Can 'Cross-Border Privacy Rules' Trump Divergent Data Protection Laws?

by Justin Brookman [1]
October 4, 2011

As privacy has become an increasingly important issue to people around the world, we have seen scores of countries pass data protection laws designed to give consumers control over the collection and disclosure of their personal information. This is good for consumers, but can be confusing and frustrating for businesses, as these laws are rarely identical and are even, at times, contradictory. As the world embraces cloud computing and data flows are increasingly global in nature, it's becoming more and more of a struggle for companies to keep track of new laws, or even figure out which apply, and when. If a French company stores data about a Mexican citizen on a data server in the Philippines owned by a U.S. cloud provider, what are the rules?

Over the past 15 years, privacy professionals have thought about this issue primarily in the European context, as the EU's Data Protection Directive prohibits sending data to jurisdictions that are not deemed "adequate" by European regulators (only a handful of other countries have been so blessed; the U.S., without any baseline privacy law [2] at all, certainly is not one of them). Over time, we've developed a few creaky workarounds to the adequacy requirement, such as the US-EU Safe Harbor program and the Binding Corporate Rules process. Both have been widely criticized, however: the former for being toothless, the latter for being too bureaucratic and burdensome.

For several years, the member economies of the Asia Pacific Economic Cooperation (APEC) have been working on a separate framework to allow for transnational data flows between countries with varying privacy requirements. Two weeks ago, I attended the biyearly meeting of the Electronic Commerce Steering Group (ECSG) within APEC in San Francisco where they formally approved the Cross Border Privacy Rules (CBPR) initiative as an effort to facilitate data flows while ensuring meaningful privacy protection within the region. If successful, the CBPR system could serve as a model for other international efforts to balance the competing values of privacy, commerce, and national sovereignty.

The structure for the CBPR system is that member economies within APEC will be able to recommend third party "accountability agents" to certify that domestic companies both comply with the privacy principles [3] outlined in the APEC Privacy Framework, and have internal procedures in place to ensure that privacy will be protected in practice. Participation in the CBPR by APEC member economies will be optional; a Joint Oversight Panel is being set up among those who opt to participate to formally grant recommended accountability agents the authority to certify compliance with the privacy principles across the entire region. The ECSG has also approved a very detailed set of criteria upon which accountability agents should access companies for compliance, though adherence to that particular checklist is not mandatory.

In many ways, the final iteration of the Cross Border Privacy Rules framework is significantly less ambitious than when APEC began working on the issue. Back then, it was hoped that complying with Cross Border Privacy Rules would essentially mean that you were compliant with all privacy laws in the Asia Pacific region. However, APEC is a consensus-based organization without the ability to bind its members, and since the Framework was agreed to in 2004/2005, many of the member economies have passed new data privacy laws imposing substantive (and varying) requirements on companies that process their citizens' data. Today, the APEC framework explicitly says that you still need to comply with differing privacy laws. The hope, however, is that by engaging in the CBPR system, the APEC economies will start to see a convergence of understanding as to what constitutes appropriate privacy protection, and that being certified as compliant with the APEC Privacy Principles will give companies confidence (if not certainty) that they are likely to be considered to be following each country's own privacy law as well.

Of course, it's an open question whether companies are going to want to engage in the APEC process

for this limited reassurance. Depending on how it's implemented, the accountability agent certification process has the potential to be costly and bureaucratic; in some ways, it resembles the unwieldy European *ex ante* notification and Binding Corporate Rules processes that the APEC process was ostensibly designed to avoid. Corporate willingness to pay for certification will probably be contingent upon how many countries move to formally participate in the CBPR system — so far, development of the CBPR framework has largely been driven by the United States.

From the standpoint of American consumers, who currently lack any substantive protections for most of our data, the CBPR system has the potential to ensure that our data is treated pursuant to the Fair Information Practice Principles [4], at least when it's shipped overseas (CBPR protections don't apply if the data is stored, processed, and transferred domestically). Of course, the costs of compliance will be passed on to us as well, and it remains to be seen how robust the privacy protections implemented by the CBPR system will be. One of CDT's criticisms of modern privacy protection both in the U.S. and abroad has been that it often favors process over substance: a team of lawyers is brought in to fill out forms and draft bewildering policy language, but at the end of the day, the company can pretty much do whatever it wants with your data. That's great for lawyers and privacy professionals, but it's not much help for consumers trying to exercise control over their information. If the end result of CBPR implementation is strictly monitored compliance with fundamentally weak privacy protections, the process will be a failure for all concerned (except the accountability agents, that is).

Fortunately, there are incentives for the system to provide meaningful protections for consumers — most notably, if the system isn't trusted by data protection authorities within APEC economies (and without), compliance with CBPRs won't make much headway into alleviating the restrictions on transnational data flows. While the CBPR system has been formally endorsed by the ECSG, the hard work on the details of implementation is just beginning, and we'll have a better sense of how CBPRs work in practice as the Joint Operating Panel is set up and accountability agents are approved to offer their accreditation services. In the meantime, CDT will continue to participate in the APEC process to further the worthy goals of the CBPR process: setting up a framework that allows for efficient and, well, frictionless [5] data flows, while ensuring that consumer privacy is meaningfully protected.

- Cross Border Privacy Rules
- CBPR
- Asia Pacific Economic Cooperation
- APEC

Source URL:
https://cdt.org/blogs/justin-brookman/410can-%E2%80%9Ccross-border-privacy-rules%E2%80%9D-trump-divergent-data-protection-laws

Links:
[1] https://cdt.org/personnel/justin-brookman
[2] http://www.cdt.org/issue/baseline-privacy-legislation
[3] http://www.apec.org/Groups/Committee-on-Trade-and-Investment/%7E/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx
[4] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf
[5] http://www.poynter.org/latest-news/media-lab/social-media/147638/with-frictionless-sharing-facebook-and-news-orgs-push-boundaries-of-reader-privacy/