

**COMMENTS ON THE FEDERAL COMMUNICATION COMMISSION'S NOTICE OF PROPOSED
RULEMAKING ON PROTECTING THE PRIVACY OF CUSTOMERS OF BROADBAND AND OTHER
TELECOMMUNICATION SERVICES**

WC DOCKET NO. 16-106

SUBMITTED VIA ELECTRONIC FILING

May 20, 2016

The Centre for Information Policy Leadership (CIPL)¹ appreciates the opportunity to respond to the Federal Communication Commission's request for comments on the Notice of Proposed Rulemaking (NPRM) on Protecting the Privacy of Customers of Broadband and Other Telecommunication Services that was released on April 1, 2016. CIPL supports the attention given by the FCC to the issue of privacy protections for the personal information of customers of Internet Service Providers. As a global information and privacy policy think tank, CIPL has been on the forefront of a wide range of policy debates and initiatives around the world relating to improving privacy protections for individuals. One of the core questions that underpins the entirety of our work in this area is how to achieve effective privacy protections in ways that also enable technological innovation and the full range of beneficial data uses made possible by the modern information age. We believe that the FCC's proposal reflects the same concern.

However, in one significant way we believe it may not. Thus, we would like to focus our comments only on this particular issue, as we have been exploring it in other contexts, which may be relevant and instructive for the context of the NPRM. Specifically, we would like to address the potential over-reliance in the NPRM on the concept of affirmative express consent or "opt-in approval", which we believe is anachronous and ineffective in an increasing number of modern contexts.

¹ The Centre for Information Policy Leadership (CIPL) is a privacy and data protection think tank in the law firm of Hunton & Williams LLP and is financially supported by approximately 42 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices to ensure effective privacy protection in the modern information age. For more information, please see CIPL's website at <http://www.informationpolicycentre.com/>. Note that nothing in this submission should be construed as representing the views of any individual CIPL member or of the law firm Hunton & Williams.

Rethinking Consent and Developing Alternative Measures for Privacy Protection

- **The problem with consent**

In the age of big data analytics, the IoT, cloud computing and other modern information practices and uses, overreliance on consent and individual control may result in significant impediments to putting personal data to beneficial and productive uses, thereby frustrating or slowing down economic and social advancements without countervailing benefits to privacy or to individuals, as other, more effective mechanisms and tools to protect individuals are available.

Privacy policy makers and regulators around the world are grappling with the issue of consent and what role this traditional core privacy principle can and should continue to play in the modern information economy. Many believe that big data, the IoT, and the sheer size and complexity of the digital economy have eclipsed the usefulness of affirmative, express consent in an increasing number of contexts, rendering consent an ineffective tool for individual control or privacy protection in these contexts. Thus, more and more policy makers and regulators are looking for alternatives to consent for contexts where consent is no longer practical or effective.

Below, we highlight a few key considerations on this subject, attaching several of CIPL's more detailed papers on the subject.

- **Alternatives to consent**

Alternatives to consent already exist. By way of one example, both the EU Data Protection Directive² and the new EU General Data Protection Regulation³ permit data processing on the grounds of "legitimate interest", which allows for data processing in contexts where consent is not feasible and if the processing is necessary for the purposes of the legitimate interests of the business or a third party and these interests are not overridden by the interests or fundamental rights of the data subject. Thus, it essentially allows for processing on the basis of a favorable benefits/risk analysis rather than consent.⁴

² Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, No. L 281/31, Art. 7(f).

³ General Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 6(f), published on 8 April 2016 following the European Council's adoption of its position at the first reading of the Regulation, available at <<http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf>>. On 14 April 2016, the European Parliament approved the GDPR.

⁴ The EU's "legitimate interest" basis for data processing, while useful as an example of the fact that alternatives to consent are important and currently in use, has limitations of its own, such as the fact that it does

This basis for processing is being considered in the development of other legal regimes outside of the EU. For example, the two principal Brazilian draft privacy laws making their way through the legislative process in Brazil include “legitimate interest-based” processing.

Further, the discussion paper “Consent and Privacy” released by the Canadian Office of the Privacy Commissioner just last week, asks whether Canada should adopt a similar option for processing without consent (among other alternative options). It suggests that Canada may have to rethink its privacy law’s current reliance on consent, “[g]iven the challenges to the consent model in the digital environment.”⁵

CIPL has addressed the challenges of consent and the possible solutions in a number of white papers and articles. Rather than recapping them at length here, we simply attach them for your detailed review.

- **CIPL papers on consent and alternative frameworks of protection**

The first is a short article entitled “**Empowering Individuals Beyond Consent,**” which was first published by the IAPP in July 2015. It describes the ineffectiveness of consent in an increasing number of contexts and points to several alternative measures that can be used to protect and empower the individual in the modern information age. It does not argue that consent can and should not be improved through better transparency and choice mechanisms where consent still is feasible and appropriate. (See Appendix A).

The second is a discussion paper on “**The Role of Enhanced Accountability in Creating a Sustainable Data-Driven Economy and Information Society,**” which we issued in October 2015. It discusses how in contexts where individual control, choice and consent are not practicable or feasible (because, for example, the intended data uses and flows are too complex, manifold, or even yet unknown), the responsibility of privacy protections must fall on the business rather than the consumer. It further describes how this responsibility can be discharged through a number of measures, all of which are encompassed by the concept of “enhanced accountability,” which means that an organization has a comprehensive accountability or information management and privacy compliance program in place that includes effective transparency measures, benefit/risk assessment, training, internal oversight, written policies,

not apply to processing of “special categories of personal data”, including data revealing race, ethnicity, religious beliefs, or data concerning genetics, health and sexual orientation, among other sensitive data. See EU GDPR, Article 9. In the accountability and risk-based frameworks we are proposing below and in our attached materials, the sensitivity of the data would be one factor to consider in a benefit/risk analysis and in the selection of appropriate mitigations and controls.

⁵ “Consent and Privacy – A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act”, Office of the Privacy Commissioner of Canada, May 11, 2016, available at https://www.priv.gc.ca/information/research-recherche/2016/consent_201605_e.asp.

privacy by design, complaint handling and dispute resolution, as well as frameworks for “fairness” and ethical considerations, all of which would be subject to governmental oversight and enforcement. Within this framework, effective transparency will have the important role of explaining the value-exchange between individuals, society and the organizations that put data to beneficial uses (including unknown future uses) as well as the measures taken to protect individuals from harm, thereby creating public trust that data will be used responsibly. The paper argues that organizations that implement such enhanced accountability frameworks with respect to their information collection and use practices should be able to use information in all ways commensurate with the opportunities of the modern information age where specific consent is not available, practicable or effective. (See Appendix B)

The third is a discussion paper on “**The Role of Risk Management,**” which we issued in February 2016. In that paper, we focus specifically on risk assessment as one of the core elements of any accountability framework. Effective benefit/risk assessments with respect to proposed data uses will enable businesses to understand the potential harmful impacts of their proposed products and services on individuals (taking into account the purpose and scope of the proposed use, the nature of the data, including its degree of sensitivity, among other factors) and enables them to make better decisions about whether and how to proceed with the proposed use and what mitigations and controls to implement in light of the specific risk and benefits. Formalized and structured risk assessments also enable businesses to demonstrate their accountable decision-making processes to enforcement authorities in the event of an investigation. (See Appendix C)

- **The effects of consent under the NPRM**

We believe that the issues and potential alternatives to consent discussed in these papers are directly relevant to the NPRM’s proposal to require opt-in consent for sharing customer proprietary information with certain affiliates and third parties or for using information for the ISP’s own unrelated purposes.

The NPRM asks in paragraph 128 whether ISPs and their affiliates “need or benefit” from using customer proprietary information for non-marketing purposes and “what are those uses and are they consistent with consumer expectations?” However, the nature of the modern information economy, including big data, the IoT and other components of this environment, ensures that the question of “what are those uses” cannot always be answered in advance with any specificity.

Indeed, this is precisely the value of modern information uses that must be protected. Analyzing and combining data in new ways may lead to unexpected insights and uses that will be beneficial not just to individual businesses, but also to consumers and society. The Canadian consent report notes that modern technology can result in future uses of data that “defy our imagination” and that are “difficult to anticipate” and thus can’t be governed by a “consent”

that was given at the time when the data was collected.⁶ In many instances, requiring opt-in consent for the entire range of known, possible or yet unknown future beneficial uses of data would not only overwhelm and burden individuals, thereby undermining true individual control and empowerment, it would also likely result in a chronic failure to give consent for no good reason simply because the individual cannot or won't dedicate the time and energy to consider the request. Thus, we believe that any aspect of the NPRM that potentially hinders the beneficial uses of information for new purposes should be subjected to intense further scrutiny and compared to alternatives that are more protective of privacy and the individual,⁷ as outlined in our attached papers.

- **The relevance of the FTC model**

We also note that the accountability-based alternatives we propose, including and particularly the benefit/risk assessment element of such accountability-based frameworks, are very much in line with the FTC's privacy enforcement model under its "unfairness and deception" authority. Particularly the unfairness standard, which requires businesses to weigh the countervailing harms and benefits of an action and be able to prove the legitimacy of their analysis to a regulator, provides a framework that is better suited to the modern information context where using information will as a matter of necessity become less and less a matter of individual control and more and more a matter of fair and responsible processing of data, backed up by credible oversight and enforcement.

Thank you for accepting and considering our comments and recommendations. If you have any questions about this submission, please contact Bojana Bellamy, President, Centre for Information Policy Leadership, bellamy@hunton.com or Markus Heyder, Vice President and Senior Policy Counselor, Centre for Information Policy Leadership, mheyder@hunton.com.

⁶ *Id.* at 7

⁷ For similar reasons, we would also discourage the FCC from adopting *ex ante* rules limiting the collection of customer data by ISPs. Data collection limitations would interfere with beneficial data uses in similar ways as requiring opt-in consent would and would have negative societal consequences. Any risk to individual privacy can and must be minimized through the alternative means discussed in our papers.

Appendix A

July 2, 2015

Empowering Individuals Beyond Consent

by *Bojana Bellamy and Markus Heyder*

Originally appeared on the [IAPP's Privacy Perspectives](#)



Individual consent to data processing has been an anchor of data protection and privacy laws around the world. The assumption is that consent ensures that information practices are focused on the rights and interests of individuals by enabling them to control the use of their personal data. Most lawmakers resort to the consent-based model by default.

But is consent really the best and only way in this modern Information Age to provide meaningful control and to protect the individual?

This question is arguably the most burning question in data protection today. It is particularly relevant at a time when the legislative process on the new European Data Protection Regulation is entering the final furlong and other countries are revising their privacy laws (Japan) or legislating for the first time (Brazil).

We do not believe that consent is the best or only way to empower individuals in this day and age for three reasons.

First, consent has become overused and an over-relied-upon in practice, calling into question its function as indicator of meaningful individual choice and control. Privacy policies and notices are too numerous, long and complex to result in valid consent. In their efforts to cover all possible scenarios, comply with multiple variations of national privacy laws and avoid legal liability for deceptive practices, organizations feel compelled to cram their privacy policies with information that can neither be absorbed by ordinary mortals nor empower them to make valid choices. While privacy policies will always have their place in protecting organizations from legal liability, they do not effectively protect individuals or provide them with real control.

The solution to this problem will not simply be in developing shorter and better privacy policies in order to obtain more valid consent.

Second, modern information practices are on a collision course with canonical consent requirements as envisaged in many data privacy laws today. Increasingly, there are situations where consent will simply not work because:

- The context makes it impossible to obtain valid individual consent, such as where there is no direct interaction with individuals or individuals may not have a relationship with organizations that may touch their data in the context of machine learning or in an ecosystem of mobile devices and the Internet of Things (IoT);
- The context makes consent inappropriate, such as in fraud prevention or information systems and network security, where seeking consent would prejudice the very purpose of processing;

Empowering Individuals Beyond Consent

by Bojana Bellamy and Markus Heyder
Privacy Perspectives | July 2, 2015

- The practical implementation of a consent requirement would unduly burden individuals, such as where consent requests by multiple organizations in some online service ecosystem would constantly interrupt and seek the attention of individuals as they go about their daily lives, especially in connection with processing that is expected.

As Airbnb's Douglas Atkin eloquently said, "In the distant future, we'll forget the idea of engaging in technology at all. We'll swallow it, absorb it and wear it, without us really thinking we're engaging in technology per se."

How would consent and individual control look in a world where we will not specifically engage in technology but the technology becomes part of us and everything around us?

Third, and perhaps most importantly, are other mechanisms in our ever-growing privacy toolkit and existing legal regimes that, in the appropriate contexts, are able to deliver privacy protection and meaningful control more effectively than consent. However, while these alternative mechanisms already exist, they must be better understood, further developed and more broadly accepted.

Policy-makers and lawmakers, as well as privacy regulators, should be shifting a significant portion of their attention from consent to these other mechanisms and safeguards. And organizations, in turn, must be prepared to embrace such alternative and innovative ways to deliver privacy and empowerment to individuals. Of course, there will always be situations where freely given and specific consent will be appropriate and the only way to use people's information. However, these situations are limited and must be narrowly construed to ensure the validity of the consent.

Here are some of these additional mechanisms and "individual empowerment" tools that we believe will play an increasing role in the Information Age. They will allow organizations to manage data in a way that truly focuses on the individual, provides more effective compliance and privacy protection and facilitates actual individual control in appropriate circumstances.

- **Legitimate Interest Processing.** European privacy laws already provide for a range of alternative legal bases for data processing that are on equal footing with consent. These bases include performance of a contract, legal obligation, vital interest of individuals, public interest or exercise of official authority and, crucially, legitimate interests of the controller or a third party, provided that individuals' rights and freedoms are not prejudiced. Legitimate interest-based processing is particularly relevant as it provides the necessary flexibility to face future technology and business process changes, while requiring organizations to be proactive, think hard and consider and mitigate risks and harmful impacts on individuals as they process personal data. Legitimate interest processing can legitimize 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 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 where consent is not feasible and the benefits of the proposed uses outweigh any privacy risks or other harmful impacts on individuals. In its [Opinion of April 2014](#), the Article 29 Working Party underscored legitimate interest-based processing as an example of true organizational accountability and responsible data management and provided specific guidance for organizations.
- **New Transparency.** Notice and consent have often been conflated. The time has come to firmly separate the two as stand-alone requirements. While there cannot be meaningful, informed consent without full notice, there can be useful and effective privacy policies where consent is neither sought nor necessary. Many legal regimes already treat notice as a separate legal obligation from consent. That distinction should be further emphasized and clarified to facilitate a transition from traditional privacy policies to new and effective transparency that clearly communicates an organization's information practices in the Information Age. Of course, traditional privacy policies and legal notices

Empowering Individuals Beyond Consent

by Bojana Bellamy and Markus Heyder
Privacy Perspectives | July 2, 2015

will continue to exist as matter of discharging an organization's legal obligations. However, new transparency will go beyond what's required in a legal notice, focusing on individuals and explaining the current and potential uses of data in a way that makes sense. It will address future uses that are not yet known and any associated concerns. It may explain the rationale and benefits of additional uses of data as a matter of customer relationship and be presented in an innovative and user-friendly manner, through dashboards, portals, interactive apps and, where required or possible, may set forth innovative ways to exercise choice and control.

- **Focus on Risk and Impact on Individuals.** Risk management and the need to understand, assess and address risks and harmful impact to individuals is fast becoming an integral part of organizational accountability and increasingly a legal obligation in many privacy laws. From formal data privacy impact assessments and privacy by design for new products and services, to consideration of risk and harm to individuals when deciding on appropriate security measures or on whether to provide breach notification, risk is an integral part of how organizations prioritize and implement their privacy compliance programs. This approach puts individuals firmly at the center of an organization's information management practices and results in better protection and compliance for individuals, especially in contexts where individual consent is neither required nor feasible.
- **Individuals' Rights to Access and Correction.** Access and correction rights are important elements of individual control and central to many data privacy regimes around the world. The ability of individuals to have access to their data and be able to correct inaccurate or obsolete data is an essential mechanism of control that should be made available as widely as possible. Access and correction are also intrinsically related to transparency and organizations may be able to innovate here too.
- **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. Fair processing, however, goes beyond privacy notices and we believe the time has come to resurrect this principle back into practice. In its [2014 report on big data and data protection](#), the UK Information Commissioner's Office (ICO) elaborates on the concept of fair processing in the context of big data. The ICO suggests organizations should consider factors such as whether the proposed use was known or reasonably "expected" by individuals, whether it may result in "drawing conclusions or making decisions about individuals," whether individuals were deceived or misled about how their data will be used, the impact of the proposed processing on the individual and the integrity and accuracy of data. These fair processing factors ensure that information practices are focused on the individual data subject and go a long way in effectively protecting the individual from harmful impacts.

We have over-relied on consent at the expense of other individual empowerment mechanisms and tools. We have overburdened individuals and deputized lay people to play privacy professional in contexts that are increasingly complex and difficult to follow. Plus, we have underestimated the need to adapt our privacy principles to the rapid changes that technology is bringing to society.

Deployed appropriately, alternative tools can enhance the value of consent by limiting its use to situations where indicating actual agreement is actually possible and meaningful. Where this is not the case, the hard work on privacy must come from these alternative tools and from responsible practices of accountable organizations, but without ever losing the focus on the individuals whose personal data are being used. The many ongoing processes to reform existing privacy regimes and to create new ones provide an opportunity to get individual empowerment right.

Appendix B

Protecting Privacy in a World of Big Data

Paper 1

The Role of Enhanced Accountability in Creating a Sustainable Data-driven Economy and Information Society

Centre for Information Policy Leadership at Hunton & Williams LLP

This is the first paper in a three-part series on Protecting Privacy in a World of Big Data. The second paper is on “The Role of Risk Management,” and the third paper (forthcoming) will be on how to interpret and apply traditional privacy principles in the modern information age.

I. Summary

In the modern information age of big data, the Internet of Things and cloud computing, new data-driven products and services are enabling scientific and societal developments at a rapid pace and are the key drivers of economic growth. Our digital information society depends and thrives on the ability to generate, collect, aggregate, link and use information, including personal data, through increasingly complex technologies and global processes. Understanding how our personal information is being used in this environment is becoming increasingly difficult if not impossible for the average person. Thus, expecting individuals to take an active role in deciding how their personal information is used in all instances is increasingly unrealistic.

Yet, data protection and privacy are important societal norms and in many countries fundamental or constitutional rights. Individuals must have confidence and trust that their data are being used responsibly and consistent with these norms and rights. Thus, where still possible, individuals must be empowered to make informed decisions that relate to the use of their personal data. Where they can no longer control each particular use of their personal information in this new environment, other protections and mechanisms must be put into place that create the necessary confidence and trust among the public and regulators that personal information is being used responsibly and for purposes that are beneficial to individuals or society.

The existing concept of “organisational accountability” goes a long way to enable this public trust and the responsible use of data. Indeed, organisational accountability has become a key building block of modern privacy law and policy and is being implemented by enlightened global organisations in their corporate privacy and information management programs. However, to fully realise its potential as the basis for enabling and legitimising modern data uses, the core elements of organisational accountability need to be further developed and supplemented with additional elements, as further described in this paper.

This “enhanced accountability” will provide the necessary tools to empower and protect individuals with respect to the use of their personal data, through informed consent where possible and appropriate and

through other mechanisms where necessary and appropriate. It will give organisations the tools to take full responsibility for mitigating the harmful impacts of the technologies they deploy, especially in the increasing number of circumstances in which individuals can no longer do so themselves. It will enable a sustainable virtuous cycle of lawful and ethical data collection and responsible and beneficial data use, as well as a data cycle that treats individuals, society and organisations more like partners and joint beneficiaries in this exchange. Indeed, the more organisations adopt and demonstrate a commitment to this enhanced accountability and the culture of responsible data uses, the more they will be able to innovate, use data productively and drive benefits to individuals and society at large. However, regulators and policymakers must provide incentives for organisations that implement enhanced accountability and allow the organisations to leverage these additional responsibilities to pursue the multitude of reasonable, beneficial and innovative uses of data available in the modern information age.

II. The Accountability Landscape

The origin of accountability principle lies in the requirement for organisations to protect and be accountable for the protection of the personal information they collect and use regardless of whether the information stays within their organisations or is shared with third parties, including across borders. In other words, under the concept of accountability, the protections that apply at the point of collection flow with the information, regardless of where it goes, and the organisations that collected the information remain responsible to ensure that such protections continue to be applied.

Accountability can be achieved through organisations creating comprehensive privacy management programs that implement external privacy requirements and/or internal privacy policies that apply throughout the entire lifecycle of personal data, including to transfers to third parties and countries. The Centre for Information Policy Leadership (CIPL) has previously led a multiyear research project on organisational accountability, culminating in a number of white papers on the topic that outline in detail the essential elements and proof points of accountability, and helping to promote the concept of accountability globally.¹ The elements of accountability that make up traditional accountability-based privacy management programs include leadership and oversight, risk assessment, policies and procedures, privacy by design, transparency, training and awareness, monitoring and verification, and response and enforcement. (See diagram on p. 6)

In recent years, the concept of accountability has become widely accepted around the world.² Organisational accountability in the form of corporate privacy management programs, codes of conduct, corporate rules, cross-border privacy rules and similar schemes is now included in an increasing number of laws and legislative proposals³, elaborated upon by data protection authorities in regulatory guidance⁴,

¹ See [CIPL accountability project documents](#).

² See e.g. Bojana Bellamy, [“The Rise of Accountability from Policy to Practice and Into the Clouds”](#), IAPP Perspectives, December 2014.

³ See [Singapore Personal Data Protection Regulations 2014](#), § 10; [Hong Kong Guidance on Personal Data Protection in Cross-border Data Transfer](#) Section 33(2)(f); [Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data](#), Articles 26(2) and 27; Proposed EU General Data Protection Regulation, [Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data \[General Data Protection Regulation\]](#), proposed text of the Council of the European Union, Brussels, 11 June 2015, Section 5; Australian Privacy Principles, [Australian Privacy Principle 8 – Cross-border disclosure of personal information](#); Mexico’s [Federal Law on Protection of Personal Data Held by Private Parties \(2010\)](#), Article 44; [Brazil Ministry of Justice Draft Law “On the](#)

promoted by regional and international organisations⁵, implemented by multinational companies, and studied and promoted by forward-looking industry groups.

III. Creating Future-oriented and Responsible Data Management Programs Through Enhanced Organisational Accountability

To create the conditions for effective privacy protection and the beneficial and sustainable use of data in our digital society, it will be necessary to develop an “enhanced accountability”. This will require further development of some of the above-listed core elements of accountability and supplementing them with additional tools and considerations.

1. **New transparency.** Transparency has always been an essential element of accountability and has been implemented, primarily, through traditional privacy policies and notices. Such policies and notices will continue to be available and helpful to individuals in certain contexts. However, in the modern information age, technological developments and the ever-proliferating new uses of information will always outstrip the ability of individuals to understand fully how and by whom their information is being used. This reality requires a new application of transparency that extends beyond its traditional function of providing legal notice of specific uses.

New transparency will focus on providing individuals with more contextually useful information, contrasting with the detail of traditional privacy policies whose primary purpose is to fulfill a legal disclosure requirement. Its purpose will be to effectively communicate the general value of the intended uses of personal information for the individual, including any unexpected, out-of-context and non-obvious future uses. New transparency will explain how the individual and society may benefit from such uses and address any associated concerns and how the organisation will mitigate them. New transparency will engage individuals at a time and in a manner that is convenient to them and will give them the confidence that they can go about their lives in our digital society without having to unnecessarily burden themselves with detail concerning the potential uses of their personal information. It will enable public trust and confidence that organisations will do the right thing in contexts that do not allow for specific engagement or informed choices concerning the use of personal data.

Organisations have already experimented with better transparency over the past years, for example by making legally required notices more user-friendly through layered notices, informational videos and other means. A shift towards new transparency suitable for the modern

[processing of personal data to protect the personality and dignity of natural persons](#)”, Section 5, Article 30; [Consumer Privacy Bill of Rights Act, 2015 US Administration Discussion Draft](#); see also The White House administration’s 2012 white paper [“Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy”](#), Chapter III.

⁴ See [Privacy Management Framework: Enabling Compliance and Encouraging Good Practice](#), Office of the Australian Information Commissioner; see also [Getting Accountability Right with a Privacy Management Program](#), The Office of the Privacy Commissioner of Canada and the Offices of the Information and Privacy Commissioners of Alberta and British Columbia.

⁵ See e.g. the [Binding Corporate Rules for controllers and processors \(BCR\)](#) and relevant [Article 29 Data Protection Working Party \(WP 29\) explanatory documents](#); [APEC Cross-Border Privacy Rules \(CBPR\)](#) and [APEC Privacy Rules for Processors \(PRP\)](#); ISO 27018 cloud data privacy standard, [ISO/IEC 27018:2014, Code of practice for protection of personally identifiable information \(PII\) in public clouds acting as PII processors](#); ISO data security standards, [ISO/IEC 27001, Information Security Management](#).

information age will empower organisations to continue to refine their transparency mechanisms, for example through innovative and user-friendly methods embedded in the technology itself, or through dashboards, portals, interactive apps and other mechanisms. As this new transparency becomes more a matter of customer relationship and trust, it will require cross-functional input and participation within organisations, as well as oversight that goes beyond legal and compliance departments.

However, in order for organisations to embrace and further develop this new function of transparency, this function must be recognised by the relevant legal regimes and regulators. In an era when there will be less opportunity for, and emphasis on, consent and more reliance on organisations to protect the individual without his or her input, new transparency is essential for creating the public trust that will enable this shift. Thus, new transparency is a matter of survival and success for both the data-driven economy and data-driven businesses. An informed public and informed regulators that understand the beneficial uses of personal information and trust the organisations using the information are less likely to be skeptical of such uses.

2. **Better risk assessment.** Risk management and the need to assess, understand and mitigate privacy risks to individuals is an integral part of organisational accountability. Risk management is becoming even more important in the era of big data and the IoT, as it enables organisations to achieve and go beyond privacy compliance while also enabling the beneficial uses of data.⁶ From formal privacy impact assessments and privacy by design for new products and services to consideration of risk and harm to individuals when deciding on appropriate security measures or whether to notify a data breach, organisations need to understand the benefits to the individual and society of proposed data processing as well as any risks to individuals. This is essential in order to implement and prioritise effective privacy protections and compliance measures internally. As such, risk management is one of the most important elements of organisational accountability. However, to fully realise this function of risk management, consistent and universally accepted methodologies for identifying and assessing both the benefits and risks of processing and for determining the appropriate mitigations and controls still remain to be developed.⁷
3. **Fair processing.** Fair processing has been a stand-alone data protection principle in many data privacy laws in Europe and beyond. For example, under the EU Data Protection Directive, the first principle of data processing is that data must be “processed fairly and lawfully”.⁸ However, often the interpretation and implementation of the “fair processing” principle has been limited to providing privacy notices to individuals. Fair processing, however, goes beyond providing privacy notices.

In its 2014 report on big data and data protection, the UK Information Commissioner’s Office elaborated helpfully on the concept of fair processing in the context of big data.⁹ The report

⁶ This is the subject of Paper 2 in this series: “Protecting Privacy in a World of Big Data – The Role of Risk Management”.

⁷ CIPL has been exploring such a methodology in its Privacy Risk Framework Project and has published the following two white papers on this subject: [“The Role of Risk Management in Data Protection”](#), 1 December 2014, and [“A Risk-based Approach to Privacy: Improving Effectiveness in Practice”](#), 19 June 2014. See also Paper 2 in this series, fn. 6 *supra*.

⁸ Directive 95/46/EC, fn. 3 *supra*, at Section I, Article 6.1(a).

⁹ UK ICO report on [“Big Data and Data Protection”](#), July 2014.

suggests that organisations should consider factors such as whether the proposed use of data was known or reasonably “expected” by individuals, whether it may result in “drawing conclusions or making decisions about individuals”, whether individuals were deceived or misled about how their data will be used, the impact of the proposed processing on the individual and the integrity and accuracy of data.

In the US, Section 5 of the Federal Trade Commission (FTC) Act prohibits “unfair” business practices.¹⁰ Under the FTC’s unfairness standard, business practices are unfair if they cause substantial consumer injuries that are not reasonably avoidable by consumers and not outweighed by countervailing benefits to consumers or competition.

Regulators and privacy practitioners in accountable organisations should refocus on this important principle and develop policies and procedures that operationalise this principle consistently throughout their organisations. The implementation of this principle will become tremendously helpful in the age of big data when enhanced accountability by organisations can enable and legitimise data uses in contexts in which individual consent is not possible or practicable.

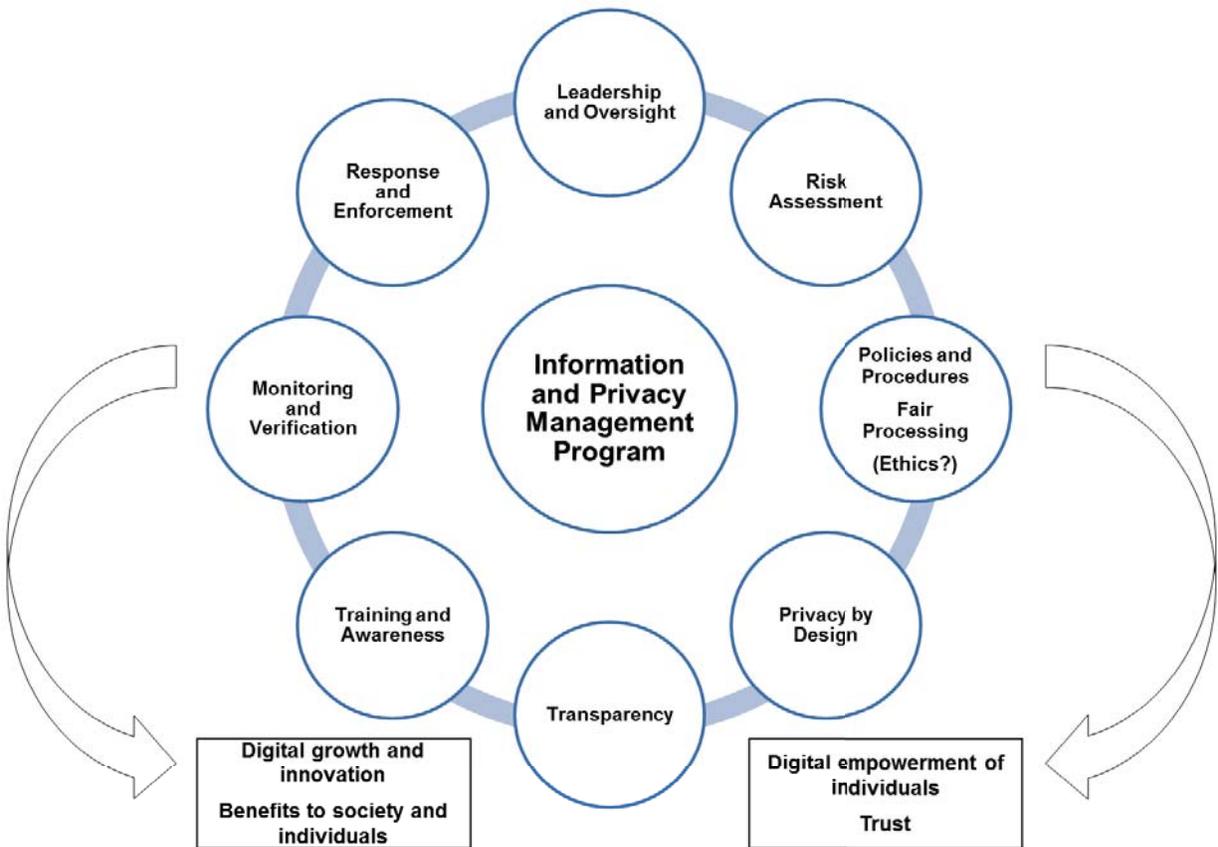
4. **Data ethics.** There is an increasing recognition that decisions on whether and how to process information must occur with reference to an appropriate ethical framework. This notion is encapsulated in the recent opinion of the European Data Protection Supervisor (EDPS) titled “Towards a new digital ethics”,¹¹ in which the EDPS calls for “developing an ethical approach to data protection” and announces the creation of an “Ethics Advisory Board” that will “help define a new digital ethics”. Of course, regardless of how the exploration of data ethics as well as this particular initiative develop, the elements of accountability and the tools for ethical decision-making on information uses will likely interrelate and overlap in many ways. For example, ethical considerations may be part of privacy by design or impact what harms we consider and how we weigh them in any privacy risk assessment, influence our selections of mitigations and controls, and inform our assessments of the benefits of specific data uses.¹²

¹⁰ 15 USC § 45(n).

¹¹ EDPS, [Opinion 4/2015, “Towards a new digital ethics: Data, dignity and technology”](#), 11 September 2015.

¹² Early work on this issue is underway also outside of the EDPS. See e.g. the Information Accountability Foundation’s [Big Data Ethics initiative](#) and [The case for data ethics](#), Accenture Outlook.

**ENHANCED ACCOUNTABILITY
ENABLES EMPOWERMENT OF THE INDIVIDUAL AND BENEFICIAL DATA USE**



Information management programs based on the elements of enhanced organisational accountability will create sustainable virtuous cycles of data contribution and benefit creation that maximise both privacy and effective use of data, thereby unlocking the full potential of the modern information age.

IV. Enhanced Accountability as Enabler of a Sustainable Digital Society and Economy

An organisation that adopts and demonstrates its commitment to enhanced accountability is sending a clear signal on its commitment to data privacy and security. This is partly a matter of policies, procedures and practices, but also a matter of culture, brand and reputation and how the organisation wants to be perceived by its customers, suppliers, employees, investors and regulators. There is no “one-size-fits-all” formula for implementing this next generation of accountability. Each organisation must find its own way to embed, implement and communicate its approach to organisational accountability and the responsible use of information.

To better understand its benefits, it is helpful to examine this enhanced accountability not just in terms of its essential elements and requirements, but also in terms of its specific “deliverables”. All these deliverables are necessary for creating a sustainable digital economy and all are relevant to both the private and public sectors. Enhanced accountability can enable:

- (1) “interoperability” between privacy regimes to support cross-border data transfers;
- (2) organisational compliance with local privacy requirements;
- (3) effective privacy protections, exceeding the required minimum where appropriate;
- (4) a flexible framework for responsible, trustworthy and ethical information processing;
- (5) flexible application of privacy principles in light of technology developments; and
- (6) effective regulatory oversight and enforcement and public/private coordination.

1. Enhanced Accountability as an Interoperability Bridge and Enabler of Cross-Border Data Flows

Enhanced accountability can serve as an interoperability bridge between different legal regimes and enable cross-border data flows in two ways.

First, a company’s internal privacy program based on the elements of accountability allows it to align its privacy policies and practices with the various requirements of the different jurisdictions in which it does business. The company thus creates a practical bridge and convergence between different legal requirements by setting a uniform and high level of privacy protection, policies and procedures for the company across multiple jurisdictions or even globally.

Second, existing certified accountability schemes, such as the EU BCR and the APEC CBPR¹³, enable cross-border data transfers. They are designed to meet an agreed privacy standard of multiple jurisdictions, or to serve as a recognised cross-border transfer mechanism in jurisdictions that impose certain data transfer restrictions in their privacy laws.¹⁴

There is enormous untapped potential for accountability-based schemes to serve as a bridge between different legal regimes. For example, BCR, CBPR and similar schemes could be made interoperable with each other¹⁵ and serve as a model for creating a truly global accountability-based data transfer scheme. Certainly, global organisations are interested in such schemes. The more local compliance issues and cross-border transfer restrictions can be addressed through a single accountability-based system or a set of coordinated and interconnected systems, the better for companies and for their customers and regulators.

¹³ See *supra* at fn. 5.

¹⁴ For example, Australia’s privacy law, fn. 3 *supra*, allows for “binding schemes” that ensure that the recipient of Australian personal data protects the data at the Australian level. The CBPR or BCR are such a binding scheme. Guidance by the Hong Kong Privacy Commissioner on cross-border data transfers, *id.*, provides for various options based on “due diligence” that could include contracts or “non-contractual oversight means” (presumably, such means include CBPR) by which an organisation can ensure that data remains protected at the Hong Kong level after transfer. Singapore’s Personal Data Protection Regulations, *id.*, provide for the use of binding corporate rules for cross-border data transfers.

¹⁵ In fact, there is an ongoing effort between the European Union’s Article 29 Data Protection Working Party and the APEC Data Privacy Subgroup to develop tools to make it easier for companies that seek approval under both the BCR and CBPR.

2. Enhanced Accountability as an Enabler of Legal Compliance

Implementing an accountability-based program, whether certified or not, helps companies ensure and prove local law compliance. This is because such programs implement either local legal requirements or a formally recognised code of conduct or similar scheme that is recognised by multiple countries on the basis that it is substantially consistent with their own local legal requirements. As a result, implementing such programs improves legal certainty for companies and goes a long way towards compliance with the applicable local legal requirements. Also, because accountability-based schemes require an internal compliance infrastructure, including written policies and other documentation, they enable the company to verify and demonstrate its accountability and compliance in the event of an investigation or enforcement action.¹⁶

3. Enhanced Accountability as an Enabler of Proactive Privacy Protections

Accountability-based programs also create an environment or infrastructure for organisations to proactively implement strong and effective privacy protections for individuals that in some instances even go above and beyond applicable legal requirements, including in contexts in which no privacy laws exist at all. For example, many accountable organisations voluntarily apply internal security breach reporting and response practices even in countries where there is no legal requirement to notify the breaches. Similarly, some organisations voluntarily extend the right of access to all its customers and employees, even when there is no strict legal obligation to do so. Finally, some organisations might certify to the APEC CBPR even in countries where the privacy protections of the scheme exceed those found in any domestic laws. Thus, organisational adherence and implementation of accountability schemes through privacy programs are more likely to result in effective privacy protection for individuals and are, therefore, also bound to improve consumer trust and be attractive to potential business partners. For example, a data processor might distinguish itself from its competitors by participating in BCR for Processors or the newly created APEC Privacy Recognition for Processors (PRP). Finally, accountability and cross-border schemes that go beyond local legal requirements contribute to the international convergence of privacy protections and norms. Such convergence will benefit businesses, individuals and regulators alike.

4. Enhanced Accountability as an Enabler of Trustworthy Big Data

Today's advanced technology causes much of data processing to occur outside the knowledge and awareness of the public. This reality challenges the established interpretation of traditional privacy principles that emphasise notice and consent. However, enhanced organisational accountability will create the necessary trust among the public and regulators that organisations will process personal data responsibly in the absence of direct individual involvement and thus enable organisations to implement these principles in more flexible and meaningful ways that are appropriate for the context at hand. As such, enhanced accountability is a real enabler of our digital society and the *sine qua non* of truly realising the benefits of big data where it relies on personal information, for example in the area of personalised medicine.

¹⁶ Of course, it may be the case that certain local requirements are not covered by a formal, multilateral accountability scheme and, therefore, must be addressed by an organisation outside of the scheme. Indeed, the CBPR specifically allow for such add-on obligations based on local variation. But this does not substantially diminish the fact that accountability schemes simplify and streamline compliance management and, therefore, enhance the likelihood of local compliance.

As explained, without the tools and mechanisms to earn public trust, legitimate uses of information may fall victim to unnecessary opposition and restrictions. At a time when more and more organisations as well as society at large are discovering the enormous untapped commercial and societal value of the personal data they hold and are searching for ways to use it legitimately, it is essential that they employ tools that ensure they do so in a responsible, transparent and ethical manner and subject to the appropriate privacy controls. Enhanced accountability is such a tool. It enables a clear understanding of both the risks and benefits of particular data uses, as well as effective communication to the public of the intended benefits and possible tradeoffs of such uses, so that the public is fully aware and in a position to accept the value exchange that takes place between businesses and individuals.

5. Enhanced Accountability as Enabler of Flexible Application of Privacy Principles

If they are to remain relevant in the era of big data and the IoT and the growing collection and use of information associated with them, traditional privacy principles such as notice, consent, purpose specification and collection limitation must be open to flexible, context-specific and creative interpretation and implementation. For example, the principle of “notice” must be re-conceptualised to a broader vision of transparency that enables individuals to better understand and accept the exchange between them and the organisations that use their data even where specific consent is not possible. Also, where specific consent is not feasible, the concept of “legitimate interest” processing can be used to accomplish the same underlying goal of empowering and protecting the individual.¹⁷ Thus, in many modern information use contexts, the goals of traditional privacy principles of empowering individuals and protecting their legitimate privacy interests must be accomplished through new interpretations and alternative mechanisms. Enhanced accountability enables such new interpretations and mechanisms. It helps organisations to apply privacy principles flexibly and contextually while also effectuating the fundamental goals of data protection.¹⁸

6. Enhanced Accountability as an Enabler of Regulatory Oversight and Public/Private Coordination

It is not surprising that regulators and privacy enforcement authorities around the world are increasingly embracing the concept of accountability as well as various specific accountability-based schemes. Data privacy authorities are charged with enforcing existing privacy laws, but often with limited budgets and personnel resources. Accountability schemes, in which a third-party certifying organisation has front-line implementation and “enforcement” responsibility, can augment and extend the limited capacity and reach of data privacy authorities.¹⁹ Enhanced accountability will be even better positioned in that regard.

Privacy regulators and enforcement authorities also need to cooperate with their counterparts across borders in an increasing number of cases. Cooperation is usually possible only when there is agreement on the underlying principle that is being vindicated. In recognised cross-border schemes based on the elements of accountability or, in the future, enhanced accountability and digital responsibility, that

¹⁷ See a more detailed discussion of this point in Paper 2 in this series on Protecting Privacy in a World of Big Data, entitled “Protecting Privacy in a World of Big Data – The Role of Risk Management.” See also Bojana Bellamy, Markus Heyder, [“Empowering Individuals Beyond Consent”](#) (IAPP Privacy Perspective, 2 July 2015).

¹⁸ See also Paper 3 in this series on Protecting Privacy in a World of Big Data entitled _____ (forthcoming).

¹⁹ For example, much of everyday complaint handling, small-scale consumer disputes and failures to comply with applicable requirements might never get resolved or rise to the attention of an enforcement authority, but will get resolved within the context of an accountability scheme that provides for complaint handling and dispute resolution.

agreement is inherently present. Therefore, such schemes directly enable and improve cross-border privacy enforcement cooperation and, ultimately, privacy protections for individuals.

Moreover, privacy enforcement authorities often investigate factually complex matters. It is in an organisation's best interest to be able to provide clear and understandable documentation of the conduct under investigation. Accountability requires comprehensive internal privacy programs and the ability to provide that information to regulators and enforcement authorities on request. This "investigation readiness" helps not only the authorities but also the organisation under investigation.

Finally and importantly, in the same way that enhanced accountability enables a more flexible and thus effective interpretation and application of privacy principles by organisations, it also enables such flexible and more effective interpretation by regulators and privacy enforcement authorities. However, it is important to develop a common and coordinated approach between organisations and regulators to the flexible application of traditional privacy principles through the lens of enhanced accountability.

V. Conclusion

Adhering to enhanced accountability and implementing information management programs based on the elements of accountability facilitates the free flow of data across borders; creates practical bridges across diverging legal regimes; enables legal compliance, proactive privacy protection, public trust and more effective interpretations of privacy principles; and supports oversight, enforcement and effective coordination between regulators and businesses. All these "deliverables" of enhanced accountability are prerequisites for maximising both the effective use of personal data and the protection against privacy harms in the modern information age. By adopting and implementing enhanced accountability as a matter of organisational culture, organisations put themselves in a position to be trusted to use personal information in a way that is truly commensurate with the modern information age.

Appendix C

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 Privacy 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 both negative 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.