The Rise of Accountability from Policy to Practice and Into the Cloud

Bojana Bellamy, CIPP/E
Privacy Perspectives | **Dec 10, 2014**

Over past several years, the concept of "accountability" has become a cornerstone of effective data protection and a dominant trend in global data privacy law, policy and organisational practices. From the OECD Guidelines, the APEC Privacy Framework, the U.S., Canada, Mexico, Hong Kong and Singapore to the proposed EU Data Protection Regulation, the term encapsulates what most regulators now expect of responsible organisations that handle personal data and what many privacy laws have incorporated as a matter of legal compliance.

Accountable organisations are expected to build, implement and verify corporate privacy programs in order to deliver effective privacy compliance and protection on the ground while demonstrating the existence of the program, both internally to their corporate board and externally to their business partners and regulators.

The pioneering work on organizational accountability by the Centre for Information Policy Leadership (CIPL) has been validated by a host of developments.

- There is now a wealth of experience in leading global organisations, many of them CIPL members, building and implementing first-rate privacy programs.
- The privacy commissioners of Canada and Hong Kong have issued must-read regulatory guidance on privacy programs and their requirements.
- In the U.S., the Federal Trade Commission's consent decrees now spell out the requirements of accountable corporate privacy programs, signaling to organisations what it expects of them. Also, the Obama administration's progressive 2012 Privacy Bill of Rights included an accountability requirement.

- In Europe, Binding Corporate Rules (BCR) are not only a mechanism for legitimising intra-group transfers of data but are also full-blown accountability frameworks. Equally, the Article 29 Working Party's seminal opinion on accountability is as relevant today as when it was published in 2010.

- In Asia-Pacific, the APEC Cross Border Privacy Rules (CBPRs) have emerged as an increasingly significant accountability framework, gaining traction and momentum by the day for companies large and small.

- Finally, research and consulting organisations, such as Nymity, have been developing smart operational tools to help privacy officers implement and demonstrate accountability and internal privacy programs.

Clearly, accountability has already manifested itself in many forms and contexts. Indeed, the concept inherently allows for its adaptation to additional frameworks and tools, such as new codes of conduct, third-party certifications, privacy seals and even international standards.

What all of these accountability mechanisms have in common is that they imply the existence of substantive privacy rules, based on external laws or internal rules established by the accountability scheme itself; internal implementation and verification measures to comply with the rules, and some form of external certification/verification.

But the examples above are just the beginning.

New ISO Cloud Privacy Standard: The Proof Continues To Be in the Pudding

While speaking on a panel at the Cloud Law Summit in London recently, it struck me that a real example of how accountability has come of age and has been implemented in practice is actually the recent ISO 27018 data privacy cloud standard that was adopted last summer.

The ISO standard and certification is another important step in a long line of accountability milestones and a significant addition to the arsenal of compliance tools that cloud providers can use going forward.

ISO standards have not traditionally been perceived by the privacy community as accountability mechanisms. Yet all of us who have been working as privacy officers, in either service provider or client/customer companies, have encountered many ISO security standards either as a part of our due diligence process for choosing a service provider, in contractual negotiations between controllers and processors or when actually undergoing internal ISO certification processes.

In the information security world, ISO standards have always been an assurance and accountability mechanism.

Indeed, the new ISO cloud standard is a significant development both for cloud computing and accountability. It is a concrete example of a practical implementation of accountability and the pivotal role external verification and certification play in providing necessary assurances in both corporate and consumer contexts.

- For the first time, a comprehensive "accountability scheme" with specific privacy and security requirements has been developed by ISO for cloud service providers.

- With the growing prevalence of cloud computing, there is a practical need to translate generic privacy principles and requirements into different cloud services and technologies and to address numerous complex legal and commercial privacy and security challenges in a more consistent fashion across the industry.

- The increased adoption and success of cloud computing heavily depends on the trust of cloud users and the ability of corporate cloud customers and providers to comply with complex and diverging privacy requirements, stemming from both privacy laws and cloud contracts. Cloud service providers are quite rightly being pushed hard to earn and demonstrate that trust and reassure customers of their responsible data privacy and security practices. The new ISO certification intends to provide the cloud customers and users with that reassurance.

- Finally, the need to provide effective privacy protection in the cloud above and beyond specific legal regimes and across national borders has to be a major driver for both cloud users and providers who rely on borderless cloud technology.

Certified Accountability: A Cornerstone of Trust in the Cloud

Accountability, including external verification and certification, is *sine qua non* for trust and growth in cloud computing. Therefore, it is not surprising that ISO has decided to tackle this need and provide both cloud customers and providers with this useful accountability tool.

To me, the latest ISO standard and all the other developments mentioned above provide evidence of growing global convergence and consensus on accountability.

The ISO standard and certification is another important step in a long line of accountability milestones and a significant addition to the arsenal of compliance tools that cloud providers can use going forward.

Interestingly, the European Commission's special cross-industry expert group is also busy drafting an industry code of conduct for data protection in the cloud, for potential adoption by Article 29 Working Party. It will be important to ensure that the two accountability mechanisms, the ISO cloud standard and the EU Code of Conduct, remain consistent with each other.

The Future of Accountability Is Bright

To me, the latest ISO standard and all the other developments mentioned above provide evidence of growing global convergence and consensus on accountability.

Perhaps, even more importantly, they are a sign of a consensus on the increasing role it plays in the modern Information Age:

- to provide effective privacy management and protection for organisations and individuals;
- to translate substantive legal requirements into everyday business practices, adapting to different business models and different industries;

- to build trust among all players and stakeholders in today's digital ecosystem: organisations, shareholders, business partners, individuals, regulators and policy-makers and

- finally, to bridge jurisdictional and legal divides by creating real interoperability, by virtue of the fact that accountability can facilitate operations in multiple jurisdictions based on mutually agreed or commonly accepted privacy and implementation standards.

In her presentation at the last International Conference of Data Protection and Privacy Commissioners in October, Article 29 Chairwomen and CNIL President Isabelle Falque-Pierrotin eloquently described this phenomena as "integration." She explained how legal norms and rules are being supplemented by and integrated with effective accountability mechanisms, such as privacy compliance programs, BCRs, CBPRs, certifications and seals.

Finally, it is hugely encouraging that the proposed EU Data Protection Regulation endorses accountability and envisages codes of conduct, certifications and seals as additional means of demonstrating accountability. One can only hope the final text will remain flexible and progressive enough to connect all the accountability dots and allow it, in all its incarnations, to flourish and fulfill its potential.

More broadly and globally, it is essential to preserve this promising trajectory for accountability as a bridging concept in today's Information Age, an age heavily based on borderless, data-driven economies that face persisting differences in privacy and legal regimes around the world.