Interoperability: analysing the current trends & developments

Over the last 18 months, policymakers around the world have engaged in efforts to review and revise privacy and data protection law, regulation and guidance. These initiatives respond to dramatic and fast-paced changes in information technologies, data-driven business models, the ubiquitous collection and use of information, and advances in powerful analytics and cloud services - all of which challenge long-held beliefs about how best to responsibly manage information and mitigate against the risks its uses raise for individuals. Fueling these changes is the ability to quickly move and access data anywhere in the world, to store and process it remotely, and to make it available for use when and for the purposes it is needed. Paula Bruening, Vice President - Global Policy at the Centre for Information Policy at Hunton & Williams LLP, discusses the challenges of diverse data privacy regimes, and how interoperability and accountability could work in practice, among others.

Policymakers recognize the need for robust, protected data flows if the benefits of an information economy are to be realized. While the global flow of data is essential for innovation and economic growth, companies confront significant challenges when attempting to comply with often conflicting requirements of diverse national and regional data protection laws and regulations. Emerging policy initiatives stress the need to create a streamlined system which allows for the smooth movement of data across regimes, but in a manner that ensures that individuals enjoy the protections afforded by their local laws and regulations. They suggest the need to increase the interoperability of privacy frameworks to lower barriers to data flows and simplify compliance, while at the same time protecting individuals' rights as data about them travels across borders.

The challenge of diverse data protection regimes

Privacy is a culture-specific value that reflects that traditions, mores and sensibilities of a place and its people. Ideas about privacy relate to how individuals define the boundaries of their personal space and their perceptions about appropriate limits on government involvement in their personal affairs. Local ethics about privacy also depend upon a shared understanding of what people, depending upon the nature of their relationships, should appropriately be able to know about one another, and to what extent individuals should be able to control with whom and under what circumstances they share certain data about themselves.

Such differences are apparent when one compares how ideas about privacy manifest themselves in Anglo-Saxon-based cultures, such as the UK, where a person's home is considered to be his or her castle and the US where privacy was once defined as 'the right to be left alone', to some cultures where the English word privacy has no direct translation into the vernacular. Similarly, ideas about privacy in Asia will differ from those in Australia, which, like those in the UK and the US, are also rooted in an Anglo-Saxon tradition.

Not surprisingly, data protection laws that emerge from these divergent cultures also differ, so that privacy regimes around the world vary considerably. They may impose differing substantive requirements or diverge in their approaches to compliance, based on their civil law or common law tradition, or their reliance on self regulation to govern data protection. Data that flows across borders is stored in remote servers, or is accessed simultaneously in various countries around the world, and organizations must comply with a myriad of laws, regulations and privacy promises. Faced with requirements that may conflict or overlap, organizations are often forced to make difficult choices between privacy regimes when determining where and how to comply.

These challenges are well recognized. In its recent report, '*Protecting Consumer Privacy in an Era of Rapid Change*', the US Federal Trade Commission (FTC) reported companies' assertions that more consistency between privacy regimes would reduce costs and increase compliance. It suggests that bridging these differences would provide the consumer with better, more consistent and predictable protections, wherever their data is processed. In '*Consumer Data Privacy: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*', released in early 2012, the Obama Administration noted that the obligations of different privacy laws burden companies, often requiring them to obtain multiple regulatory approvals to carry out even routine operations.

Such diversity makes compliance challenging at best. But equally important, it makes more difficult the task of protecting individuals and mitigating the risks the uses of data may raise. Organizations must invest significant time and money into understanding and

complying with the requirements of multiple privacy regimes. Doing so directs resources away from more effective mechanisms that might be put in place to assess and address risks to individuals.

Interoperability

While the challenges posed by this diversity are real, it is increasingly clear that solutions do not lie in attempting to map one national or regional approach to another. Because privacy is fundamentally cultural in nature and policy approaches – while equally legitimate – may differ significantly, imposing a regime, or adapting the law of one country or region to mirror that of another will not work. Any solution will need to respect differences inherent in national and regional privacy regimes, and honor the requirements of local protections, even as data travels globally. At the same time, it must facilitate the flow of data that fuels innovation and economic growth.

Policymakers refer to interoperability as a way to facilitate the global flow of data across diverse privacy regimes. In its Report, the Obama Administration cites interoperability between privacy regimes as critical to the continued growth of the digital economy. The FTC recognizes the value in greater interoperability among data privacy regime as consumer data is increasingly transferred and access around the world. The principles supporting the Asia-Pacific Economic Cooperation Privacy Framework (APEC) form the basis for a cross-border privacy rules system that would facilitate data transfers across APEC economies. And in 2011, the Organization for Economic Cooperation and Development (OECD) issued a report '*Thirty Years After: The OECD Privacy Guidelines*', in which it discussed the demands of the global data environment, national and regional attempts to bridge differences, and the shared responsibility of national and regional authorities to promote protected data flows across borders.

Because privacy is fundamentally cultural in nature and policy approaches – while equally legitimate – may differ significantly, imposing a regime, or adapting the law of one country or region to mirror that of another will not work

The term interoperability refers to the ability of diverse systems and organizations to work together. The IEEE Glossary defines interoperability as the ability of two or more systems or components to exchange information and to use information that has been exchanged. For purposes of international transfers of data, interoperability requires three elements: 1) common principles; 2) accountability; and 3) cooperation between regulators.

Commonly accepted principles and accountability

As long established, widely recognized principles of data protection, fair information practices provide common principles and a set of shared expectation about responsible data management. Fair information practices, as expressed in law, regulation and guidance, can provide a platform for interoperability across diverse privacy regimes.

Accountability recognizes differences in privacy law and regulation, but neither requires one country or region to necessarily adopt or adapt to the system of another, nor forces all systems to bend to a common regime. Rather, it takes the view that obligations - in law, regulation, best practices or an organization's promises - attach to data and must be met wherever or by whomever the data is processed. Accountability vests the user of data with responsibility for ensuring that the obligations are honored. Within its own organization, a data user adopts privacy policies linked to recognized external criteria - applicable law, regulation, and guidance based on fair information practices. Accountability requires organizations to understand the risks to individuals raised by new ways in which data is collected, processed and stored, and to mitigate those risks.

An organization that is accountable also implements mechanisms that ensure that those policies are carried out in practice. These 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. Accountable organizations oversee and internally review its risk assessment processes, the success and shortcomings of its privacy programs, and the decisions it makes about how it will use and protect information.

Accountability facilitates interoperability because the organization's responsibility for data does not end at the doors of its enterprise or the borders of its home country. Rather, when making decisions about, for example, transferring data to a third party for processing, storing data in the cloud, or making data accessible to researchers in far reaching corners of the globe, organizations must ensure that the obligations that attach to the data can be met in those locations, and by the organizations that are entrusted with the data. A Canadian organization that might want to store data in a private cloud in the Czech Republic would need to determine whether the cloud provider is prepared to provide necessary security to protect against possible breach or other compromise of data, and

whether it is equipped to understand and meet the requirements of the organizations' commitments. It would also provide necessary information so that the cloud provider understands what is required of it, which obligations attach to the data it receives and how those obligations must be met, and the limitations on how the data can be used beyond specified processes.

Cooperation among regulators

While agreements between organizations can facilitate the protected flows of data, interoperability also requires the cooperative involvement of data protection authorities to provide rigorous oversight, and recourse for individuals when their information - no matter where in the world it is processed - is used inappropriately or outside the bounds of law, regulation or representations made by a company.

Regulators and their authorized representatives can provide individuals with recourse. But to facilitate necessary cooperation, they will need assurances among themselves that processes and oversight of regulatory bodies can be trusted, and that data can be safely shared between them where necessary to resolve disputes or address instances of malfeasance. Organizations must also be answerable to regulators for their assessments about the risks data transfer and use raise, for the decisions they make about moving data across borders, and for the assertions they make about their ability meet the obligations in law, regulation and guidance that come with data they process. While many issues will likely be resolved through contractual agreements between companies, the oversight of government bodies and their authorized agents will keep organizations honest, responsible to individuals, and foster the trust of the international community.

Work at APEC has made significant inroads in considering how such an oversight infrastructure might be designed, anticipating the establishment of an oversight panel, criteria to assess a company's privacy programs and processes, and mechanisms for enforcement cooperation. The OECD has also invested significant effort to develop a framework for cooperation among privacy enforcement authorities. To facilitate that oversight, however, organizations will need a vehicle and a common set of criteria whereby they demonstrate their trustworthiness to regulators. It is not enough for organizations to assert that they have in place the conditions necessary to honor the obligations associated with the data; they must be required, under appropriate circumstances, to stand behind their assertions.

Conclusion

While the need for interoperability is clear, considerable work remains if it is to work in practice. A shared understanding of what accountability is, agreement on common, high level principles, and trusted cooperation between privacy enforcement authorities will be essential to successful interoperability. While the challenges to accomplishing these goals are significant, important progress has already been made. Because robust and protected data flows are so fundamental to economic growth, there is no alternative but to complete the task.

Paula J. Bruening
Vice President - Global Policy Centre for Information Policy
Hunton & Williams LLP