DISCUSSION DRAFT 16 February 2016

# Protecting Privacy in a World of Big Data

# Paper 2

# The Role of Risk Management

Centre for Information Policy Leadership at Hunton & Williams LLP

*This is the second paper in a three-part series on offering practical solutions to Protecting Privacy in a World of Big Data. The first paper is on "The Role of Enhanced Accountability in Creating a Sustainable Data-driven Economy and Information Society" and the third paper, "Reinvigorating Privacy Principles", examines how to interpret and apply traditional privacy principles in the modern information age.*

## I. Summary

Risk management has long played an important role in data protection. Over the past three years, the Centre for Information Policy Leadership at Hunton & Williams LLP has hosted a series of multinational workshops and published two white papers on risk management and its role in effective modern data protection.[1]

In this paper we focus on the interaction of risk management with other data protection concepts and tools and the steps necessary to implement privacy risk management in the context of big data and analytics. It is increasingly apparent that in addition to legal norms, risk management is essential to protecting privacy effectively in a world of significant technological developments, including big data, ubiquitous surveillance, interconnected devices (i.e. the "Internet of Things"), exponential increases in storage capacity (and decreases in storage costs), computational capacity and pervasive networks.

For risk management to achieve its true potential, a collaborative effort by regulators, industry, civil society and academics is necessary to help develop a science of risk management with the following elements:

- a framework of privacy harms or other negative impacts;
- a framework for analysing benefits resulting from data processing;
- a shared vision of risk management as a tool for reducing and managing (rather than eliminating) risk or harm while preserving the potential benefit and weighing the residual risk or harm appropriately against the benefits to determine if it's acceptable;
- a shared collection of risk management best practices; and

[1] Centre for Information Policy Leadership at Hunton & Williams LLP, *A Risk-based Approach to Privacy: Improving Effectiveness in Practice* (2014); *see also* Centre for Information Policy Leadership at Hunton & Williams LLP, *The Role of Risk Management in Data Protection* (2014).

- a clear understanding of the role risk management plays in context with other modern data protection concepts and tools.

Those tools include legitimate interest processing, fair processing, transparency and a renewed focus on data use. Systematic risk management is critical to them all; none can be used effectively without it.

The development of risk management can serve another critical purpose as well: it can help bridge gaps that too often separate disparate data protection legal regimes. If we can work together across national boundaries to build consensus around a science of risk management, a framework of privacy harms, a collection of risk management best practices and other key steps, data protection may be not only relevant, but also effective, efficient and consistent with valuable data flows that routinely cross national boundaries.

## II. Risk Management as a Foundational Requirement of Data Protection

Data protection has long relied on risk management—the process of systematically identifying and managing harms and promoting or preserving the benefits that could result from an activity—as a tool for complying with legal requirements and ensuring that data are processed appropriately and that the fundamental rights and interests of individuals are protected.

Risk management is an explicit requirement of many data protection laws. For example, the 1988 US Computer Matching and Privacy Protection Act requires government agencies to perform a cost-benefit analysis of proposed data matching.[2] Security breach notification laws often link notice to an assessment of the risk to individuals posed by the data breach. As the Article 29 Data Protection Working Party has noted, for notification to be effective "it is important to have an appropriate risk management framework in place …"[3] And risk management is the goal of Privacy Impact Assessments, which are also increasingly required in data protection laws and regulatory guidance.[4]

Risk management in data protection is "not a new concept, since", as the Article 29 Working Party stressed in its 2014 *Statement on the role of a risk-based approach in data protection legal frameworks*, "it is already well known under the current Directive 95/46/EC."[5] However, there

[2] 5 USC § 552a(o).

[3] Article 29 Data Protection Working Party, *Opinion 03/2014 on Personal Data Breach Notification*, 693/14/EN WP 213 (2014), 4.

[4] *E.g. E-Government Act of 2002* (requiring PIAs for US federal government agencies); UK Information Commissioner's Office, *Conducting Privacy Impact Assessments Code of Practice*, 2014 (Guidance); New Zealand Privacy Commissioner, *Privacy Impact Assessment Toolkit*, 2015 (Guidance); Australia Guide to undertaking privacy impact assessments, 2014 (Guidance).

[5] Article 29 Data Protection Working Party, *Statement on the role of a risk-based approach in data protection legal frameworks*, 14/EN, WP218 (2014), 2. The EU Data Protection Directive 95/46/EC requires that security measures must "ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected" (Article 17); that "processing operations likely to present specific risks to the rights and freedoms of data subjects" be subject to "prior checking" by Member States (Article 12); that personal data may be processed when "necessary for the purposes of the legitimate interest pursued by the controller or by the third party or parties to whom data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subjects …" (Article 7(f)); and that access rights to

has been an unhelpful shift towards interpreting it as risk elimination rather than risk management.

In recent years, as we wrote in 2014, "risk management has started to take on a more prominent role in data protection as information technologies have advanced and proliferated and regulators and organisations have focused more attention on accountability for data processing."[6]

In 2013 the Council of Ministers of the Organisation for Economic Co-operation and Development (OECD) revised the *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, first adopted in 1980, to "implement a risk-based approach."[7] The drafters noted the "importance of risk assessment in the development of policies and safeguards to protect privacy."[8]

There have been a host of recent government reports on risk management in data protection. The French Commission Nationale de l'informatique et des Libertés (CNIL) led the way with its *Methodology for Privacy Risk Management*, revised most recently in 2012, which "describes *a method for managing the risks* that the processing of personal data can generate to individuals."[9] There the CNIL writes: "Using a risk management method is the safest way to ensure objectivity and relevance of the choices to make when setting up a processing of personal data."[10]

The US Federal Trade Commission (FTC) in 2012 published a report recommending that companies should "implement accountability mechanisms and conduct regular privacy risk assessments to ensure that privacy issues are addressed throughout an organization."[11]

The US National Institute of Standards and Technology (NIST) in 2014 issued a privacy risk model discussion draft to help organisations "assess the privacy impact on individuals whose information is collected, used, stored, and transmitted by information systems, and how organizations can prevent adverse impact on those individuals."[12] 2014 also saw publication of the Article 29 Working Party's *Statement on the role of a risk-based approach in data protection legal frameworks* in which it noted support for "the inclusion of a risk-based approach in the EU data protection legal framework."[13]

---

data processed for scientific research may be limited "where there is clearly no risk of breaching the privacy of the data subject" (Article 13(2)).

[6] *The Role of Risk Management in Data Protection*, at 7-8.

[7] Organisation for Economic Co-operation and Development, *Supplementary Explanatory Memorandum to the Revised Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (2013), 30.

[8] Organisation for Economic Co-operation and Development, *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, C(80)58/FINAL, as amended by C92013)79 (2013), 12.

[9] Commission Nationale de l'informatique et des Libertés, *Methodology for Privacy Risk Management* (2012), 4.

[10] Id., at 9.

[11] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* (2012), 30.

[12] National Institute of Standards and Technology, *NIST Privacy Engineering Objectives and Risk Model Discussion Draft* (2014), 3.

[13] Article 29 Data Protection Working Party, *Statement on the role of a risk-based approach in data protection legal frameworks*, 14/EN, WP218 (2014), 2.

The text of the agreed European Union General Data Protection Regulation focuses significantly on risk management. The regulation stresses the need for "the controller or processor" to "evaluate the risks inherent to the processing and implement measures to mitigate those risks"[14] and to determine "the likelihood and severity of the risk for the rights and freedoms of individuals."[15]

## III. The Data Explosion

Much of the growing focus on the role of risk management in data protection reflects dramatic changes in the role of data and technology in society. It responds to the digitalisation of our daily lives and the explosion not only in the volume of personal data being generated, but also in the comprehensiveness and granularity of the records those data create about each of us—a phenomenon often described as "big data".

We live in a world increasingly dominated by the creation, collection, aggregation, linkage, storage and sharing of vast collections of data pertaining to individuals. Some of those data we generate and reveal by choice, for example, through social media and email, or through compulsory disclosure, for example, as a condition of banking or travelling.

Other data are collected by sensors that surround us in our smartphones, tablets, laptops, wearable technologies and even sensor-enabled clothing, cars, homes and offices. Increasingly, even public spaces are equipped with video cameras that recognise faces and gaits and microphones that record conversations and detect ambient noises. With the growth of the Internet of Things, connected sensors process an astonishing volume and variety of data without our even being aware. According to a 2014 study by HP, nine out of ten of the most popular consumer Internet-connected devices carry personal data.[16]

Still more data are calculated or inferred based on demographic information and past behaviour. Those data are created, not collected. Moreover, data that may not originally appear personally identifiable may become so or may generate personally identifiable information through aggregation and correlation.

A large volume of these data are held by businesses with which we have infrequent contact or by third parties with whom we have no direct dealings. According to the *New York Times*, one company alone in 2012 engaged in 50 *trillion* data transactions a year, almost none of which involve collecting data directly from individuals.[17]

"Big data" is both fostered by, and contributes to, a wider range of developments that include: ubiquitous surveillance as part of efforts to fight terrorism and other crimes; detecting money-

[14] 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 (General Data Protection Regulation) (15 December 2015), ¶ 66.
[15] Id., ¶ 60(b).
[16] HP, Internet of Things Research Study (2014).
[17] Natasha Singer, "You for Sale: Mapping, and Sharing, the Consumer Genome," *New York Times*, 16 June 2012.

laundering; facilitating a range of public goods from tax collection to public safety; interconnected sensors (i.e., the "Internet of Things") to improve product safety and supply; enhancing public convenience; supporting sustainability and energy efficiency; improving medical research and health care, including supporting in-home health care for the elderly and disabled; supporting connected cars, and myriad other purposes; exponential increases in storage capacity and decreases in storage costs; dramatic increases in, and widespread distribution of, computational capacity; and increasingly pervasive networks.

## IV. The Challenge for Data Protection

The proliferation and interconnection of big data raise significant new privacy issues and challenges to the existing approaches to data protection regulation and compliance, all of which will require effective risk management as part of the solution.

For example, dramatic increases in the ubiquity of data collection, the volume and velocity of information flows and the range of data users (and re-users) challenge **the transactional model of data protection**, reflected in the OECD Guidelines and most modern privacy laws. Adopted 35 years ago, the transactional model assumes that data will be collected from individuals with their knowledge and, in most cases, consent, based on a notice describing intended uses, and not reused for different purposes.

Under the OECD's Purpose Specification Principle, for example, "the purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose."[18]

However workable this approach may have been in 1980, when adopted by the OECD, it seems out of date in a world of big data, which, in the words of Professor Paul Ohm, "thrives on surprising correlations and produces inferences and predictions that defy human understanding."[19] As Professor Ohm writes: "How can you provide notice about the unpredictable and unexplainable?"[20]

Similarly, big data and the other phenomena connected with it challenge **the continuing reliance on notice and choice at time of collection**, which has been a hallmark of OECD-based data protection systems. Under the OECD Guidelines, personal data should be obtained "where appropriate, with the knowledge or consent of the data subject", and used for any different purpose than that specified in the notice only with "the consent of the data subject; or by the authority of law."[21]

---

[18] *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, C(80)58/FINAL, as amended by C92013)79 (2013), supra at 12.

[19] Paul Ohm, "Changing the Rules: General Principles for Data Use and Analysis," in Julia Lane, Victoria Stodden, Stefan Bender, Helen Nissenbaum, eds., *Privacy, Big Data, and the Public Good* 100 (Cambridge 2014).

[20] Id.

[21] Id. at ¶¶ 9-10.

But in a world of big data this focus on notice and consent places an untenable burden on individuals to understand the issues, make choices and then engage in oversight and enforcement each time they interact with technology and when data about them is used as they conduct their daily activities. This untenable burden may not be "appropriate." Similarly, personal information is increasingly used by parties with no direct relationship to the individual or generated by sensors (or inferred by third parties) over which the individual not only exercises no control, but with which he or she also has no relationship.

As a result, the focus on notice and choice runs the risk of both underprotecting privacy and seriously interfering with—and raising the cost of—subsequent beneficial uses of data. It also requires the data protection community to think more creatively about ways of informing and empowering individuals. This may explain why the May 2014 report by the US President's Council of Advisors on Science and Technology, *Big Data and Privacy: A Technological Perspective,* described the "framework of notice and consent" as "unworkable as a useful foundation for policy" in a world of big data.[22]

Another set of challenges presented by big data concerns **deidentification, anonymisation and pseudonymisation**. These terms reflect a critical concept in modern data protection law, because personal data that are deidentified, anonymised or pseudonymised rarely have to comply with those laws' requirements because the data are no longer considered "personally identifiable" or "personal data".

Unfortunately, with sufficient interconnected data, even deidentified, anonymised or pseudonymised data may, in certain circumstances, be rendered personally identifiable. For example, in one study, Professor Latanya Sweeney showed that 87 per cent of the US population is uniquely identified with just three data elements: date of birth, gender and five-digit ZIP Code.[23] There are well-publicized examples of Google's, Netflix's, AOL's and others' releasing deidentified data sets only to have the data reidentified within days by researchers correlating them with other data sets.[24] As *The Economist* wrote in August 2015, "the ability to compare databases threatens to make a mockery of such [data] protections."[25]

Similarly, previously nonidentifiable data may act to identify unique users or machines in a world of big data. For example, browser choice and font size, when used together, can provide an accurate, unique online identifier.[26] In a world of big data, Cynthia Dwork writes, "'De-identified data' isn't."[27]

---

[22] Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values xi (2014).
[23] Latanya Sweeney, Simple Demographics Often Identify People Uniquely, Carnegie Mellon University, Data Privacy Working Paper 3 (2000).
[24] *See* Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA Law Review 1701 (2010).
[25] We'll See You, Anon, *Economist*, 15 August 2015.
[26] *See, e.g.,* Peter Eckersley, How Unique Is Your Web Browser?, Electronic Frontier Foundation.
[27] Cynthia Dwork, "Differential Privacy: A Cryptographic Approach to Private Data Analysis," in Julia Lane, Victoria Stodden, Stefan Bender, Helen Nissenbaum, eds., *Privacy, Big Data, and the Public Good* 297 (Cambridge 2014).

The challenge we face literally around the world is to evolve better, faster and more scalable mechanisms to protect personal data from harmful or inappropriate uses, without interfering with the benefits that data are already making possible today and promise to make even more widespread in the future. After all, as *The Economist* recently noted, "the electronic 'data exhaust' people exhale more or less every time they do anything in the modern world is actually useful stuff which, were it freely available for analysis, might make that world a better place."[28] Risk management that protects individuals but avoids unnecessary impediments to the beneficial use of personal information is key to addressing the above issues and to protecting privacy effectively in the 21st century.

## V. A More Systematic and Well-Developed Use of Risk Management

By assessing the likelihood and significance of both harms and benefits, risk management helps organisations identify mitigation strategies and ultimately reach an optimum outcome that maximises potential benefits while reducing the risk of harms.[29] As the editors of Oxford University Press' *International Data Privacy Law* (*IDPL*) opined:

> [We] applaud the attention being given to risk management and its role in data protection. In its proper place, risk management can help prioritize the investment of scarce resources in protecting privacy and enforcing privacy obligations. It can identify serious risks to privacy and measures for mitigating them. It can expand our collective thinking about the range of risks that the processing of personal data can present to individuals, organizations, and society, especially in a world of nearly ubiquitous surveillance, big data, cloud computing, and an onslaught of Internet-connected devices. And it can help bring rigor and discipline to our thinking about data processing and how to maximize its benefits while reducing its costs.[30]

However, to achieve risk management's full potential, six key steps are necessary:

### 1. A Science of Risk Management

Most data protection risk management processes, whether undertaken by businesses or regulators, have been informal and unstructured and failed to take advantage of many of the widely accepted principles and tools of risk management in other areas. As the *IDPL* editors note, "despite the longstanding role of, and intensified recent attention to, risk management in

[28] We'll See You, Anon, supra.
[29] International Organization for Standardization, *ISO 31000:2009 Risk management—Principles and guidelines. See generally*, Centre for Information Policy Leadership at Hunton & Williams LLP, *A Risk-based Approach to Privacy: Improving Effectiveness in Practice* (2014); Centre for Information Policy Leadership at Hunton & Williams LLP, The Role of Risk Management in Data Protection (2014).
[30] Christopher Kuner, Fred H. Cate, Christopher Millard, Dan Jerker B. Svantesson & Orla Lynskey, Risk management in data protection, *International Data Privacy Law*, vol. 5, no. 2, 95 (2015). See also Jules Polonetsky, Omer Tene & Joseph Jerome, Benefit-Risk Analysis for Big Data Projects (2014).
[30] Id.

data protection, it is still a developing field that lacks many of the widely accepted principles and tools of risk management in other areas."[31]

It is critical that risk management around data protection, while remaining flexible, not continue in the largely ad hoc, colloquial terms in which it has evolved today. Other areas—for example, financial and environmental risk—have seen the development of a professional practice of risk management, including specialised research, international and sectoral standards, a common vocabulary, and agreed-upon principles and processes. The same is needed in data protection risk management. In some cases, these can be borrowed from areas in which formal risk assessment is better developed, but in others it requires the collaboration of regulators, industry and academics to fill important gaps.

## 2. A Framework of Harms

Risk management in the field of data protection has suffered from the absence of any consensus on the harms to individuals that risk management is intended to identify and mitigate. This is the starting point for effective risk assessment in other fields, yet in data protection, regulators and businesses alike have failed to articulate a comprehensive framework of harms or other impacts, much less to reach consensus regarding those that should be part of effective risk management. Much work remains to be done on the critical issue of identifying the relevant impacts that should be considered in risk management.

In the Centre for Information Policy Leadership's 2014 white paper *A Risk-based Approach to Privacy: Improving Effectiveness in Practice*, we first focused on this critical issue: "Data protection and privacy laws are meant to protect people, not data. But from what exactly are people being protected? What threats? What harms? What risks?"[32] At the time, we also offered a preliminary matrix of tangible and intangible harms. Later that year, NIST issued a Risk Model Discussion Draft in which it noted: "Harms from security breaches are generally well understood. In privacy, consensus is still being developed around what constitutes harms. However, if the privacy engineering objectives are intended to mitigate the risk of privacy harms, then the underlying harms need to be explicated in order to assess the utility of the objectives."[33]

Surprisingly, despite almost 50 years of experience with data protection regulation, a clear understanding of underlying harms is still lacking—in the scholarly literature, in the law and in organisational practices. In part this is due to focusing on simplistic and legalistic compliance with notice and consent requirements and equating harm to data collection without proper notice and consent, while failing to address the potential negative impacts on individuals of the data collection and uses themselves.

That does not equate with the way most people think about data-related harms, which is more focused on data's being used in a way that might cause them injury or embarrassment or distress, rather than the presence or content of privacy notices. Hence, there is a widespread need to think

[31] Id.
[32] *A Risk-based Approach to Privacy: Improving Effectiveness in Practice*, 2.
[33] *NIST Privacy Engineering Objectives and Risk Model Discussion Draft,* at 3, n.9.

more critically and more systematically about what constitutes a harm that the risk management framework should seek to minimise or prevent when evaluating data uses.

There are a wide range of possibilities for what might constitute a harm, but it seems clear that the term must include not only a wide range of tangible injuries (including financial loss, physical threat or injury, unlawful discrimination, identity theft, loss of confidentiality and other significant economic or social disadvantage), but also intangible harms (such as damage to reputation or goodwill, or excessive intrusion into private life) and potentially broader societal harms (such as contravention of national and multinational human rights instruments). What matters most, though, is that the meaning of harm be defined through a transparent, inclusive process and with sufficient clarity to help guide the risk analyses of data users.

## 3. A Broader Understanding of Benefits

In addition to assessing potential harms, it is also important for both organisations and regulators to examine the benefits (or purposes) of data processing systematically and objectively. The benefits need to be evaluated and understood at the outset of any risk management process, because without understanding the benefits at stake, it is impossible to determine the appropriate level of mitigations or controls for the risks of harms. Further, after mitigating such risks to the appropriate level in light of the identified benefits, it must be determined if any residual risks of harm are acceptable.

As with harms, this assessment of benefits should include both the magnitude of benefit and its likelihood of occurring. The range of benefits should include benefits to individuals (e.g. ability to complete a transaction, obtain a desired good or service, be protected from fraud, enjoy greater efficiency or convenience and access, and improved medical treatment and prevention) and to the data user (e.g. ability to attract customers, deliver goods or services more efficiently and reduce fraud and other losses).

The benefits that should be considered as part of risk assessment should also include those likely to be enjoyed by society more broadly (e.g. use of data for social good such as reducing the spread of infection diseases, enhancing research in health care and other areas that benefit the public, guarding against terrorism and other crimes, reducing environmental waste, delivering services to the public with greater efficiency and fairness, etc).

As with harms, analysing the likelihood and magnitude of benefits as part of a broader framework will enhance the ease, accuracy and consistency of the analysis. It will also reduce the cost and burden of risk assessment and make that assessment more tenable for smaller organisations. A framework can help provide predictability for individuals. And developing a framework of benefits can provide both individuals and regulators an opportunity to participate meaningfully in the process, while helping to ensure that the data protection facilitated by the framework serves critical social and individual values.

As the *IDPL* editors note, the "absence of a widely accepted framework of impacts to be avoided or sought out presents both an opportunity and a challenge." The "challenge is to do so quickly

to keep pace with dramatic changes in technology and human and institutional behaviour." The opportunity is to "develop modern, effective risk management tools and a framework of impacts—both harms and benefits—building on decades of experience with risk management broadly."[34]

## 4. A Clear Objective of Risk Mitigation

Rarely can risk be eliminated entirely. Therefore, the goal of the risk management process is to assess risks and benefits, focus attention on those activities presenting the greatest risk to privacy, identify measures that can reduce the risk as fully as practical and prudent in light of the benefits at stake, and be explicit about the remaining risks and how they will be managed so that the controller, and ultimately the data subjects and the regulators, understand the risks and undertakings that remain. We must be clear about these goals.

The Explanatory Memorandum that accompanied the 2013 revisions to the OECD Guidelines made clear that management of "risk" is intrinsically connected with "proportionality", indicating, in the context of transborder data flows for example, that "any restrictions upon transborder data flows imposed by Member countries should be proportionate to the risks presented (i.e. not exceed the requirements necessary for the protection of personal data), taking into account the sensitivity of the data, the purpose and context the processing."[35] In its 2015 report on *Data-Driven Innovation* the OECD stressed that "a certain level of risk has always to be accepted for the value cycle to provide some benefit."[36]

The Article 29 Working Party has recently echoed this theme in the context of applying legitimate interests under Article 7(f) of the EU Data Protection Directive: "The purpose of the Article 7(f) balancing exercise is not to prevent any negative impact on the data subject. Rather, its purpose is to prevent disproportionate impact. This is a crucial difference."[37] After all, in the words of the consulting firm PricewaterhouseCoopers: "Overcontrolling risk can be costly and stifle innovation."[38]

## 5. Risk Management in Practice

To be effective, risk management must work in practice. This requires that risk management tools be efficient, scalable and flexible, so that they work for large organisations and for SMEs.

This was a particular focus of the negotiations over the EU General Data Protection Regulation. In its 3 October 2014 note to the Council detailing efforts to reach agreement on a "partial general approach" to Article IV, the Presidency noted "the need to further reduce the administrative burden/compliance costs flowing from this Regulation by sharpening the risk-

[34] Risk management in data protection, supra at 97.
[35] OECD, *Supplemental Explanatory Memorandum,* at 30.
[36] Organisation for Economic Cooperation and Development, *Data-Driven Innovation* (2015), 212.
[37] Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC,* at 41.
[38] PricewaterhouseCoopers, *A Practical Guide to Risk Assessment* (2008), 33.

based approach."[39] As one step towards that end, the final text provides that "best practices to mitigate the risk" could be provided by "approved codes of conduct, approved certifications, guidelines of the European Data Protection Board or through the indications provided by a data protection officer."[40]

In addition, one risk management exercise may be applied to a variety of similar data processing activities. For example, the regulation provides that a "single assessment shall be sufficient to address a set of similar processing operations that present similar" high risks.[41]

After taking into account those measures that the data user can take to reduce risk, risk management can even be used to create presumptions concerning common data uses so that both individuals and organisations can enjoy the benefits of predictability, consistency and efficiency in data protection.

For example, some uses in circumstances that present little likelihood of only negligible harms might be expressly permitted, especially if certain protections such as appropriate security were in place and the purpose or benefits of the uses otherwise justify them. Conversely, some uses where there is a higher likelihood of more severe harms might be prohibited or restricted without certain protections in place, especially where the harms are not outweighed by the applicable purpose or benefits. For other uses that present either little risk of more severe harms or greater risk of less severe harms, greater protections or even a specific and fuller notice and/or consent might be required so that individuals have an opportunity to participate in the decision-making process.

The OECD stressed in its 2015 report on *Data-Driven Innovation*: "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."[42]

## 6. Risk Management in the Context of Other Privac Tools and Requirements

Risk management works hand in hand with other privacy requirements, concepts and tools, especially in the context of big data. Risk management is necessary to all of these, but it does not replace any of them. Its effectiveness as a sensitive privacy protection tool for big data may be greatly enhanced when used in combination with these. These privacy elements with a necessary interplay with risk management include legitimate interest processing.

- **Legitimate interest** processing, as recognized by European data protection laws, can legitimise many ordinary business uses of data, such as improving and marketing a company's own products or services, or ensuring information and network security. It

[39] Note 13772/14, 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 (General Data Protection Regulation) [First reading]—Chapter IV (2014), at 1.
[40] General Data Protection Regulation, at ¶ 60c.
[41] Id., art. 33, ¶ 1.
[42] OECD, *Data-Driven Innovation* at 226.

also plays an increasingly significant role in the context of big data, the Internet of Things and machine learning by enabling beneficial uses of data in the ever-increasing circumstances where consent is not feasible. But its successful operation requires a thoughtful assessment of privacy risks to individuals, the benefits that may result from responsible use of the data and measures for reducing negative privacy impacts.

- **Fair Processing**. Fair processing is a stand-alone data protection principle in many data privacy laws in Europe and beyond. Over the years, practitioners and regulators have equated fairness with providing privacy notices to individuals; however, the Centre for Information Policy Leadership's president, Bojana Bellamy, and vice president, Markus Heyder, have argued that fair processing "goes beyond privacy notices and we believe the time has come to resurrect this principle back into practice."[43] Determining whether proposed processing is "fair" requires assessing the risk of harms or benefits that it creates, and the tools available for mitigating those harms. For example, the broad authority of the US FTC to stop "unfair … acts or practices in or affecting commerce", which it has applied with increasing frequency in the area of data protection, requires a risk assessment by both industry and the Commission. The FTC's unfairness authority applies only to practices that cause "substantial" injury to consumers that are "not reasonably avoidable by consumers themselves" and are "not outweighed by countervailing benefits to consumers or to competition."[44] As a result, the FTC, and businesses subject to its jurisdiction, must consider both "injuries" and "benefits" and must explicitly balance them.

- **Transparency Tools**. Under many data protecting regimes, transparency has been conflated with notice. In a world of big data, ubiquitous surveillance, remote sensing and other technological developments, meaningful notice is increasingly difficult to provide or to consider as an adequate substitute for true transparency. Moreover, notice has been used so widely, especially as a response to security breaches, that even when they may be valuable, they are often ignored by a public suffering from legal notice fatigue. Fortunately, there are many other ways to provide meaningful transparency and individual participation through surrogates, technologies, dashboards, access and the like. The content of transparency tools will also be impacted by risk management considerations. The greater the risk, the more transparent and more meaningful privacy notices and other transparency tools should be. Additionally, in the context of big data and analytics where consent may not be practicable or required (due to legitimate interest processing, for example), transparency will increasingly have to be reconceptualized from mere notice (as the basis for consent) to a broader explanation of the value exchange between individuals who provide their data and organisations that use it, as well of how the organisations protect the data from misuse and individuals from harm based on an appropriate risk assessment.

[43] Bojana Bellamy & Markus Heyder, Empowering Individuals Beyond Consent, International Association of Privacy Professionals Privacy Perspectives (2015), at 3.
[44] 15 USC § 45(n).

- **Renewed Focus on Context and Data Use**. There is often a compelling reason for personal data to be disclosed, collected or created. Assessing the risk to individuals posed by those data almost always requires knowing the context in which they will be used. Data used in one context or for one purpose or subject to one set of protections may be both beneficial and desirable, while the same data used in a different context or for another purpose or without appropriate protections may be both dangerous and undesirable.[45] As a result, data protection should, in the words of the US President's Council of Advisors on Science and Technology, "focus more on the actual uses of big data and less on its collection and analysis."[46] Risk management is essential to assessing the potential for bothnegative and positive impacts of a proposed use of personal data, identifying appropriate privacy protection tools and ultimately determining which uses should be permitted. This does not take away the value of understanding risks at the time of data collection, but it is more appropriate to focus on the whole life cycle of data—from its collection to its various uses. Professor Susan Landau wrote in 2015 in *Science* that "the value of big data means we must directly control use rather than using notice and consent as proxies."[47] Indeed, the terms under which data use would be controlled are determined by systematic risk assessment.

## VI. Conclusion

Risk management has long played an important role in data protection. Today, however, risk management is essential in the world of big data and other technological innovations. It facilitates thoughtful, informed decision making by organisations by requiring them to explicitly consider both the harms and benefits not only to the organisations but also to the data subjects, and by focusing increasingly scarce resources of both organisations and government regulators where they are needed most.

For risk management to achieve its true potential, a collaborative effort by regulators, industry, civil society and academics is necessary to help develop a science of risk management with essential elements such as a framework of privacy harms or other negative impacts; a framework for analysing benefits resulting from data processing; a shared vision of risk management as a tool for reducing and managing (rather than eliminating) risk or harm; a shared collection of risk management best practices; and a clear understanding of the role risk management plays in context with other modern data protection concepts and tools.

The need to do so is clear because risk management is critical to those concepts and tools, including legitimate processing, fair processing, transparency and a renewed focus on data use. None of these measures can be used effectively without systematic risk management. And the failure to deploy these tools will only contribute to the erosion of privacy. By contrast, when used together, these tools can ensure that data protection and legal norms remain relevant in the 21st century.

[45] *See* Helen Nissenbaum, *Privacy in Context* (Stanford University Press 2010).
[46] Big Data: Seizing Opportunities, Preserving Values, supra at xiii.

The development of risk management can serve another critical purpose as well: it can help bridge gaps that too often separate disparate data protection legal regimes. If regulators, industry leaders, academics and others can work together across national boundaries to build consensus around a science of data protection, a framework of privacy harms, a collection of risk management best practices and the other key steps outlined above, data protection may not only be relevant, but also effective, efficient and consistent with valuable data flows that routinely cross national boundaries.