologies could help inform non-privacy experts of the implications of their activities towards fundamental human rights. By identifying concrete objectives, it was hoped that this approach would further promote the adoption of appropriate safeguards.

Other points raised during the discussion included:

- the need for greater *legal certainty* (e.g., by formally identifying which type of processing operations are considered "risky by nature");
- the need for *simplicity* and *scalability,* so that organisations of all sizes can evaluate risks;
- the need to appropriately *allocate responsibilities* for risk assessment (e.g., between "data controllers" and "processors");
- the importance of *education and awareness raising* to promote implementation of risk management tools; and
- the need for practical guidance towards SMEs, application developers and engineers.

Session III. Implementing Access Rights

The OECD Privacy Guidelines consider "individual participation" an essential privacy protection safeguard.[6] Paragraph 13 stipulates that individuals should have the right (a) to obtain confirmation of whether or not a data controller has data relating to them; and (b) to see these data erased, rectified, completed or amended, as appropriate.

While the importance of individual participation is widely recognized, its practical implementation is fraught with difficulties. The objective of the third session was to reflect upon the main challenges to effective individual participation and to discuss how they might be overcome. Questions raised at the beginning of this session included:

- How can individual participation be improved, particularly in contexts where the use of personal data has a strong impact (e.g. in credit, housing, employment, finances, and insurance)?
- Which measures can help individuals understand what data an organisation has about them?
- Does the increased use of "observed" and "inferred" data raise new access challenges?
- What are the benefits and risks of allowing consumers to access to their own data in a portable format? What are the business incentives?

Importance

In order to highlight the importance of transparency and individual participation reference was made to the increased proliferation of consumer profiles. In the United States, for instance, data brokers continuously gather, derive and infer various types of information about consumers. On the basis of this information, consumers are associated with one or more profiles or "consumer segments," which may have names like: "*Rural and Barely Making It*", "*Ethnic Second-City Strugglers*", "*Credit Crunched: City Families*." These profiles can be used for a variety of purposes, some of which might be beneficial to the individuals concerned. However, there is also a risk that these profiles are used in a harmful manner (e.g., by targeting financially vulnerable consumers with "risky" credit products; or by discriminating unfairly against certain segments of the population). Without an appropriate level of transparency, the risk of inappropriate use is likely to be greater. Moreover, individuals may remain unaware of these practices or not know how to take action.

Potential benefits

It was pointed out that transparency can act as a safeguard in two ways. First, transparency can provide individuals with a *better understanding* of which types of data are being collected (or generated) by which entities. It can also provide them with a better understanding of how they might deal with these data. Second, transparency enables *scrutiny* ("sunlight is the best disinfectant"). Through transparency, not only the individuals concerned, but also society at large (e.g., investigative journalists, academics, policy makers) can scrutinize how data are being used. This in turn enables a collective understanding about data usage, as well as a collective judgment regarding the propriety of those uses.

6 See OECD (1980), *Explanatory Memorandum to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, paragraph 58.

Challenges and opportunities

Having recalled the importance and potential benefits of transparency, the Roundtable then turned to consider some of the challenges towards effective individual participation. A first challenge is that an increasing number of companies which collect and generate personal data are *not consumer-facing* (e.g., data analytics companies, data brokers). While recognising that certain industry players have taken "a first good step" towards increasing transparency, it was argued that a more comprehensive approach is needed. Returning to the example of the data broker industry, the argument was made that consumers should have access to a *single portal* (a "one-stop shop") which informs consumers of who the data brokers are, what data they keep about them, and from where these data originate. In addition, this portal should also inform consumers of how they might control the these data (e.g. requests for deletion or correction).

A second identified challenge concerned the *complexity* of data processing. Increasing amounts of data are not collected from the individuals concerned, but are instead observed, derived or inferred. Very often, the technical and analytical processes underlying these data uses are quite complex. How can these practices be communicated to individuals in an intelligible way? How detailed should the information be? In this respect it was argued that *visualisation tools* can be particularly helpful in explaining complex processes to lay people. It was also noted that it may be sufficient, in certain contexts, to explain how the data is being applied (its "impact"), without going into technical details. An example from the credit industry was cited, whereby consumers where shown through a "slider" how their credit score might be impacted based on certain information (e.g. taking out of a loan).

A third set of challenges involved the *accommodation* of access rights. Properly responding to an access request can be difficult in contexts where data is either poorly indexed or heavily "siloed". While separation of data may actually be beneficial to an individual's privacy, it may also complicate transparency. The absence of direct identifiability presents similar issues. Increasingly, individuals are not identified directly (e.g., by way of unique identifier such as an account number), but indirectly (e.g. through one or more attributes). As a result, it is not necessary for data to be "about" a particular individual for it to affect that individual. This means that individuals might experience the effects of a particular data use (e.g., inference) without being directly identified. It was suggested that creating transparency of those practices may require measures which operate independently of the "identity" of the individuals concerned.

A fourth identified challenge concerned the *burden for individuals*. Very often, disclosure of personal data by individuals is made very easy (e.g., data can be provided through an online form). However, exercising access rights or seeking correction of these data can be burdensome (e.g., a posted letter is required). Many organisations lack sufficient incentives to make it as convenient to disengage as it is to enrol. More efforts may therefore be needed to persuade organisations to lessen the administrative burden for individuals who wish to exercise their access rights.

Discussion

During the discussion, it was noted that consumers often experience difficulties when exercising their rights of access. In fact, a substantial portion of the *complaints* received by the UK Information Commissioner's Office concerns access requests. This suggests a need to increase efforts to make sure data controllers respond adequately to these requests. One participant suggested that it might be useful to further develop the evidence base regarding consumer experiences. Another participant cautioned, however, that such figures might be misleading (e.g. many individuals might simply be unaware of their rights or even of the existence of a formal complaint mechanism).

Several participants emphasized the need for transparency to be *meaningful*. Data controllers should not limit themselves to revealing the data they hold, but should also inform individuals of how these data

are being used and in which context. In addition, individuals should also be informed of how they can act upon the information presented. In other words: transparency and education should go hand in hand. Several participants also cautioned that providing too much transparency at once can be overwhelming. Data controllers should therefore take additional care to present information in an understandable way, particularly in situations where large amounts of information are at issue.

It was also noted that the appropriate *degree of transparency* may vary depending on the context. For example, one participant argued that access to "raw data" is mainly useful in the context of a dispute or investigation. Therefore, data controllers should not provide such data on a continuous basis, as the provisioning of such information might overwhelm both consumers and regulators. Furthermore, it was argued that the use of data needs to be considered in context. Access to raw data by itself may result in a skewed perspective if viewed in isolation. Other participants argued that greater transparency of data processing practices would be beneficial.

One participant suggested that more thought should be put into the development of c*ollective transparency mechanisms*. In other words, future transparency efforts should perhaps focus less on increasing involvement by individuals, but rather on the development of mechanisms that enable scrutiny by the community at large.

On several occasions, reference was also made to the use of *technological tools* to increase transparency. One participant highlighted the availability of web "plug-ins" that aim to enhance transparency towards Internet users (e.g., with regard to the placement of so-called "tracking cookies" by third parties). Another participant suggested that data controllers might put in place an Application Programming Interface (API) which allows consumers to obtain access to their data in real-time. It was also recognized, however, that providing a user interface which provides individuals with access to their data in a meaningful way can be difficult, particularly if one also wishes to offer them means to exercise control over these data.

Other points raised during the discussion included:

- the need to improve transparency of data uses *across the value chain* (e.g., not to limit oneself to large consumer-facing companies);
- the need to appropriately *allocate responsibilities* for individual participation (e.g., between "front-end" and "back-end" companies);
- the importance of ensuring openness and individual participation *at the moment of "impact"* (e.g., when a consumer is confronted with an unfavourable decision); and
- the importance of *not conflating* transparency and individual participation.

IV. Back to Basics: Revisiting the Basic Principles of the OECD Privacy Guidelines

The revised OECD Privacy Guidelines left intact the basic principles of national application as defined in 1980 (i.e., collection limitation, data quality, purpose specification, etc.). The Expert Group, which had helped prepare the 2013 revisions, had discussed several issues relating to these principles. The Report of the Expert Group documented these issues as topics "for possible further study and discussion".[7]

[7] See OECD (2013), "Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines", *OECD Digital Economy Papers*, No. 229, OECD Publishing. http://dx.doi.org/10.1787/5k3xz5zmj2mx-en.

Identified topics included: (1) the role of consent; (2) the role of the individual; (3) the role of purpose specification and use limitation; and (4) the definition of personal data.

Many of the questions raised by the Report of the Expert Group are currently being considered in initiatives outside the OECD context. The objective of the fourth session was to take stock of some of those efforts and to consider whether they could aid policymakers and practitioners in protecting privacy in the context of a data-driven economy.

Prevalent critiques

The fourth session began by introducing some of the prevalent critiques concerning the basic principles of national application. It was noted that several commentators have begun to question the continued relevance of "traditional" approaches to privacy. A "traditional" approach, in this context, refers to privacy instruments based on fair information principles as articulated in the OECD Guidelines.

The critique of the "traditional" approach starts from several assumptions. One is that this approach places a strong emphasis on purpose specification and consent ("notice and choice"). Another is that it seeks to limit the collection and use of personal data. And finally that it draws a rigid distinction between "personal" and "non-personal" data. On the basis of these premises, a number of challenges have been offered:

- requiring prior specification of all purposes is difficult and can be socially undesirable (as it can be difficult to predict future uses, which may be of benefit to society);
- obtaining meaningful consent is increasingly challenging (in light of cognitive biases and the finding that individuals often have no choice other than to simply "take or leave it");
- a focus on collection is misplaced in an era where personal data is increasingly "inferred" rather than "collected"; and
- the principles of data minimisation and collection limitation are inimical to the use of "Big Data", which seeks to detect new patterns and correlations free from limitations.

Use model

It was pointed out that several commentators have called for a "use model" as an alternative construct to the traditional approach. Such a model would shift the focus away from the initial collection of data, to focus instead on how these data are used ("*focus on use, not collection*"). One rationale given for this approach is that it is the use (rather than the collection) of data which provides benefits or causes harms. Although there are variations in the how the "use model" is articulated, common elements include:

- *Greater flexibility and accountability*. The use model is explicitly intended to provide organisations with greater freedom to decide about data usage. The apparent trade-off would be an increased emphasis on accountability and "data stewardship".
- *Increased emphasis on risk*. The use model places a very strong emphasis on risk. It is based on the underlying assumption is that there will be some entity assessing the risks and the benefits and then decide whether or not the use is acceptable.
- *Increased emphasis on context.* The use model also places strong emphasis on "context" in assessing the ethical use of information.

- *Decreased emphasis on personal data.* In principle, the use model can be applied regardless of whether or not data are "personal" or not. The potential impact on individuals is what counts.

Responses to the Use Model

As a preliminary matter, it was noted that much of the criticism directed at the traditional approach seems to be directed at the "notice and choice" model. While acknowledging that this model is central to several national privacy frameworks, it was also pointed out that the model does not figure as strongly in others. For example, in the EU, consent is only one of six legal bases for processing.

It was questioned whether the use model actually provides a better alternative to the traditional approach. Even if one were to accept the criticisms of the "traditional" approach, it is not entirely clear whether the use model would actually remedy these issues. For example, it remains unclear how the use model would overcome the identified challenges to transparency and individual participation. If it is not possible or desirable to specify purposes in advance, how can individuals challenge the usage of their data or exercise their rights? How is any assessment or scrutiny regarding the propriety of data usage possible? In this context, reference was made to what one author has referred to as the "transparency paradox": while the use of so-called "Big Data" and analytics enables greater insights about individuals, the machinery behind it is anything but transparent.

A number of questions were also raised in relation to the increased emphasis on risk. The use model suggests that organisations should assess risks and then balance potential harms and benefits. This approach would present additional challenges for regulatory oversight and enforcement. For example, are regulators able to evaluate whether the social or economic benefits of a particular use outweigh the risks to the individuals involved? Would an increased emphasis on risk assessment not exacerbate national and regional differences? If assessments are driven by cultural and social norms, would the risk of fragmentation not become greater?

Before discussing these questions, the Roundtable turned to consider how some of these issues are currently being perceived at national level, in particular in Japan.

Experience at national level

On December 20th, 2013, the Japanese Cabinet Secretariat decided to amend Japanese Privacy Act of 2003. It was noted that these amendments intend to implement the revised OECD Privacy Guidelines. It was also pointed out that much of the topics debated in Japan are similar to those debated during the Roundtable discussion.

A first topic of discussion concerns *risks of re-identification*. A proposal was made to formally recognise certain categories of data as posing diminished risks (e.g., "pseudonymised" and "anonymised" data). However, this proposal was abandoned in light of the finding that it may be too difficult to draw clear distinctions, in particular between "identifiable" and "non-identifiable" data. Furthermore, several experts found that complete anonymisation of data is impossible. While data may be successfully anonymized today, there is no guarantee that it will remain anonymous in the future.

Another topic relates to the *risk-based approach*, which is generally viewed as promising. In Japan, there is already some experience with conducting risk assessments, given the mandatory obligation to conduct a privacy impact assessment (PIA) in the context of the national ID number system. It was noted that Japanese experts have benefited from the French, Canadian, US and UK practices.

A third dimension of the Japanese reforms concerns *data subject rights*. Here the main question is how implement the principles of openness and individual participation in practice. Many Japanese companies provide very detailed privacy notices to consumers, which may be too time-consuming to read. The focus is therefore on simplification and the reduction of overly lengthy notices.

Other topics include the *economic value of personal data*, particularly in the context of consumer remedies. Here the question is how courts can assess the appropriate compensation for individuals if their data are compromised. Likewise *enforcement mechanisms* have been discussed. Until recently, there was no independent privacy enforcement authority in Japan. While the decision to introduce this institution has already been made, the question of how to ensure effective enforcement still remains the topic of some debate. It was noted that cultural values play a very important role in determining the effectiveness of oversight mechanisms.

In conclusion, it was noted that there is a need to *bridge the gaps* between privacy rights and privacy governance; between lawyers and engineers; and between Western and Eastern cultures.

Proposals for change

The Roundtable then turned to consider a specific set of proposals for revising the basic principles of the OECD Guidelines. Before introducing these proposals, a number of preliminary observations were made concerning technological and social changes since the initial enactment of the Guidelines. A first identified change concerned the *role of consumers*. Many consumers now volunteer much more data about themselves than in the past. Quite often, the data being revealed or generated are of a far more personal nature than could be reasonably anticipated in 1980. Likewise the overall *amount of data* being collected and created has increased. As sensors have become ubiquitously present (e.g., video cameras, audio recording devices), there has been a dramatic increase in both the collection and creation of data. Moreover, increasing amounts of data are being created through inference. A final factor identified was *increased surveillance capabilities* and pressure from governments on the private sector to collect and store certain types of data.

Having set forth these preliminary observations, and recalling the above critique of the traditional approach, some proposals for change were put forward:

- *A shift from "collection" to "use"*: In order to increase the focus on use, the principle of collection limitation would be limited to a narrower set of practices (e.g., personal data should not be collected in violation of legal restrictions, through deception, or in a ways that are not apparent or reasonably discernable or anticipated by individuals).

- *A broad notion of "use"*: In the proposed revisions, "use" is defined broadly as "relying on or consulting personal data for decision-making or other assessment concerning an individual, using personal data to create or infer other personal data, or disclosing or disseminating personal data to a third party." It was pointed out that this definition encompasses virtually any operation which can be performed upon personal data, other than its collection, storage, or destruction.

- *A broad notion of "personal data"*: The proposed revisions define personal data as "any information that identifies an individual, could reasonably be used to identify an individual, or is linked to data identifying an individual and used in any manner affecting that individual." This proposal seeks to alleviate the uncertainties regarding the "personal" or "non-personal" nature of data by emphasising how the data are being used. In other words, even if the data are not "personal", if they link to or affect an individual, they would still be covered.

- Use principles: The permissibility of data uses should be determined in light of the risks presented. Routine data uses which do not present a high risk would be permitted under broad terms, which regulators would help to define. Data usages which present a reasonable likelihood of significant harm, would in principle be prohibited and individuals would not be able to validly consent to these uses. Data usage which presents moderate risks would be contingent upon the results of a risk management process. This process would be undertaken in accordance with a framework identified by national regulatory authorities. It would also provide documented evidence of the assessments made and an overview of tools adopted to mitigate risks.

- Individual choice: The proposed revisions envisage that individual choice should only be required if meaningful and, if required, should be (i) clear, (ii) provide real choice; and (iii) be accompanied by relevant, understandable information about the choice and its consequences. This proposal aims to prevent reliance upon consent in situations where individuals have no real choice but to consent if they wish to obtain a particular service.

- Accountability and enforcement: The proposed revisions would put emphasis on the accountability and obligations of data stewards and establish liability for reasonably foreseeable harm. Governments would create and properly finance privacy enforcement authorities.

In conclusion, it was reiterated that the proposed revisions were merely intended to stimulate further discussion. It was also argued, however, that the proposed revisions would be a step forward, as opposed to leaving the basic principles intact. In particular, the argument was made that the revised principles are both more intuitive and more consistent with the way practitioners currently approach data protection. It was also reiterated that the revised principles would reduce the burden on individuals; shifting the burden back to the responsible organisations. They also envisage a substantial role for national regulators, who would be called upon to lead a multi-stakeholder dialogue and develop methodologies for dealing with risks.

Discussion

A vigorous discussion ensued, in which both the need for changes to the principles and the proposals themselves were contested. One focus was the proposed distinction between *"collection" and "use"*. One participant argued that the distinction (as presented) fails to take into account that the mere collection and storage of data also creates privacy risks. Moreover, it was argued that this approach would run afoul of the principles of "data minimisation" and "privacy by design". Application of these principles implies limiting the collection of personal data as a way to reduce risks. As a result, it was argued that collection and use cannot be separated in the manner suggested by the proposals.

Another participant observed that the basic principles as defined today, including the principle of "collection limitation", provide an analytical framework which can be reiterated throughout the information lifecycle. For example, the principles of collection limitation and data quality should be applied not only at the moment of initial collection, but also at the moment of every subsequent "collection" (when the data are used as input into another processing activity). While recognising that a greater emphasis on use might be more intuitive, it was argued that the current principles can be applied effectively to both collection and use.

A second discussion topic concerned the principle of *purpose specification*. It was argued that the concept of "purpose" is quite similar to the notion of "benefits". Specifying the purposes (or "benefits") of data processing was viewed as being instrumental to a proper evaluation of data usage. Without specification of purpose(s), it would be impossible to determine the appropriate balance between harms and benefits. It would also prevent any subsequent scrutiny as to whether the appropriate balance had been struck.

A third topic of discussion concerned the role of *privacy notices*. There was little disagreement with the proposition that overly lengthy and complex privacy notices do not lead to meaningful individual participation or valid consent. One participant observed that many of the issues concerning privacy notices pertain to the underlying incentive structure: quite often, the main incentive for the drafter of a privacy notice is to create a document which protects the organisation, rather than to inform individuals in a meaningful manner. Others cautioned that the role of privacy notices should not be reduced to a means of obtaining "informed" consent. Disclosure of data use practices was also deemed important to enable scrutiny by other stakeholders, such as regulators, civil society representatives and academics. Short "just-in-time" notices were put forward as useful tools for promoting individual awareness and control.

A fourth topic of discussion concerned the criticisms regarding the *role of consent*. It was argued that these criticisms overstate the intended role of consent under the OECD Guidelines and other instruments. It was therefore suggested that the issues reside primarily at the level of practical implementation, rather than at the level of the principles themselves. While agreeing with these observations, other participants emphasised that there are still many situations in which individuals can (and should) be given the opportunity to express valid consent (e.g., with regard to the use of location data). At the same time, there was also a recognition that overemphasis on consent may unduly inhibit societal benefits. Striking the appropriate balance and determining when reliance on consent is (not) "appropriate" was therefore identified as an important issue going forward.

Other points raised during the discussion included:

- the need to ensure *consistency of purposes* when personal data are processed by multiple entities;
- the importance of ensuring *data quality* as a means of risk mitigation;
- the need to consider *compatibilit*y, *context and risk* when assessing the legitimacy of data usage;
- the need for *enhanced accountability* when data usage is justified on the basis of the "legitimate interests" of the data controller; and
- the need to view risk management methodologies as *tools for implementing* the principles rather than as a vehicle to discount certain obligations.

ANNEX A

OECD Expert Roundtable Discussion

Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking

21 March 2014

AGENDA

The challenges of applying traditional privacy principles to contemporary data uses have become increasingly clear. Trends in data analytics and the advent of an Internet of Things will only exacerbate the difficulties in making these principles operate effectively. This expert roundtable will bring together a wide-cross section of privacy experts to exchange views about possible approaches that could be used to update or reshape privacy frameworks to more effectively address the privacy challenges, while at the same time enabling the promise of a data-driven economy. These themes are at the crux of current OECD work in this area, which is expected to produce a study on privacy and related trust issues raised by data and analytics by the end of 2014. The insights gleaned during the Roundtable should feed the preparation of that study, as well as informing the implementation of aspects of the newly revised OECD Privacy Guidelines.

Venue: OECD Conference Centre -- Room CC4. Directions and information about the venue is available at: www.oecd.org/conferencecentre. Advance registration is required and participants to should arrive to the conference centre by 9:00 with photo identification to obtain a visitor badge.

Participants: Invited experts and delegates from the OECD Working Party on Security and Privacy in the Digital Economy

Format: The discussion will be organised in roundtable format, with 2 or 3 experts asked to serve as discussion leaders to stimulate and moderate the discussion. Several of the discussion leaders will prepare short papers to be circulated in advance of the Roundtable. The goal is a broad and robust dialogue. Participants will be asked to respect the "Chatham House Rule" to ensure a frank and open discussion. Please note that there will be no interpretation available for this meeting, which will be conducted in English.

Morning Session

Welcome remarks (9:30 – 9:40)

I. Personal data taxonomies and governance (9:40 – 10:55)

***Discussion Leaders*:** **Martin Abrams**, The Information Accountability Foundation
David Smith, Information Commissioner's Office (United Kingdom)

***Session Objectives*:** A taxonomy of personal data might include three categories: volunteered, observed, and inferred. The first generation of privacy concepts developed during the 1970s contemplated an environment in which the bulk of personal data probably fell within the "volunteered" category, with the percentage of observed or inferred data being much smaller. Notwithstanding the tremendous growth of personal data being generated and volunteered by individuals themselves today, even greater growth is evident in the volume of observed and inferred data. Although harms to privacy and individual liberties may arise with respect to all of these categories of data, the appropriate governance structure and most effective and workable means to protect against those harms will vary. This session will explore that hypothesis.

Coffee break (10:55 - 11:15)

II. Implementing Privacy Risk Management (11:15 – 12:30)

Discussion Leaders: **Richard Thomas**, Centre for Information Policy Leadership
Claudia Diaz, KU Leuven
Florence Raynal, Commission Nationale de l'Informatique et des Libertés (France)

Session Objectives: The revised OECD Privacy Guidelines introduce risk management as a key theme across the Guidelines, and in particular in the context of developing privacy management programmes. However, the concept of risk management has not been widely applied in the privacy context. To be effective, the scope of any risk assessment must be both sufficiently broad to take into account the wide range of harms and benefits, and sufficiently simple to be applied routinely and consistently. How should organisations assess the relevant risks, which may be subjective? How can they assess the severity and likelihood of impact? The move to a risk assessment approach may also raise challenges for privacy enforcement authorities with oversight responsibilities. This session will consider approaches and methodologies for risk management, as well as the role of technical tools to reducing risk.

Lunch break (12:30 – 1400)

Afternoon Session

III. Implementing Access Rights (14:00 – 15:15)

Discussion Leaders: **Julie Brill**, Federal Trade Commission (United States)
Robin Wilton, Internet Society

Session Objectives: The rights to access and correction have been part of the OECD Guidelines since the start and are incorporated into national laws around the world. But the degree to which individuals actually exercise those rights is questionable. How can access be improved to the individual dossiers that inform decision-making in areas such as credit, housing, employment, finances, and insurance? Are there transparency measures and technical tools to enable individuals to better understand what data an organisation has about them? Does the growing importance of observed and inferred data raise new access challenges? What would be the benefits and risks of allowing consumers access to their own transaction and consumption patterns in a portable format and what are the incentives for businesses to do so? This session will consider new initiatives to improve individual access to their personal data.

Coffee break (15:15 – 15:35)

IV. Back to Basics: Revisiting the Basic Principles in the OECD Guidelines (15:35 – 16:50)

Discussion Leaders: **Carman Baggaley,** Office of the Privacy Commissioner (Canada)
Fred Cate, Indiana University School of Law
Hiroshi Miyashita, Chuo University

Session Objectives: The revised OECD Privacy Guidelines leave intact the original 1980 formulation of the basic principles of national application (collection limitation, data quality, purpose specification, etc.). The Report from the Expert Group highlights that while the group considered many issues that implicate these core principles and key definitions, no clear direction emerged as to what changes might be needed. The report goes on to identify some of the issues, which include the role of consent, the role of the individual, the roles of purpose specification and use limitation, and the definition of personal data. Many of the issues raised in the Expert Group report are being considered in work outside the OECD context. This session is an opportunity to take stock of those efforts and consider in particular whether they can offer aid in dealing with a data driven economy.

Closing Remarks (16:50 – 17:00)

ANNEX B

OECD Expert Roundtable Discussion

Protecting Privacy in a Data-Driven Economy:
Taking Stock of Current Thinking

Documentation

Background Documents

Martin Abrams, The Information Accountability Foundation, "The Origins of Personal Data and its Implications for Governance" [Background Paper A] http://informationaccountability.org/wp-content/uploads/Data-Origins-Abrams.pdf

Centre for Information Policy Leadership, "A Risk-based Approach to Privacy? An Initial Issues Paper for Privacy Risk Framework and Risk-Based Approach to Privacy Project" [Background Paper B] [draft paper - not yet publicly available].

Commission Nationale de l'Informatique et des Libertés (CNIL), "Methodology for Privacy Risk Management" [Background Paper C] http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf

Julie Brill, Commissioner, U.S. Federal Trade Commission, "Big Data and Consumer Privacy: Identifying Challenges, Finding Solutions" 20 February 2014 [Background Paper D] http://www.ftc.gov/system/files/documents/public_statements/202151/140220princetonbigdata_0.pdf

Carman Baggaley, Office of the Privacy Commissioner of Canada "Rethinking Data Protection in a World of Big Data: A Discussion Paper" [Background Paper E] [draft paper - not yet publicly available]

Fred H. Cate, Peter Cullen, and Viktor Mayer-Schönberger, "Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines" (March 2014) [Background Paper F]: http://www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf

Additional Documents

This section includes a number of documents that Roundtable participants suggested as additional material that would be useful for the discussion. It is only a very small sample of a large volume of valuable resources relevant to the issues considered at the Roundtable.

OECD Resources

Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013); Supplementary Explanatory Memorandum (2013): http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

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

"Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value", (2013): http://dx.doi.org/10.1787/5k486qtxldmq-en

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

Other Resources

Article 29 Data Protection Working Party and the Working Party on Police and Justice, "The Future of Privacy" (02356/09/EN, WP 168) (2009), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf

Article 29 Data Protection Working Party, "Opinion 03/2013 on purpose limitation"(00569/13/EN WP 203) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Diaz, Tene, and Gurses; "Hero or Villain: The Data Controller in Privacy Law and Technologies" (2013), https://www.cosic.esat.kuleuven.be/publications/article-2365.pdf

Kate Crawford, Jason Schultz, "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms", http://bclawreview.org/files/2014/01/03_crawford_schultz.pdf

Garante Per La Pretezione Dei Dati Personali, "Privacy: Working with Business – Ten Corporate Best Practices to Improve Your Business" (2013), http://www.garanteprivacy.it/documents/10160/2416443/Privacy%3A+working+with+business-vademecum.pdf

Neil M. Richards and Jonathan H. King, "Three Paradoxes of Big Data", http://www.stanfordlawreview.org/online/privacy-and-big-data/three-paradoxes-big-data (2013)

Obama Administration's White Paper, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy" (2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

Omer Tene and Jules Polonetsky, "Privacy in the Age of Big Data: A Time for Big Decisions", 64 Stanford Law Review (2012), http://www.stanfordlawreview.org/online/privacy-paradox/big-data

UK Information Commissioner's Office, "Anonymisation: Managing Data Protection Risk Code of Practice" (2012), http://www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation

US Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, FTC Report (2012), www.ftc.gov/os/2012/03/120326privacyreport.pdf

World Economic Forum, "Unlocking the Economic Value of Personal Data: Balancing Growth and Protection" (2012), available at: http://www3.weforum.org/docs/WEF_IT_UnlockingValueData_BalancingGrowthProtection_SessionSummary.pdf