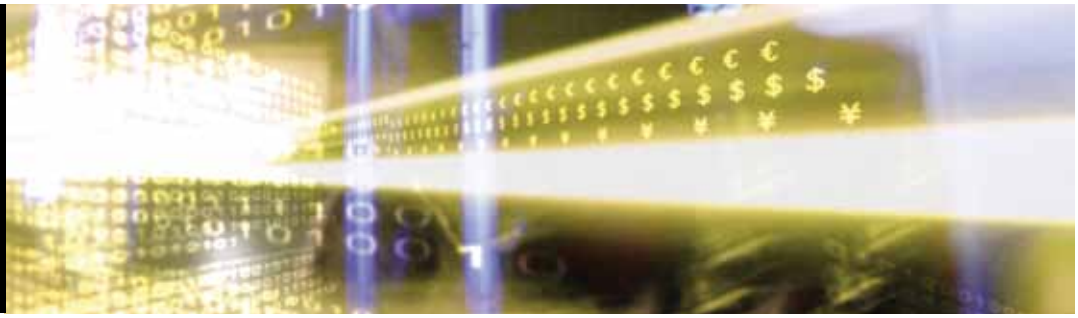
THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP



Implementing Accountability in the Marketplace
A Discussion Document

Accountability Phase III - The Madrid Project
November 2011

Prepared by the Centre for Information Policy Leadership
as Secretariat to the Madrid Project

Preface

Martin E. Abrams
Centre for Information Policy Leadership

Since its work began in 2009, the Accountability Project has described an innovative, 21st century approach to data protection. Accountability builds on traditional notions of fair information practices, but incorporates new elements that require organisations to implement comprehensive privacy programmes and base their decisions about data on credible assessment of the risks they raise for individuals and how best to mitigate them. It has articulated the conditions that must exist in an accountable organisation – conditions that organisations must be able to demonstrate and that regulators can measure.

Over the last three years, accountability has figured prominently in data protection policy development around the world. In the European Union, the work of the Article 29 Working Party referenced accountability in its submission to the Commission's consultation on changes to the Directive, and issued an opinion on accountability. Accountability has been reflected in policy instruments issued in the United States, and data protection agencies in Canada have embarked on a project to define their expectations of accountable companies. In Mexico, new data protection laws and regulations incorporate accountability. At the Asia Pacific Economic Cooperation forum, work is underway to design a mechanism based on accountability that would bridge approaches to data protection taken in different countries. In response to these advances in public policy, many companies have taken important steps toward implementing an accountability programme.

This year, the Project responded to suggestions in public policy discussions that accountability, in order to be effective, must be required across the marketplace. Participants considered what would be required of organisations in such circumstances, and what benefits the approach would offer as a result of such broad implementation. They further explored the requirements and benefits of accountability when formally recognised by a third party.

While this progress is encouraging, a great deal of work remains if accountabiity is to serve as an effective solution for data protection and privacy. Data protection authorities and agencies, organisations and third-party accountability agents will need to implement programmes and procedures to support accountability, and the practical aspects of how that infrastructure might work requires further exploration. Questions remain about how organisations will establish the validity of the statements they provide to demonstrate their accountability. More work is also needed to determine the nature of the relationship between data protection authorities necessary to resolve cross-border privacy issues, and to better understand the appropriate role and level of authority of third-party accountability agents. As the Project has considered accountability in greater detail, reaching consensus on all issues has become more challenging.The document references areas where differences remain and additional work is necessary.

The Centre for Information Policy Leadership at Hunton & Williams has been privileged to serve as secretariat for the Project, and developed this paper to document the third year of its work. As in past years, the Project has benefited from an international group of experts from business, government, data protection and regulatory agencies, and the advocacy community. The Centre is particularly grateful and encouraged by the active participation of data protection commissioners and privacy regulators from Canada, France, Germany, Hungary, Ireland, Israel, Italy, the Netherlands, New Zealand, Spain, the United Kingdom and the United States, as well as the European Data Protection Supervisor. Their active and ongoing involvement highlights the global concern about this issue.

The Centre would like to thank the Spanish Data Protection Agency for graciously facilitating the February and June meetings in Madrid, and the United States Federal Trade Commission for hosting the meeting held in Washington, DC, in March. Their insights and counsel as we planned meetings and drafted this document were invaluable to the success of this year's work. We thank all of the experts for their thoughtful contributions to the discussions and for their generous review and critique of this document. While Centre staff developed this document, the paper reflects the work of many people who contributed ideas and kindly reviewed drafts. However, it does not necessarily reflect the views of any participant, and the Centre alone is responsible for any errors that may remain.

Executive Summary

The Accountability Project entered its third year aware of the growing understanding, both within the Project and in public policy discussions, that to be most effective, an accountability approach to data protection should be explicitly required across the marketplace.

If all organisations were required to be accountable, all would implement privacy programmes proportional to the size, sensitivity and complexity of their data holdings and business models. Such broad application of accountability promises benefits to individuals, the market, and organisations. While the principles of accountability would apply to all organisations, their implementation would be custom designed – tailored to the size, sensitivity and complexity of their data holdings, their business models, and applicable law and regulation.

Accountable organisations will share several common characteristics. All accountable organisations will:

- Adopt privacy policies consistent with commonly accepted external criteria – applicable law, regulation, and recognised guidelines;
- Implement mechanisms to put those policies into effect and communicate them to individuals;
- Integrate privacy protections into corporate governance;
- Put in place an internal oversight programme; and
- Be prepared to demonstrate to a regulator its commitment to accountability and its capacity to provide necessary data and privacy protections by providing evidence, when asked, that it has implemented each of the elements described above.

Broad application of accountability promises benefits to individuals, the market, and organisations. Accountability is envisioned to:

- Heighten the confidence of individuals and organisations that their data will be protected regardless of where or by whom it is stored or processed;
- Lead to higher levels of compliance;
- Enhance data protection efficiency by allowing regulators to focus their resources on activities that raise the greatest risk to individuals;
- Improve the quality of data protection by allowing organisations to use and update tools that best respond to specific risks;
- Better position regulators to police the marketplace against activities that fall outside law, regulation and guidance through more efficient resource allocation;
- Create an expectation in the marketplace that organisations will act in accordance with the requirements of accountability; and
- Bridge data protection regimes across jurisdictions, allowing countries and regions to pursue common data protection objectives through different but equally reliable means.

While all organisations would be required to be accountable, in certain cases, when they wish to enjoy enhanced benefits or engage in certain activities, organisations might choose to take additional steps to establish their status as having attained *recognised accountability.* Recognised accountability requires that an organisation meet all of the requirements, as articulated in the essential elements, for accountability. It must also take additional steps to provide evidence and documentation that it has fulfilled the essential elements *before* status as recognised is granted. An organisation seeking recognised accountability would be required to provide:

- A description of its internal privacy and data protection policies, and evidence that those policies have been approved by the appropriate authority within the organisation;
- A description and evidence of the programmes it has put in place to implement its policies;
- A description of the manner in which it has incorporated privacy and data protection into its corporate governance, and measures or metrics by which the success of its incorporation can be assessed; and

- A description of the procedures it has implemented to oversee the effectiveness of its privacy and data protection programme, including metrics related to monitoring.

An organisation that is recognised as accountable would be expected to enjoy the following benefits:

- Relief from certain administrative regulatory requirements or administrative burdens;
- Appropriate consideration of recognised status in the context of an enforcement action;
- A consultative relationship with third-party accountability agents that allows for appropriate remediation processes/opportunities prior to enforcement actions;
- Recognition of the integrity of programme design by the appropriate supervisory authority; and
- Competitive advantage by signaling to the market its enhanced commitment to privacy and data protection.

Every organisation, whether or not it has been recognised as accountable, will be subject to oversight by a regulatory authority and/or its appointed accredited agent. The reasons for which an authority may initiate an inquiry, and the showings required in response are as follows:

As part of a random check of accountability. An accountable organisation will be required to provide a description of its:

- Internal policies based on external criteria;
- Programme that implements its internal policies;
- Integration of its privacy protection programme into overall organisation governance; and
- Privacy and data protection oversight programme.

Pursuant to an investigation of a suspected or actual privacy or data protection failure. An organisation will be required to provide:

- A description of its internal policies linked to external criteria as they apply to the area of the enterprise under investigation;
- A description of its programme implementing its privacy policies, and evidence that the programme has been implemented;
- Evidence of how it has integrated privacy and data protection into corporate governance, and meaningful metrics to demonstrate the extent of such integration; and
- A description of its oversight programme as it applies to the data activities under investigation, and metrics about that monitoring.

As follow-up to an enforcement action. An organisation will be required not only to provide evidence of its privacy and oversight programmes (as in the case of an investigation of a suspected privacy or data protection failure, above), but also to have those aspects of its privacy initiative validated by a third party.

Introduction

Since 2009, the Accountability Project (“the Project”) has engaged in an ongoing discussion about an approach to data and privacy protection that would take into account the rapid pace of technology innovation; ubiquitous collection, analysis and processing of data; powerful analytics; and global flows of information that support the information economy. The Project recognised that in this data environment, organisations must deploy effective programmes to protect individuals against the risks that the use of information may create. While individuals must continue to play an appropriate role in making choices about the use and sharing of data pertaining to them, choice must be meaningful, taking into account complex technologies, business models and data uses. At the same time, organisations need to be able to process and analyse data in creative, innovative ways that enable them to respond quickly to customer and marketplace requirements.

The Project has described *accountability* as an approach that requires companies to implement programmes that foster compliance with data protection principles and to be able to explain how those programmes provide the required protections for individuals. Accountability obligates organisations to take responsibility for the safe and appropriate processing and storage of data, wherever it occurs. It requires them to implement effective data and privacy protection policies that correspond to accepted external criteria found in law, regulation and industry best practices. Accountability asks that organisations analyze

and understand the risks that data use raises for individuals, and take necessary and appropriate steps to mitigate those risks. It further requires that organisations make judicious decisions about data use, even when traditional individual consent or choice may not be available.

The accountability principle is not new. It is a feature of both the earliest of the major international instruments on privacy, the Organisation for Economic Cooperation and Development's Privacy Guidelines,[1] published in 1980, and the most recent, the Asia Pacific Economic Cooperation's Privacy Framework,[2] endorsed in 2004. Both state that organisations "should be accountable for complying with measures that give effect" to the fair information practices articulated in the respective guidelines. It is also the first principle in Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"),[3] and has traditionally played a role in implementation of privacy processes in the European Union.[4]

New approaches currently under consideration significantly rely on accountability as a means to ensure the protection of data. "The Future of Privacy,"[5] the joint paper of the European Union Article 29 Data Protection Working Party and the Working Party on Police and Justice, notes the significance and utility of the accountability principle, and cites the challenges to data protection raised by globalization and new technologies as offering an opportunity to "innovate the current legal framework by introducing principles such as accountability." In a later Opinion on accountability[6] submitted to advise the European Commission about how to amend the Data Protection Directive, the Article 29 Working Party defined a statutory accountability principle to "explicitly require data controllers to implement appropriate and effective measures to put into effect the principles and obligations of the Directive and demonstrate this on request."

This document is the third in a series of papers issued by the Accountability Project. The first, released in October 2009,[7] articulated the essential elements that an organisation must adopt in order to be accountable.[8] It stated that an accountable organisation demonstrates commitment to accountability, implements data privacy policies linked to recognised external criteria, and implements mechanisms to promote responsible decisions about the management and protection of data. Such external criteria include applicable law, regulation, and recognised external guidelines. The paper further stated that accountability requires that organisations design and implement comprehensive data and privacy protection programmes[9] based on analysis of the risks data use raises for individuals and on responsible decisions about how those risks can be appropriately mitigated.

The second paper, issued by the Project in October 2010,[10] examined how organisations demonstrate accountability and how regulators measure it. The paper proposed fundamental conditions that accountable organisations should be prepared to establish and demonstrate to regulators.[11] It further considered how, and under what circumstances, regulators, data protection authorities, and their designated agents would measure accountability. The paper noted that accountability is not a one-size-fits-all approach: both organisations and regulators must be able to implement and measure the fundamentals in a manner suitable for the organisation, its business model, and the way it collects, uses and stores data.

---

[1] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,3343, en_2649_34255_1815186_1_1_1_1,00.html.

[2] APEC Privacy Framework, http://www.ag.gov.au/www/agd/rwpattach.sf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf.

[3] This governance was explicitly described in a 2009 publication of the Office of the Privacy Commissioner of Canada, "Processing Personal Data Across Borders: Guidelines." http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.cfm. In PIPEDA, accountability is an overarching principle that applies to protection and management of data, whether it is maintained and processed domestically or transferred outside Canadian borders for storage and processing.

[4] Paragraph 19 of the Article 29 WP "Opinion 3/2010 on the principle of accountability" (adopted on 13 July 2010, 00062/10/EN, WP 173) cites Binding Corporate Rules used in the context of international data transfers as reflecting the accountability principle. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf.

[5] http://www.garanteprivacy.it/garante/document?ID=1707337.

[6] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf.

[7] "Data Protection Accountability: The Essential Elements - A Document for Discussion," October 2009, http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf.

[8] The essential elements articulated by the Accountability Project are: 1) Organisation commitment to accountability and adoption of internal policies consistent with external criteria; 2) Mechanisms to put privacy policies into effect, including tools, training and education; 3) Systems for internal, ongoing oversight and assurance reviews and external verification; 4) Transparency and mechanisms for individual participation; 5) Means for remediation and external enforcement. The essential elements are described in more detail in Appendix A.

[9] The essential elements of accountability require that such programmes be designed to implement privacy policies linked to established external criteria.

[10] "Demonstrating and Measuring Accountability: A Discussion Document," http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.pdf.

[11] The Accountability Project identified nine common fundamentals that an accountable organisation should implement: 1) Policies; 2) Executive Oversight; 3) Staffing and Delegation; 4) Education and awareness; 5) Ongoing risk assessment and mitigation; 6) Program risk assessment oversight and validation; 7) Event management and complaint handling; 8) Internal enforcement; 9) Redress. The fundamentals are described in detail in Appendix B.

The discussions of this second phase of the work on accountability reflected a growing appreciation that for an accountability approach to data protection to be most effective, accountability should be explicitly required across the marketplace. All organisations would be required to implement privacy programmes proportional to the size, sensitivity and complexity of their data holdings and business models. Such broad application of accountability promises benefits to individuals, the market, and organisations. In certain cases, however, when they wish to enjoy enhanced benefits or engage in certain activities, organisations might choose to be formally recognised as accountable. In such instances, organisations would likely take additional steps to establish their status as having attained recognised accountability.

In 2011, the Centre for Information Policy Leadership, through a process facilitated by the Spanish Data Commissioner, convened the third international discussion about the architecture and implementation of an accountability approach to data governance – this time to focus on questions pertaining to what is required of accountable organisations, and what additional steps are required of organisations that wish to be recognised as accountable. Participants considered these issues at three meetings, held in Madrid and Washington, DC. They discussed the benefits that would accrue to the marketplace, individuals, regulators and organisations as a result of broad implementation of an accountability requirement. They also articulated what would be required of organisations seeking to attain *recognised accountability*, and the discrete, specifically identifiable benefits they would enjoy.

Participants in this phase of the Project – international experts from government, regulatory agencies, industry, academia and civil society – identified a drafting committee that oversaw Centre staff as they prepared this document, which was circulated later for comment among all participants. This paper is the result of that process.

Accountability Applied Across the Marketplace

Requirements

Accountability is built upon the essential elements described in the paper issued by the Project in 2009.[12] Accountable organisations establish data and privacy-protection policies consistent with commonly accepted external criteria and deploy programmes to carry out those policies. They rely on identification and mitigation of risks to individuals as the basis for their judgment about which measures will best protect data.

While the principles of accountability would apply to all organisations, their implementation would be custom-designed. Organisations will tailor their privacy programmes to their business model; the nature and size of their data holdings; the technologies and applications they deploy; and the risks data and its applications pose to the rights and freedoms of individuals. One size does not fit all, and the rigor, breadth and detail of an organisation's privacy programme will correspond to the risks to the rights and freedoms of individuals raised by data and its applications, as assessed by the organisation. While certain fundamentals may be found in data protection programmes, all measures will not necessarily apply to all organisations in every instance.[13] Moreover, the privacy programme may vary across an organisation. Some aspects of the organisation may process large quantities of sensitive data; others may deal only with non-sensitive information. The organisation also may implement different programmes to address the privacy risks raised by use of different kinds of data.

All programmes, however, would share several common characteristics.[14] First, accountable organisations would adopt privacy policies consistent with commonly accepted external criteria – applicable law, regulation, and recognised external guidelines. Such policies would also reflect the organisation's values and promises it has made to individuals.[15]

Second, accountable organisations would implement mechanisms to put policies into effect and communicate those policies to individuals. Mechanisms would include processes to assess, manage and mitigate the privacy risks created by data use; employee training; and the means to manage data events such as breach, inappropriate access, or failure to meet the obligations of the privacy policy.

Third, accountable organisations would integrate privacy protections into governance and apply them across all aspects of the organisation where they are relevant. Their policies would enjoy the support and commitment of executive management.

[12] See fn. 6 and Appendix A.

[13] The fundamentals proposed by the Accountability Project would serve as a toolbox for organisations as they develop their privacy programmes. In its "Opinion 3/2010 on the principle of accountability," the Article 29 Working Party suggests a similar approach, and offers an example of such a custom-designed programme. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf. Actual programmes will be designed appropriate to the nature of the organisation and its enterprise, as discussed elsewhere in this paper.

[14] In some jurisdictions, the specifics of an organisation's implementation of accountability mechanisms will be reflected in binding contracts.

[15] Ideally, an organisation's privacy policies will be consistent with policies it implements to address other risks, *e.g.,* security risks, and overarching policies of the business.

The organisations would designate a person or persons at an appropriately senior level to be responsible for privacy and data protection initiatives throughout the organisation.[16] Such person or persons would be provided sufficient staffing and resources to effectively implement the organisation's privacy and data protection policies.

Fourth, accountable organisations would put in place an internal oversight programme. Accountability requires effective oversight of the privacy programme by the individual or team responsible for privacy, and an internal monitoring and assessment process to assure that it fosters sound decisions about data use and effective protections. In addition, accountable organisations would oversee and raise awareness of third-party vendors and suppliers with whom they do business to ensure that they are meeting the obligations created by law, regulation and the organisation's privacy promises to its customers.

Finally, organisations adhering to requirements of accountability would be prepared to demonstrate to a regulator their commitment to accountability and their capacity to provide necessary data and privacy protections. They would do so by providing evidence, when asked, that they have implemented each of the elements described above.[17]

In many cases, organisations would design and build programmes to address their specific situation. This may especially be the case for large, complex and well-established companies that are deeply familiar with the data protection issues confronting their enterprise and the marketplace. In other instances (particularly for small- and medium-sized enterprises), industry associations may develop and offer models for privacy programmes that companies may tailor to their needs. In every instance, however, programmes that meet the requirements of general accountability would adopt privacy policies linked to commonly-accepted external criteria, programmes and processes to put those policies into effect, internal oversight and assurance review to determine whether privacy programmes are effective, and metrics that enable the organisation to demonstrate their accountability when asked to do so.

Benefits of Accountability Adopted Across the Marketplace

When required across the marketplace, accountability promises benefits to individuals, businesses, the market and regulators. Accountability is expected to:

- Heighten the confidence of individuals and organisations that their data will be protected wherever and by whomever it is stored or processed;
- Lead to higher levels of compliance by explicitly requiring organisations to implement comprehensive programmes that put into effect data protection principles, and to stand ready to demonstrate the capacity of those programmes to foster responsible use, management and protection of data;
- Enhance data protection efficiency by allowing regulators to focus their resources, oversight and enforcement on those activities that create the most risk for individuals;
- Help organisations improve the quality of data protection by allowing them to use tools that best respond to specific risks, and to rapidly update those tools to quickly meet the requirements of new business models and emerging technologies;
- Better position regulators to police marketplace participants whose activities fall outside the bounds of law, regulation and recognised guidance, by enabling them to direct limited resources toward organisations that have not established their accountability or that fail to comply;
- Create an expectation in the marketplace – for business partners, commercial vendors and individuals – that organisations will operate in accordance with the requirements of general accountability, that will drive organisations toward accountable practices; and
- Bridge data protection regimes across jurisdictions, by allowing countries and regions to pursue common data protection objectives through different but equally reliable means.

Recognised Accountability

While all organisations will be required to be accountable, in some cases, organisations may choose to take steps to be *recognised* as accountable.

[16] An organisation will designate a senior person or persons responsible for privacy and data protection as appropriate to the structure of the organisation.

[17] What an accountable organisation must show is discussed in detail in the section, "Responding to Official Oversight," of this document.

An organisation may adopt or deploy a new technology, application, or process, and may wish to be recognised as doing so in an accountable manner. It may wish to seek recognition for business or competitive reasons. It may wish to transfer data across borders for business processing, and want recognition that it has engaged in the appropriate risk assessment and mitigation and is implementing appropriate protections. In these and other cases, an organisation may seek recognised accountability.

Benefits to Organisations

While general adoption of accountability yields benefits to organisations, regulators, the market and individuals, companies that take the initiative to attain recognised accountability must realise discrete, identifiable benefits over and above these. Organisations will need to make investments – sometimes significant – to attain and maintain recognised accountability, and will need to experience recognisable advantages to justify the additional costs incurred.

It is envisioned that organisations that are recognised as accountable would enjoy certain benefits, including:

- Relief from certain administrative regulatory requirements or administrative burdens (*e.g.,* approval to transfer data across borders, model contracts, individual notification requirements);[18]
- Appropriate consideration of recognised status in the context of an enforcement action;
- A consultative relationship with third-party accountability agents that allows for an appropriate remediation process/opportunity prior to an enforcement action;
- Recognition of the integrity of programme design by the appropriate supervisory authority; and[19]
- Competitive advantage, by signaling to the market the organisation's enhanced commitment to privacy and data protection.

Requirements

Recognised accountability requires that an organisation meet all of the requirements for general accountability, based on the essential elements and as described above.

In addition to fulfilling the requirements of accountability, an organisation seeking recognition would be required to provide evidence and documentation of its fulfillment of the essential elements.[20] An organisation seeking recognised accountability would be required to provide:

- A description of its internal privacy and data protection policies, and evidence that those policies have been approved by the appropriate authority within the organisation;
- A description and evidence of the programmes it has put in place to implement its policies;
- A description of the manner in which it has incorporated privacy and data protection into its governance, and measures or metrics by which the success of its incorporation can be assessed;[21] and
- A description of the procedures the organisation has implemented to oversee the effectiveness of its privacy and data protection programme, including metrics related to monitoring.[22] The organisation could also provide evidence of the review of the oversight mechanism through validation by an independent auditor, regulator or third party agent.[23]

[18] Relief from administrative regulatory requirements would only be possible insofar as it is provided for by law.

[19] Not all data protection and privacy laws currently in place are sufficiently flexible to enable organisations that attain recognised accountability to enjoy these benefits.

[20] Some data protection authorities participating in the Project believe that recognition of an organisation as accountable must involve the data protection authority and occur before any benefits take effect. Others believe that self certification is possible and believe that third party accountability agents can provide the necessary assurances so that an organisation can enjoy benefits of recognised accountability. This question requires further exploration by this Project.

[21] Such metrics could include by whom and at what level in the organisation the privacy strategy and programme is reviewed; and where and at what level within the organization hierarchy the person responsible for privacy is placed.

[22] Such metrics of monitoring could include statistics about how often certain activities are reviewed; how often the organisation assesses the efficacy of its programme; an assessment of the quality of the decisions it yields; and how frequently the organisation revisits its risk assessment and mitigation strategy, particularly when new products and services are offered.

[23] European Binding Corporate Rules require that organisations and data protection authorities come to agreement about common binding references that define what is expected of organisations.

Such validation may be carried out by an independent party within the organisation, or by a third party validation agent.[24]

Type of Accountability	Internal Policies	Implementation Programme	Privacy Governance	Oversight
Accountability				
All companies would	- Develop internal policies based on external criteria - Be prepared to provide evidence of approval by appropriate internal authority	- Implement the policies - Be prepared to provide evidence of implementation	- Develop a governance programme - Be prepared to provide evidence of governance	- Develop an internal oversight programme - Be prepared to provide evidence of internal monitoring and review
Recognised Accountability				
Companies seeking and demonstrating recognised status from regulator or third-party agent would	- Provide description of internal policies based on external criteria - Provide evidence of approval by appropriate internal authority	- Provide description of implementation programme - Provide evidence of implementation	- Provide description of governance programme - Provide metrics related to governance	- Provide description of oversight programme - Provide metrics related to monitoring - Provide evidence of review by independent auditor, regulator or third party agent

Responding to Official Oversight

Every organisation, whether or not it has been recognised as accountable, will be subject to oversight by a regulatory authority and/or their appointed accredited agent. Such authorities may initiate an inquiry for a number of reasons.

Authorities may initiate an inquiry about an organisation's accountability as part of a *random check of accountability*. In such cases, organisations will be required to provide a description of its implementation of the four elements of accountability – its internal policies based on external criteria; privacy and data protection programme; integration of its privacy protection programme into overall corporate governance; and privacy and data protection oversight programme.

Authorities also may initiate an inquiry *pursuant to an investigation of a suspected or actual privacy or data protection failure*. In response to such an inquiry, organisations can be expected to be required to provide a number of things relative to the area of enterprise under investigation.

An organisation could be asked to describe its internal policies linked to external criteria, as they apply to the area of the enterprise under investigation. It may be required to provide not only a description of its programme implementing its privacy policies, but also evidence that the programme has, in fact, been implemented. The organisation may provide evidence of how it has integrated privacy and data protection into corporate governance, and provide meaningful, reliable metrics to demonstrate the extent of such integration. Such metrics could, for example, include the organisation's budget for the privacy function, the number of staff dedicated to privacy, evidence of product reviews conducted, and the number of training sessions

[24] When validation for accountability is required, it must be cost-effective for both privacy protection regulators and agencies, and the companies that seek recognition. To be optimally effective, validation methods must be recognised across the marketplace. The validation system an organisation uses must be appropriate to the nature of the organisation, its data holdings and applications, and its business model. While no validation system is foolproof, it must be sufficiently rigorous to raise the level of trust within the market that organisations have met the requirements necessary for validated accountability. Questions related to the sufficiency of different types of validation methods will be taken up in year four of the Project.

carried out for employees. However, metrics may vary depending on the nature of the organisation, the data it collects and maintains, and the risks raised by its use.

An organisation could also be asked to provide a description of its oversight programme as it applies to the data activities under investigation, and metrics about that monitoring, including how frequently the privacy team reviews data processes within business units, how often specialized security audits are carried out; and the number of business unit or process internal audits.

Finally, in *cases where a failure has in fact been identified*, the organisation could be required not only to provide evidence of its privacy and oversight programmes, but to have these aspects of its privacy initiative validated by a third party.

Officials may initiate an inquiry as a follow-up to an investigation and enforcement action, to ensure that required remediation has been carried out. Such inquiries may involve periodic independent audit of the organisation in areas that are the subject of the investigation and enforcement action.

Responding to an Official Inquiry	Internal Policies	Implementation Programme	Privacy Governance	Oversight
Organisations responding to a random accountability check would	- Provide description of internal policies based on external criteria	- Provide description of implementation programme	- Provide description of governance programme	- Provide description of oversight programme
Organisations responding to an investigation of suspected failure or resulting from evidence of actual failure would	- Provide description of internal policies based on external criteria relative to area in question	- Provide description of implementation programme relative to area in question - Provide evidence of implementation - When finding of failure, validation by a third party is required.	- Provide description of governance programme relative to area in question - Provide metrics related to governance	- Provide description of oversight programme relative to area in question - Provide metrics related to monitoring - When finding of failure, validation by a third party is required.
Organisations responding to an enforcement follow-up would				- Provide results of periodic independent audit of area in question

Conclusion

The practical success of an accountability approach will rely significantly on its broad implementation across the marketplace. When all organisations implement the essential elements, benefits accrue to individuals, the marketplace, and organisations themselves – greater confidence in data protection, better compliance, efficiencies for regulators and organisations, and a heightened expectation on the part of individuals and the market that organisations will act in accordance with the requirements of accountability. Recognised accountability offers enhanced benefits to organisations that may wish to transfer data across borders, adopt a new technology or business model, or simply signal their heightened attention to accountable practices.

Accountability continues to figure prominently in discussions about data protection and privacy within countries and in international forums. Going forward, the Project will focus in a more detailed way on the infrastructure necessary for successful implementation of an accountability approach by organisations and by regulators. While some of the mechanisms that will make up this infrastructure may require action by policymakers before they can be realised, it is important that the work begin.

APPENDIX A

The Essential Elements of Accountability[25]

An accountable organisation demonstrates commitment to accountability, implements data privacy policies linked to recognised outside criteria, and establishes performance mechanisms to ensure responsible decision-making about the management of data consistent with organisation policies. The essential elements articulate the conditions that must exist in order that an organisation establish, demonstrate and test its accountability. It is against these elements that an organisation's accountability is measured.

The essential elements are:

1. Organisation commitment to accountability and adoption of internal policies consistent with external criteria.

An organisation must demonstrate its willingness and capacity to be both responsible and answerable for its data practices.

An organisation must implement policies linked to appropriate external criteria (found in law, generally accepted principles or industry best practices) and designed to provide the individual with effective privacy protection, deploy mechanisms to act on those policies, and monitor those mechanisms. Those policies and the plans to put them into effect must be approved at the highest level of the organisation, and performance against those plans at all levels of the organisation must be visible to senior management. Commitment ensures that implementation of policies will not be subordinated to other organisation priorities. An organisational structure must demonstrate this commitment by tasking appropriate staff with implementing the policies and overseeing those activities.

2. Mechanisms to put privacy policies into effect, including tools, training and education.

The organisation must establish performance mechanisms to implement the stated privacy policies. The mechanisms might include tools to facilitate decision making about appropriate data use and protection, training about how to use those tools, and processes to assure compliance for employees who collect, process and protect information. The tools and training must be mandatory for those key individuals involved in the collection and deployment of personal information. Accountable organisations must build privacy into all business processes that collect, use or manage personal information.

3. Systems for internal ongoing oversight and assurance reviews and external verification.

Using risk management analysis, enterprises that collect and use personal information must monitor and measure whether the policies they have adopted and implemented effectively manage, protect and secure the data. Accountable organisations establish these performance-monitoring systems based on their own business cultures. Performance systems evaluate an organisation's decisions about data across the data life cycle – from its collection, to its use for a particular application, to its transmission across borders, to its destruction when it is no longer useful – and must be subject to some form of monitoring

The organisation should establish programmes to ensure that the mechanisms are used appropriately as employees make decisions about the management of information, system security and movement of data throughout the organisation and to outside vendors and independent third parties.

The organisation should also periodically engage – or be engaged by – the appropriate independent entity to verify and demonstrate that it meets the requirements of accountability. Where appropriate, the organisation can enlist the services of its internal audit department to perform this function so long as the auditors report to an entity independent of the organisation being audited. Such verification could also include assessments by privacy enforcement or third-party accountability agents. The results of such assessments and any risks that might be discovered can be reported to the appropriate entity within the organisation that would take responsibility for their resolution.

4. Transparency and mechanisms for individual participation.

To facilitate individual participation, the organisation's procedures must be transparent. Articulation of the organisation's information procedures and protections in a posted privacy notice remains key to individual engagement. The accountable organisation develops a strategy for prominently communicating to individuals the most important information. Successful communications provide sufficient transparency such that the individual understands an organisation's data practices as he or she requires. The accountable organisation may promote transparency through privacy notices, icons, videos and other mechanisms.

[25] Excerpted from "Data Protection Accountability: The Essential Elements," October, 2009 http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf.

When appropriate, the information in the privacy notice can form the basis for the consumer's consent or choice. While the accountability approach anticipates situations in which consent and choice may not be possible, it also provides for those instances when it is feasible. In such cases, it should be made available to the consumer and should form the basis for the organisation's decisions about data use.

Individuals should have the ability to see the data or types of data that the organisation collects, to stop the collection and use of that data in cases when it may be inappropriate, and to correct it when it is inaccurate. There may be some circumstances, however, in which sound public policy reasons limit that disclosure.

5. Means for remediation and external enforcement.

The organisation should establish a privacy policy that includes a means to address harm to individuals caused by failure of internal policies and practices. When harm occurs due to a failure of an organisation's privacy practices or to a lapse in its compliance with its internal policies, individuals should have access to a recourse mechanism. In the first instance, the organisation should identify an individual to serve as the first point of contact for resolution of disputes and establish a process by which those complaints are reviewed and addressed.

The accountable organisation may also wish to engage the services of an outside remediation service to assist in addressing and resolving consumer complaints. Third-party agents, including seal programmes and dispute resolution.

APPENDIX B

Common Fundamentals of an Accountability Implementation Programme[26]

Participants in the Accountability Project identified nine common fundamentals that an accountable organisation should implement. Organisations that wish to be deemed accountable should be cognizant of the fundamentals, and prepared to demonstrate their fulfillment of these conditions as appropriate to the nature of the data they collect, their business model, and the risks their use of data raises for individuals.

1. ***Policies:*** *Existence of binding and enforceable written data privacy policies and procedures that reflect applicable laws, regulations and industry standards.*

An organisation should develop, implement and communicate to individuals data privacy policies informed by appropriate external criteria found in law, regulation, or industry best practices, and designed to provide the individual with effective privacy protections. The organisation should also design and deploy procedures to put those policies into effect in light of the specific circumstances of its own organisations (e.g., what is collected, how it is used, and how systems and organisations are connected).

2. ***Executive Oversight:*** *Internal executive oversight and responsibility for data privacy and protection.*

Executive oversight will require the creation of a data privacy leader supported by appropriate resources and personnel, and responsible for reporting to organisation leadership. Commitment by top management should include appropriate reporting and oversight of the organisation's privacy programme. Top management should empower and require senior-level executives to develop and implement the organisation's programmes, policies and practices. Small and medium-sized organisations will need to allocate oversight resources appropriately, keeping in mind the extent and sensitivity of its data holdings and the nature of the use of the data.

3. ***Staffing and Delegation:*** *Allocation of resources to ensure that the organisation's privacy programme is appropriately staffed by adequately trained personnel.*

While recognizing the need to work within economic and resource constraints, accountable organisations should have in place sufficient staff to ensure the success of their privacy programme. Such staff should receive adequate training, both as they assume their role in the privacy programme and as that programme evolves to address new developments in the organisation's business model, data collection practices and technologies, and offerings to consumers. Delegation of authority and responsibility for data protection to appropriate units or parts of the organisation has been found to be effective in many accountable organisations. Staffing and delegation decisions in small and medium-sized organisations should reflect the particular circumstances of the organisation and its activities, and the nature, size and sensitivity of its data holdings.

[26] Excerpted from "Demonstrating and Measuring Accountability: A Discussion Document," http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.pdf.

4. ***Education and awareness:*** *Existence of up-to-date education and awareness programmes to keep employees and on-site contractors aware of data protection obligations.*

Organisations should provide the necessary briefings, information and education for their personnel to keep them apprised of current and emerging requirements. Such education should involve keeping employees aware of new data protection issues that may affect the performance of their job, and sensitive to the importance of data privacy to individuals and to the success and reputation of the organisation.

5. ***Ongoing risk assessment and mitigation:*** *Implementation of a process to assist the organisation in understanding the risks to privacy raised by new products, services, technologies and business models, and to mitigate those risks.*

To be accountable, organisations must assess the risks to privacy raised by their products and practices as they are developed, implemented and evolve, and as their data requirements change. In response to the findings of those assessments, organisations must take measures to mitigate those risks. Risk assessment is not static, but an ongoing function that responds to the dynamic, evolving nature of data collection, use and processing.

To be accountable for its risk assessment and mitigation practices, organisations also should be able to demonstrate the nature of their risk analysis. The organisation must show the rigor of the criteria against which analyses are carried out, and the suitability of those criteria to the nature of the data and data use. Further, the organisation should be able to demonstrate how decisions are made and steps are taken to mitigate risk. The organisation must also demonstrate that the decisions it takes to respond to identified risks are appropriate and effective.

6. ***Programme risk assessment oversight and validation:*** *Periodic review of the totality of the accountability programme to determine whether modification is necessary.*

An accountable organisation should periodically review its privacy and data protection accountability programme to ensure that it continues to meet the needs of the organisation by supporting sound decisions about data management and protection that promote successful privacy outcomes. To encourage transparency, the results of that programme review should be available to those persons or organisations external to the reviewing group tasked with programme oversight. The method by which this information is derived and reviewed must be both appropriately rigorous and cost effective for both organisations and regulators. The results of these assessment measures and/or audits should be reported to the appropriate personnel within the organisation, and when necessary, corrective action should be taken.

7. ***Event management and complaint handling****: Procedures for responding to inquiries, complaints and data protection breaches.*

An accountable organisation should implement a well-designed, reliable procedure for addressing data protection problems when they arise. Such procedures will need to effectively address data protection problems, such as data misuse, misappropriation or breach. They also must include a formal complaint procedure to address concerns of individuals regarding data protection practices, and potential or actual failures, and to ensure that the rights of individuals related to their data are respected.

8. ***Internal enforcement:*** *Internal enforcement of the organisation's policies and discipline for non-compliance.*

Accountable organisations should have in place policies and procedures for enforcement of internal data protection rules. Personnel who disregard those rules or misappropriate or misuse data are subject to sanctions, including dismissal.

9. ***Redress:*** *The method by which an organisation provides remedies for those whose privacy has been put at risk.*

Accountable organisations should establish redress mechanisms whereby individuals may have their complaints heard and resolved. The redress mechanisms should be appropriate to the character of the organisation, the nature of its data holdings, and the way the data is used and appropriate for the specific issue. The redress mechanism should be readily and easily accessible by individual, and address complaints efficiently and effectively. Industry groups may offer options for individual organisations seeking to implement a redress mechanism. As the specific attributes of an appropriate redress may vary from culture to culture and from industry to industry, decisions about redress will likely be local. Guidance about redress would optimally be developed in consultation with experts, regulators, civil society, and representatives of public and private sector organisations.

Accountability Phase III - The Madrid Project Participants

The following lists the participants in the Accountability Phase III - The Madrid Project. This list indicates participation in the Madrid Project deliberations only, and does not imply endorsement of the contents of this document.

Joseph Alhadeff, Oracle Corporation

Brendan Van Alsenoy, Interdisciplinary Centre for Law and ICT, Belgium

Carman Baggaley, Office of the Privacy Commissioner, Canada

Andrea Krisztina Bárányos, Office of the Parliamentary Commissioner for Data Potection and Freedom of Information, Hungary

Rosa Barcelo, Office of the European Data Protection Supervisor

Christophe Begot, Total, S.A.

Bojana Bellamy, Accenture

Emma Butler, Information Commissioner's Office, United Kingdom

Giovanni Buttarelli, Office of the European Data Protection Supervisor, Belgium

Fred H. Cate, Indiana University, Maurer School of Law

Peter Cullen, Microsoft Corporation

Susan Daley, Symantec Corporation

Gary Davis, Office of the Data Protection Commissioner, Ireland

Stephen Deadman, Vodafone

Elizabeth Denham, Office of the Privacy Commissioner, Canada

Michael Donohue, Organisation for Economic Co-operation and Development

Leigh Feldman, Bank of America

Lindsey Finch, Salesforce.com

Giusella Finocchiaro, University of Bologna

Peter Fleischer, Google

Christine Frye, Bank of America

Jose Leandro Nunez Garcia, Data Protection Agency, Spain

Carlos García-Mauriño, Oracle

Jennifer Barrett Glasgow, Acxiom Corporation

Rafael Garcia Gozalo, Data Protection Agency, Spain

Constance Graham, Procter & Gamble Company

Silke Harz, Office of the Federal Data Protection Commissioner, Germany

Billy Hawkes, Data Protection Commissioner, Ireland

Markus Heyder, United States Federal Trade Commission

David Hoffman, Intel Corporation

Sandy Hughes, Procter & Gamble Company

Brian Huseman, Intel Corporation

Barbara Lawler, Intuit, Inc.

Brendon Lynch, Microsoft Corporation

Jean-Guy Mahaud, Total, S.A.

Fran Maier, TRUSTe

Maria Marvan, Federal Institute for Access to Information and Data Protection, Mexico

Georgina Nelson, Which?, London

Mikko Niva, Nokia

Daniel Pradelles, Hewlett-Packard Company

Artemi Rallo, Agencia Española de Protección de Datos, Spain

Kostas Rossoglou, BEUC - The European Consumers' Organisation, Belgium

Russell Schrader, Visa Inc.

Manuela Siano, Data Protection Authority, Italy

David Smith, Information Commissioner's Office, United Kingdom

Scott Taylor, Hewlett-Packard Company

Adriana Lopez-Tafall, Merck & Co., Inc.

Bridget Treacy, Hunton & Williams LLP

Hilary Wandall, Merck & Co., Inc.

Jonathan Weeks, Intel Corporation

Nigel Waters, Australian Privacy Foundation and Privacy International

Jan-Boris Wojtan, Accenture

Martin Abrams, The Centre for Information Policy Leadership, Hunton & Williams LLP

Paula J. Bruening, The Centre for Information Policy Leadership, Hunton & Williams LLP

Richard Thomas, The Centre for Information Policy Leadership, Hunton & Williams LLP

THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP