THE

GLOBAL INFORMATION ACCOUNTABILITY PROJECT

AT FIVE YEARS

Draft Copy

22 May 2014

THE GLOBAL INFORMATION ACCOUNTABILITY PROJECT:
THE FIRST FIVE YEARS

PREFACE

Martin Abrams
Executive Director and Chief Strategist
The Information Accountability Foundation

April 2014 marks the five-year anniversary for the Global Information Accountability Project. Since its work began in 2009 in Dublin, Ireland, the Accountability Project has sought to build bridges among:

- Regulators, policymakers, civil society and business leaders
- Principles, laws and practices
- National, international and regional data protection frameworks

In the last five years, accountability has been reflected in policy instruments issued in the Europe, Americas and Asia, and data protection agencies in Canada have provided guidance to define their expectations of accountable companies. Mexico and Columbia have incorporated elements of accountability into their data protection frameworks. Finally, in response to these advances in public policy, many companies have taken important steps toward implementing an accountability programme.

At the outset of the Project, I had privileged to serve as the President for The Centre for Information Policy Leadership at Hunton & Williams, which has served as secretariat for the Project. I am pleased to be able to continue the Project's work as Executive Director and Chief Strategist for The Information Accountability Foundation ("Foundation"), a non-profit research and educational organisation founded to integrate accountability and data stewardship as key components of information policy, innovation and effective enforcement. This paper documents the past five years of the Project's work.

The success of the Project has been in large part from an international group of experts from business, government, data protection and regulatory agencies, and the advocacy community. In particular, however, I give special thanks to Paula Bruening, who skilfully guided the consensus process reflected in the various papers over five years. In addition, I give special thanks to Kiisha Jennings for her 5 years of project management. I am also very grateful to Billy Hawkes who had the vision to facilitate the project's first year. I would also like to thank Foundation Scholar John Kropf for his work on this report.

This paper provides a five-year summary of the Project and does not necessarily reflect the views of any participant, and the Foundation alone takes responsibility for any errors that may remain.

EXECUTIVE SUMMARY

The Accountability Project ("the Project") marked its five-year anniversary in April 2014. During each of its five years, the Project provided shape and definition to the data protection practices that make up accountability. The result has influenced lawmakers, regulators and policy makers to adopt elements of accountability.

The Project's first year established that, to be accountable, an organisation should design and implement comprehensive data and privacy protection programmes based on analysis of the risks data use raises for individuals and on responsible decisions about how those risks can be appropriately mitigated. Through its Galway Paper, the Project articulated essential elements of how 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. It is against these elements that an organisation's accountability is measured.

In its second year, the Project issued the Paris Paper that proposed the fundamental conditions of accountability that an organisation put in place and be able to demonstrate to regulators. It further considered how, and under what circumstances, regulators, data protection authorities and their designated agents would measure accountability. The Project anticipated that 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.

In year three, the Project considered accountability as an approach to privacy and data protection required and implemented across the marketplace, and articulated the benefits that would accrue to individuals, the market and organisations as a result. While all organisations would adopt accountability in this model, the Project presented the Madrid Paper that identified instances in which an organisation might seek recognition of its accountability. It also described under what circumstances organisations would be required to demonstrate their accountability and what exactly that demonstration would entail.

By the Project's fourth year in 2012, accountability had emerged as a recognised approach to privacy and data protection. The European Commission had proposed a data protection regulation that would apply across European Union ("EU") member countries and in which accountability played a critical role. The Federal Privacy Commissioner of Canada and Information Commissioners of Alberta and British Columbia in Canada released a document articulating what data protection authorities would expect of organisations under an accountability approach. The Asia-Pacific Economic Cooperation ("APEC") forum finalised its Cross Border Privacy Rules system, an accountability-based code of conduct for businesses in the APEC region.

In its fifth year, the Project focused on the application of accountability under specific conditions such as distributed environments, public clouds and scalability. That year, the Project introduced risk as another element of consideration. The influence of the Project could be seen in the work of the regulators with the Hong Kong Privacy Commissioner's guidance, "A Best Practice Guide." In addition, the influence of the Project included the Article 29 Working Party and the

APEC Data Privacy Subgroup release of their review of the EU's Binding Corporate Rules ("BCRs") and APEC's CBPR system. Both explicitly acknowledged the common elements of the two accountability-certifying systems that used very different assessment processes. While the work of the Project continued at the Centre, a new organisation, the Foundation was formed to provide a non-profit home for work to implement accountability into governance structures. The Foundation focused its efforts on international dialogue on specific infrastructure issues related to accountability with a presentation before the Organisation for Economic Co-operation and Development ("OECD").

I. INTRODUCTION

In 1980, the OECD issued *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* ("OECD Guidelines"). This was the first international articulation of substantive principles of data protection. Twenty-nine years later, the Global Information Accountability Project ("the Accountability Project") sought to articulate the process elements that implement the OECD's data protection principles. Accountability was not new to data protection. It has served as a rallying point to articulate existing operational concepts that had been used in practice and to provide a roadmap for future effective implementation.[1]

We are now at the five-year mark with the Accountability Project. This paper provides a review the Project's work and an assessment how accountability has influenced the real-world applications of privacy and data protection.

II. HISTORY

A. Year One: Articulating the Essentials of Accountability

In April 2009, a global dialogue began to provide guidance on how organisations might demonstrate their accountable use and management of personal information. Participants included representatives from industry, government, civil society, academia and businesses met to discuss the elements of accountability with perspectives from Europe, North America and the Asia-Pacific region. The dialogue began in Dublin, Ireland, facilitated by the Office of the Privacy Commissioner of Ireland and the Centre for Information Policy Leadership at Hunton & Williams LLP ("the Centre").

Following two rounds of discussion, the Project issued "Data Protection Accountability: The Essential Elements" in October, 2009, also known as the "**Galway Paper**."[2] The Galway Paper stated that an organisation demonstrates a commitment to accountability when it 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 in-

[1] Elements of Accountability have been embedded explicitly and implicitly in various frameworks including the EU Directive 95/46 (especially the framework for binding corporate rules, Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"), the Safeguards Rule of Graham-Leach-Bliley Act ("GLBA") as applied by the U.S. Federal Trade Commission ("FTC") and the APEC Privacy Framework.

[2] http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf

clude applicable law and regulation in addition to recognised external guidelines. The Paper articulated five essential elements of accountability:

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.

At the same time, the Galway conversations focused attention on accountability, a cross-section of regulators in the United States, Canada and the EU were also taking notice of whether accountability as an effective tool to improve compliance.[3] Most notably, in December, the EU Article 29 Working Party and the Working Party on Police and Police and Justice issued a joint contribution to the consultation that identified the challenges to the existing legal framework for data protection. The Working Party noted that "it would be appropriate to introduce in the comprehensive framework [on data protection] an accountability principle, so data controllers are required to carry out the necessary measures to ensure that substantive principles and obligations of the current Directive are observed when processing personal data and to have the necessary internal mechanisms in place to demonstrate compliance to external stakeholders, including DPAs."[4]

As a follow-on, the Article 29 Working Party issued an opinion in July 2010, proposing that accountability "would 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." The opinion considered accountability in light of both global movement of data and EU framework as a "way of encouraging data controllers to implement practical tools for effective data protection."[5]

---

[3] "Promoting Consumer Privacy: Accountability and Transparency in the Modern World," remarks of FTC Director David Vladeck, October 2, 2009, at: http://www.ftc.gov/sites/default/files/documents/public_statements/promoting-consumer-privacy-accountability-and-transparency-modern-world/091002nyu.pdf; Privacy by Design: Essential Elements for Organisational Accountability and Strong Business Practices, November 2009, a paper co-authored by Ontario's Privacy Commissioner Ann Cavoukian at: http://www.ipc.on.ca/images/Resources/pbd-accountability_HP_CIPL.pdf.

[4] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf

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

At the close of its first year, the Project had articulated elements of accountability that would serve as the foundation for the next phases of work. The Project's work was beginning to receive notice from policy makers.

B. Year Two: Establishing Conditions and Measurements to Accountability

With the essential elements of accountability articulated, the Project proposed that its second year should move to Phase II with two stated goals: 1) establish fundamental conditions that an organisation should put in place to demonstrate accountability and 2) provide regulators the ability to measure it. The Project anticipated that 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.

During 2010, discussions of Phase II were co-facilitated by the CNIL, the French data protection authority, in Paris—this time with an even larger group of participants than the year before in Ireland. The result of this dialogue culminated in the Project issuing its second major paper, Demonstrating and Measuring Accountability, also known as the "**Paris Paper**."[6]

The Accountability Project identified nine common fundamentals that an accountable organisation should implement. Organisations that wish to be deemed accountable should be cognisant of the fundamentals and be prepared to demonstrate their fulfilment 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. The nine fundamentals are:

> **1. Policies:** Existence of binding and enforceable written data privacy policies and procedures that reflect applicable laws, regulations and industry standards.
>
> **2. Executive Oversight:** Internal executive oversight and responsibility for data privacy and protection.
>
> **3. Staffing and Delegation:** Allocation of resources to ensure that the organisation's privacy programme is appropriately staffed by adequately trained personnel.
>
> **4. Education and awareness:** Existence of up-to-date education and awareness programme to keep employees and on-site contractors aware of data protection obligations.
>
> **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.
>
> **6. Programme risk assessment oversight and validation:** Periodic review of the totality of the accountability programme to determine whether modification is necessary.

[6] http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF

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

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

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

Redress was a significant part of this dialogue. 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 the 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.

By the end of Year Two, the Project had achieved its two goals of articulating fundamental conditions that an organisation should put in place to demonstrate accountability and providing regulators the ability to measure those conditions.

C. Year Three: Articulating Detailed and Customised Approaches

In Year Three, the Project continued to give shape and definition to accountability. The Project moved to Phase III with three stated goals: 1) define the benefits of accountability; 2) define what additional steps would be required by organisations seeking recognised accountability; and 3) define what would be required of organisations that respond to official oversight requests to demonstrate accountability.

The Project, through a process facilitated by the AEDP - Spanish Data Commissioner, convened the third international discussion around these issues with participants at three meetings held in Madrid and Washington, DC. The result of this dialogue culminated in the Project issuing its third major paper, Implementing Accountability in the Marketplace, also known as the "**Madrid Paper.**"[7]

In summary, the Madrid Paper addressed the three focus areas set out for Phase III: benefits, recognised accountability and circumstances for demonstrating accountability.

1. Benefits

•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

[7] http://www.hunton.com/files/Uploads/Documents/Centre/Centre_Accountability_Phase_III_White_Paper.pdf

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 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.

2. Recognised Accountability for an Organisation

•A description of its internal privacy and data protection policies in addition to 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;
•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; and
•The organisation could also provide evidence of the review of the oversight mechanism through validation by an independent auditor, regulator or third party agent.

3. Responding to an official oversight requests to demonstrate accountability had a variable set of criteria depending on the circumstances.

- Random check;
- An investigation of a suspected or actual privacy or data protection failure; and
- Cases where a privacy or data protection failure has in fact been identified.

With the issuance of the Madrid Paper, the Project had provided definition to the benefits of accountability and defined what recognised and demonstrated accountability might look like.

D. Year Four: Recognition and Adoption by Authorities

When the Project continued into its fourth year, accountability had emerged as a recognised approach to privacy and data protection. Policy leaders, lawmakers and regulators around the world had adopted elements of accountability into their approaches to privacy and data protection. Significant examples included:

- In January 2012, the European Commission had proposed a data protection regulation that would apply across European Union member countries and in which accountability played a critical role.[8]
- In April 2012, the Federal Privacy Commissioner of Canada and the Information Commissioners of Alberta and British Columbia published a document articulating what data protection authorities would expect of organisations under an accountability approach.[9]
- The Asia Pacific Economic Cooperation forum (APEC) finalised its Cross Border Privacy Rules system, an accountability-based code of conduct for businesses in the APEC region.[10]
- Throughout 2012 and earlier, the FTC's settlements against, Google, Facebook and others mandated comprehensive privacy and information security programmes—programmes that followed the elements of accountability.[11]

Accountability elements also influenced the development and implementation of data protection law and policy in Latin America. Most notably, Mexico[12] and Columbia[13] incorporated the principles of accountability in their respective frameworks.

In light of the evolution of accountability into an accepted, practical approach to privacy and data protection, the Project moved to Phase IV and set as a goal development of a tool that would assist organisations in evaluating the steps they have taken internally to establish the conditions for accountability and in demonstrating them to data protection authorities or their recognised third party agents. By the end of 2012, the Project with input from international experts from government, industry, academia and civil society, issued a **Self-Assessment of a Comprehensive Privacy Programme: A Tool for Practitioners (Self-Assessment Tool).**[14] The tool was the product of the Project's past three years of work and provided a practical means to help organisations implement and evaluate the programmes and practices necessary to establish accountability for responsible data protection.

At the end of Year Four, accountability had been a significant influence on policy makers, regulators and practitioners. The Project itself continued to make accountability more practical by providing the Self-Assessment.

---

[8] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF

[9] http://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp

[10] http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx

[11] See generally, http://www.ftc.gov/enforcement/cases-proceedings

[12] https://www.privacyassociation.org/media/pdf/knowledge_center/Mexico_Federal_Data_Protection_Act_July2010.pdf

[13] Implementing directive in Spanish only at: http://www.littler.com/files/press/related-files/DECRETO%201377%20DEL%2027%20DE%20JUNIO%20DE%202013%20%282%29%20%282%29.pdf

[14] http://www.informationpolicycentre.com/files/Uploads/Documents/Centre/Phase_IV-Self_Assessment_Comprehensive_Privacy_Programme_A_Tool_for_Practioners.pdf

E. Year Five: Distributed Environments, Scalability, Risk and Global Interoperability

In Year Five of the Project, accountability principles continued to build influence with privacy and data protection regulators as well as the larger global dialogue. Phase V of the Project began with regulators in Europe and North America facilitating events in Warsaw and Toronto. In February 20013, in Warsaw, GIODO (Polish Data Protection Authority) facilitated panels that focused on the challenges of accountability in distributed environments using the examples of mobile applications and the public cloud.[15] The session illustrated that such environments no longer had a single comptroller, or comptrollers in a chain, but rather had many comptrollers, some with relationships with each other, but others that mostly had a relationship with the individual. For example, mobile computing includes the chip manufacturer, handset manufacturer, operating system, network, app designer and app sponsor. Defining the responsible party provided a challenge to the Project.

In May, the Office of the Federal Privacy Commissioner of Canada hosted a second meeting in Toronto focused on two elements of accountability: scalability and risk. A hypothetical German butcher shoppe provided an example of a small enterprise. The session demonstrated that by using an existing player, such as merchants associations, accountability is scalable. The Centre's Global Strategy Adviser, Richard Thomas, proposed a framework for risk, and Canada used recent cases to the test the framework. The Centre will continued that work and will publish on risk in 2014.

Concurrent with other activity, the OECD was completing its work on revised Privacy Guidelines. A most striking change was the enhancement of the commentary on the Accountability Principle that reflected the work of the Accountability Project. This revised commentary gave additional direction on the importance of accountability to data governance.[16]

During the fifth year, a new organisation, the International Accountability Foundation ("Foundation") was formed as a non-profit research and educational entity. The Foundation is the new home for the project. The dedicated non-profit structure creates a foundation to bring additional resources to fund specific projects related accountability governance implementation. The Foundation has received grants to pursue two topics. The first is accountability and government use of private sector, while the second is ethical accountability processes for big data governance.

As we entered year six, the Project saw the influence of its work through the guidance of regulators. For example, in February 2014, the Privacy Commissioner for Personal Data, Hong Kong issued, "A Best Practice Guide," which outlined a comprehensive privacy management programme consistent with accountability.[17]

---

[15] http://www.informationpolicycentre.com/files/Uploads/Documents/Centre/Accountability_Phase_V_Draft_Agenda_Winter_Meeting.pdf

[16] http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

[17] http://www.pcpd.org.hk/pmp/files/PMP_guide_e.pdf

Accountability was also a critical element to the emerging discussion on global interoperability. In March 2014, the Article 29 Working Party released a referential on EU's Binding Corporate Rules (BCRs) and APEC's CBPR system that explicitly acknowledged the value of "accountability agents."[18] The referential is the next step in creating interoperability between accountable organisations in the European Union and APEC region.

The Foundation has participated in a number of forum in Europe and North America. In March 2014, the Foundation presented a discussion paper, "The Origins of Personal Data and its Implications for Governance," to the OECD.[19] An Expert Roundtable Discussion was convened to consider possible revisions to the OECD Guidelines, among them a more fully developed description of the principle of accountability. Later in the year, the Foundation is co-sponsoring an International Conference in Pereira, Colombia, and is involved with the International Conference of Data Protection and Privacy Commissioners.

IV. A LOOK FORWARD

The Accountability Project over the past five years has helped establish accountability as a keystone of responsible information management and oversight. During that period, it has moved from key concepts, to guidance on building and overseeing comprehensive privacy programmes, to the manner that accountability would be built into revised laws and regulations. The next five years will be focused on applying accountability to emerging data governance challenges. In the immediate future, this includes work on advanced analytics often referred to as big data, accountability in emerging privacy and data protection regimes, and rethinking the openness principle to encourage greater individual participation beyond consent to guide appropriate data stewardship.

To meet this challenge, the Foundation needs to find new mechanisms to meet the community's needs. This may mean smaller, more targeted discussions, sponsored research and professional workshops. The Foundation will continue to focus on the future of governance as the organisation looks three to five years ahead.

V. CONCLUSION

In five years of outreach, education and consensus building, **t**he Project has demonstrated that it is possible to bridge the gap between policy and practice, among regulators, organisations and individuals, and across different global frameworks. Accountability can be made practical for both regulators and organisations. During this time, we have seen the emergence of the Cloud, Internet of Things and Big Data. Accountability provides a practical vehicle for protection of data in these environments that were not anticipated by early privacy guidance. While the objectives reflected in the OECD Guidelines are still appropriate, accountability allows for implemen-

[18]Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU ("European Union") and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents. See: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf

[19] http://informationaccountability.org/wp-content/uploads/Data-Origins-Abrams.pdf

tation in the information age providing protections that work. Lawmakers and regulators have recognised the utility of accountability and its influence can be seen through new laws and regulations, guidance and policy papers. Organisations that have actively participated in the Project have built accountability into their programmes and can measure its effectiveness. Now, at the five year mark, the Project looks ahead to advance practical applications of accountability in compliance and enforcement and global interoperability.

John W. Kropf
Foundation Scholar
The Information Accountability Foundation
Washington, DC