Moving Information Across Borders

The Need for a Global Accountability Framework

Remarks by Peter Cullen
General Manager, Trustworthy Computing Group and Chief Privacy Strategist
Microsoft Corp.

Presented at the 30th International Conference of Data Protection and Privacy Commissioners
Strasbourg, France
16 October, 2008

Moving Information Across Borders: *The Need for a Global Accountability Framework*

When it comes to data protection and privacy today, there is much discussion about the future of regulation and business practices in a globalized environment where information flows across borders like water. How will yesterday's regulatory and business accountability models evolve to help face tomorrow's data protection challenges? What would this new model look like? How would it work? How can it ensure the consumer is adequately protected?

The future of data protection will require much more than simply talking about the regulatory model. Yes, the regulatory framework needs substantial change. But the business accountability model must also change, along with the way business and regulatory communities engage with each other.

To face the challenges of today as well as tomorrow — the growing diversification of information collection, and the global flows of this information — an entirely new model is needed, one that will require a fundamentally different type of partnership between policy-makers, regulators, business and civil society.

The Need for Change

Why is such broad change needed? Simply put, there are three reasons:

- Today's regulatory models were designed for a different era. Data flows much differently today than it did a decade ago, and it will flow much differently a decade from now.
- Organizations, both public and private, have not shown enough accountability to meet the data-protection challenges of this new world.
- As a result, today there is too much responsibility placed on the consumer.

Today, business models that involve vast and diverse data flows — once reserved for large organizations — are being used by small and medium enterprises and even consumers, who choose for themselves where their data goes. These business models are being enhanced to provide greater value, which often means data is dispersed around the world. The flow of data is also being enabled and affected by other factors, such as the increasing number of devices that connect with each other, and the emergence of "cloud computing," which creates mirrored data around the world. Today, information flows are truly global.

The terms "privacy" and "data" are also changing. Formerly, "data protection" was limited to such things as name, address and credit card number. Today there is a range of other information to be considered, such as IP addresses and other unique numbers associated with the Web 2.0 world.

Today, there are more players in the field, and new entrants to the market, such as advertisers, who until recently would not have thought of themselves as part of the data protection schema.

The diversity of these challenges is compounded by the diversity of new threats, often through new vulnerabilities targeted for exploitation by criminals, making the entire picture infinitely more complex than it was just yesterday.

What does all this mean to organizations? What does this mean for consumers, in a world where the ultimate criminal "prize" is personal information? What does the current "notice and consent" model provide for consumers who have to wade through the complexity of broader data use and the real threats of today?

Clearly a new level of transparency and accountability is needed. After all, today's organizations have shown time and again that they cannot effectively protect data as evidenced, for example, by the large number of data breaches globally. As the threat landscape continues to evolve, rapidly and dramatically, there is little doubt this complex arena will continue to evolve, just as dramatically, just as rapidly, over the next decade. In this new world, business accountability needs to evolve and, as well, the current regulatory model needs to change.

Harmonized Principles, Disjointed Approaches

The diversity of regulatory models around the world illustrates the challenge. There are umbrella models in the EU, Canada, Australia and New Zealand. There are patchwork, piecemeal approaches such as in the U.S. In places such as Vietnam, the Philippines, Malaysia and Singapore, and APEC countries overall, new hybrid models are emerging.

Some have said that harmonizing the principles of these different approaches is all that's needed. This is not the issue. There is a surprising overlap in their principles.

The issue is that approaches to regulation in each region are fundamentally different. Even in so-called "harmonized" markets there is a lack of harmonization.

For example, today there are more than 20 different approaches to registering data processing within the EU alone. The U.S. approach features a dizzying combination of sectoral, state and issue-driven regulation, combined with self-regulation. The spectrum of approaches to this issue is almost as diverse as the threat landscape they're trying to address, which only adds complexity to an already confusing equation.

Worse, many of the more advanced economies, including the EU, seem to believe that geographically and culturally created points of view are both sustainable and exportable. Regulatory bodies find it difficult to even recognize each other's efforts — would it be better to have no privacy law in Vietnam than to have a privacy law that does not include an "independent data protection commissionaire"?

In the face of all this change, business, policy-makers and regulators are not communicating enough to even understand today's challenges in a way that positions the industry for tomorrow. How can regulators understand new and complex business models without effective communication? How can that happen in the EU, much less in Singapore or Peru? How can businesses become truly accountable, when today accountability is not even fully described? How can this model support compliance when regulators do not have the resources to investigate and promote a viable framework? What's the incentive for all parties?

To date, attempts at figuring this out have not proven successful. Binding Corporate Rules have not been successful despite the considerable amount of time and money spent on them. The Article 29 Working Party has acknowledged these challenges and announced efforts to help, but there is yet much work to do, and it is not clear if this will be enough.

The overall model today is untenable, let alone workable in the future. In this world of more players and broadening data and its implications to privacy, a different approach is needed.

Adaptable and Accountable

To get to a more acceptable point, business, government and civil society are going to have to work together in fundamentally different ways. Those who set and enforce policies must become adaptable. And at the same time, as the keepers of valuable personal information that often cuts across national boundaries, organizations must become more accountable to common standards of data protection.

Regulators must be open to thinking about new regulatory models that are not rooted in historical, traditional points of view. Regulators must understand not only today's and tomorrow's data flows, but also what's going to be required to make business more trustworthy. This can only be accomplished by inviting broad participation from all stakeholders, including civil society, to engage in a level of global partnership that has not occurred in the past.

Developed economies must work in cooperation — and compromise — with developing economies, recognizing how cultural, legal, economic and business climates differ — and what each entity is facing regarding information protection and privacy.

Regulators must work closely with businesses to define their role, their responsibilities and what accountability means in the new information age. What are the standards? How can they create an atmosphere of mutual trust? Is it certification? If so, is it self-certification, or perhaps a regulatory body using a Trustmark agency to validate compliance — in effect expanding the regulator's resources?

Underneath those options lies a fundamental need to define what it means to be accountable, and to develop a system that helps ensure compliance — a system built on mutual recognition, and on growing mutual trust. The ultimate goal is to improve transparency between organizations, regulators and policy-makers.

Building for the Future

So is anyone getting this right today? The APEC privacy initiative is as close as anyone has come to this kind of cross-border engagement. In APEC there is an attempt to address the challenges of cross-border data flow with an ethic of mutual recognition, where more developed economies work inclusively with developing ones.

The APEC privacy initiative represents progress in two ways. Number one, the inclusion and mutual recognition of varying economies, capabilities and cultures. Number two, a process that takes the best of existing regulatory models, focuses on the challenge of cross-border data flows and business responsibility, and works to create a privacy framework that works for everyone.

Outside of APEC, a group of like-minded experts under the leadership of the Irish Data Protection Authority, Billy Hawkes, will explore the components of organizational accountability in 2009. As with changes to the regulatory approach, the model for organizational practices needs to change if business is to be seen as trustworthy.

Ultimately, this challenge is beyond regional. This is not about meeting directives doled out from one part of the world to create another, standalone, regional solution. This is global. This challenge belongs to all, and therefore everyone needs to be sitting at the table.

Without the kind of broad partnership and coordination demonstrated by APEC on a global scale — without mutual recognition — more of the same limited, regional regulatory approaches will be developed. The result will be even more complexity in the regulatory ecosystem, and this complexity will remain the industry's greatest vulnerability.

By pursuing "more of the same," protection for the people that matter most will degrade rather than improve, because whether these problems are fixed or not, the flow of information globally will continue, and it will grow. If business and government fail to adapt and evolve, the ability to protect data worldwide will gradually erode. These problems cannot be solved immediately, but something must be done now, with cooperation and collaboration from all stakeholders.