Centre for Information Policy Leadership
Hunton & Williams LLP

DISCUSSION DRAFT 21 October 2015

# 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 proposals[3], elaborated upon by data protection authorities in regulatory guidance[4],

[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 organisations[5], 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 Albert 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.

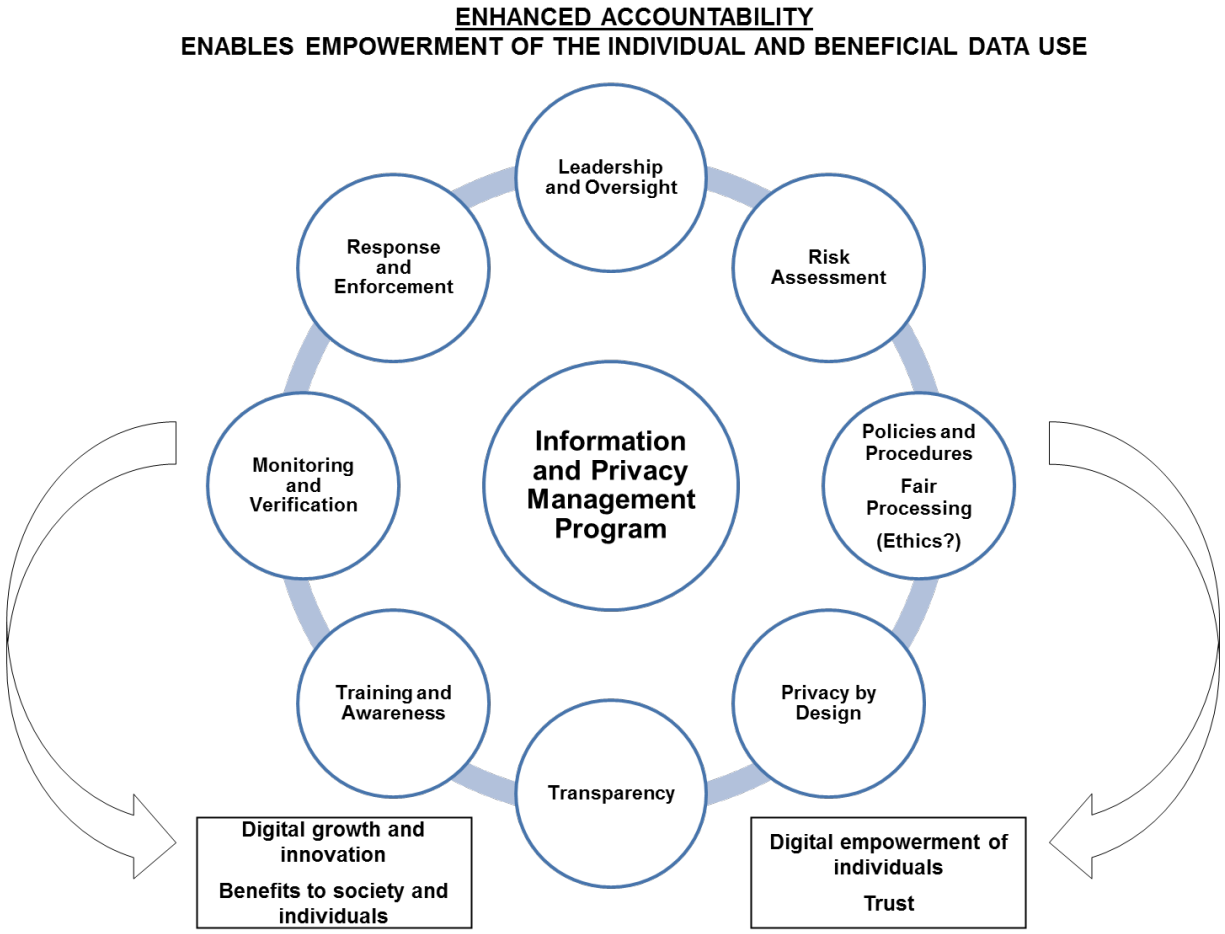
Regulators and privacy practitioners in accountable organisations should refocus on this important principle and develop policies and procedures that operationalise this principle consistently throughout their organisations. The implementation of this principle will become tremendously helpful in the 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.




*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 CBPR[13], 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 other[15] 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.