

Going Global: Privacy in the Fifth Dimension

By Brian Tretick

Prepared remarks before the Federal Communications Bar Association International Telecommunications and Privacy and Data Security Committees

12 January 2011. Washington, DC.

It wasn't until the 20th century that we could even begin to put space and time together into space-time. We were comfortable with our three-dimensional view of space and understood time to be an independent dimension. Then—bam—with quantum physics, we needed to adjust our understanding of the universe. We now operate comfortably in four dimensions and have adapted to space-time. I contend that dealing with privacy while going global requires us to cross into a universe view that contains a fifth dimension that is neither spatial nor temporal. It is a dimension of international laws, regulations, social norms, and cultural behaviors that is really difficult to comprehend and operate in. I have been there, and at least we know they have oxygen.

We have covered most of the globe in tonight's discussions, but the main challenge is Europe. The regulatory and social regimes, similar yet notably distinct across the 27 member nations of the European Union, extend to the non-Union members as well. The Asia-Pacific region confronts us as an obvious conglomeration of different economies and regulatory regimes. Europe seems to soothe us with a regime that is on its surface apparently homogenous when viewed from our current dimension, but underneath which we discover a bubbling and turbulent atmosphere of distinct, disparate, and dynamic environments that make managing privacy very complicated indeed. In fact, it cannot be effectively from here, but only by stepping into that fifth dimension.

Knowing that there is oxygen should be comforting. Also, knowing that our government is active to give us a sort of grand unification theory of privacy is also comforting, but that part of the future is a long way away.

You will need, however, to address some new issues in new ways in order to operate there. Here are a few of them to start with:

First and foremost, you must:

Comply with national privacy laws and regulations in your new markets. Your foreign affiliates need to be established so that they meet local, applicable laws and regulations in the jurisdictions in which they operate, both for customer information and for employee information. Different approaches are needed, just as we approach a relativistic universe differently than a quantum universe. They have gravity, for example, but it operates differently there.

Next, you must consider local diplomacy by:

Consulting with works councils and other employee representative bodies. In Europe, it is common that these bodies have a consultative role in how employee information is processed, notably when it comes to trans-border transfer. In the US, for example, we only have company softball teams and they don't have a clue about privacy. So, the diplomacy you use should be thoughtful and begun early.

To comply locally, you will in all probability need to:

Seriously challenge your US-oriented approach. Many US-based organizations, on going global, find that their original policies and standard operating procedures are very US-focused. It will not be enough to establish policies and procedures for your foreign affiliates, but also will require you to review, rethink, and revise your corporate policies and procedures so that they are useful in your new markets. It's not uncommon for privacy policy, security policy, records management policy, acceptable use policy, and a host of similar corporate regimes to be

parochial and limited in their world view. Even website privacy statements will need to be revisited to address your global market. We have had such a 4-dimensional space-time view of the universe to date, and it will absolutely not work across dimensions. Period. It is time to adapt.

The next issue to address, once the local issues are understood, is to deal with trans-dimensional flow. Specifically, you will need to:

Legitimize the trans-border transfer and processing of personal information. In the US, personal information can come and go as you please, thank you very much. It's second nature just to transfer it between operating locations and with service providers. But when we factor Europe into the mix, there is no room for our second nature anymore. Every transfer of European personal information, each hop from entity to entity and location to location, must be legitimized. Safe Harbor, model contracts, binding corporate rules, and contracts and more contracts—some combinatorial cocktail of these techniques—is needed to cover a complex multinational corporation. It is rare that one technique suffices, and it's seldom easy. Outsourced and offshore operations, shared service centers, consolidated websites and global ecommerce platforms, and global systems and processes challenge our ability to understand and account for such a tangled web of information flows and processing. In a US-centric view, the concept of legitimizing the transfer and processing is alien indeed. It is, however, the crux of making privacy work when going global.

Compliance is not done, however, until the paperwork is done. This involves:

Registering, notifying, and seeking authorization from data protection authorities. Once you can decipher the alien glyphs and languages, registrations and notifications are fairly straightforward processes but still they are difficult to manage consistently. Some of your transfers, however, will likely require the additional, time-consuming steps associated with seeking authorization from some of the authorities. You should look to local counsel and well-organized files to help you establish and maintain your regulatory filings. However, we heard that these filings need to be completed before you actually need them, before you begin your transfers—so begin as well to investigate how to time warp backwards.

After dealing with the local issues and the trans-dimensional flow, you will need to address your control environment by:

Aligning your internal control and audit strategies to the international dimension. Each of the primary tools used to legitimize transfer and processing—such as Safe Harbor, model contracts, and binding corporate rules—involves first applying procedures and controls that may be new and different for your organization, and then validating them periodically, such as through audits. This not only requires them to be in place and operating effectively over time, but more of a challenge it requires others in your organizations to understand and recognize the new regimes. These cultural and institutional changes may be your most challenging.

At this point, you would have recognized the differences across dimensions and accounted for both the new operating environment and the trans-dimensional flow of information. It does not, however, stop. A dynamic and changing universe brings new operating conditions, new rules, and changes that must be addressed continuously.

In fact, we need to prepare ourselves for the establishment of other dimensions where neither a US-centric view nor even a somewhat common European view will suffice, as the privacy regimes of the Asia-Pacific region and South America continue to form and evolve. It will result, I am sure, in a never-ending pursuit for regulatory compliance and effective operations across the universe.

Thank you.

About the speaker

Brian Tretick is Managing Director for Athena and a member of the board of directors for the International Association of Privacy Professionals. He may be reached at brian.tretick@athenaprivacy.com.