

Department of Commerce Symposium
A DIALOGUE ON PRIVACY AND INNOVATION
Friday, May 7, 2010

Panel 1: Privacy, Innovation and Global Trade

Fred H. Cate

Over the past 15 years, we have witnessed the emergence of national, regional, and provincial privacy laws. All claim to reflect the OECD 1980 Guidelines,¹ but in reality *these laws are often very different*, even in countries within regions such as the European Union, that are implementing the same data protection directive. Yet for all of these new laws, *it is difficult to argue that individual privacy is better protected today than it was in 1980.*

I wish to highlight seven points about these laws:

1. *Privacy restrictions are imposing real impediments to trade in products and services that consumers want and expect.* These laws aren't limited to Europe² and aren't enacted at only the national level. Canadian provinces, for example, have adopted laws prohibiting the flow of certain personal data outside of Canada.³ As technologies are making our world smaller and bringing us closer together, divergent privacy laws are driving us farther apart.
2. The impact of increased privacy regulation may be greatest in information products and services—areas of significant innovation and importance to our economy—but it is certainly not limited to those. *Robust information flows are critical to most economic and social activities, conflicting privacy regimes are imposing burdens across society, and are likely to be even more burdensome as information technologies that ignore geographic boundaries—technologies such as cloud computing—proliferate.*
3. It is not just that data protection laws may be overly restrictive or bureaucratic, but also that a great deal of uncertainty surrounds many routine and critical data flows. *Both businesses and consumers need certainty.*
4. Government cannot solve these problems alone, but *the problems will not be solved without government involvement.* Government must take the lead on greater multinational cooperation on standard-setting, law-making, and enforcement. Where national laws conflict directly, government must not stand by and leave industry and individuals in the middle. We need a stronger and more appropriate U.S. voice at international data protection dialogues. I applaud the Department of Commerce for its leadership on the U.S.-EU Safe Harbor framework⁴ and the APEC privacy framework.⁵ *But there is much more to be done, and Commerce is the right agency to do it.*
5. U.S. government engagement in multinational data protection discussions will lack credibility until the United States both does a better job of explaining how and to what extent U.S. law protects privacy, and *puts in place a more rational, more consistent, and more substantive standard of privacy protection.* Again, the Department of Commerce is the appropriate agency to take the lead in advising the President on what such a law should entail.
6. Demands by the U.S. and other governments for personal data, especially those held by the private sector data, are expanding privacy concerns in general and concerns about multinational data flows in specific. *The unwillingness of some U.S. government agencies to admit of any*

substantive limits on their power to access private-sector data is fatal to effective multinational cooperation and to personal privacy. The government must address these issues because *only the government can*: there is nothing business can do to resolve other nations' concerns that personal data are vulnerable to government access.

7. *There is an urgent need to act and this is an opportune, even strategic time for such action.* There is at present a great deal of intellectual and political foment surrounding data protection around the globe. The EU data protection directive is under review. The FTC and Department of Commerce are conducting independent privacy inquiries. There is evidence of new collaboration among Data Protection Authorities and emerging agreement on enforcement. And we see an increased focus on new, less bureaucratic, approaches to data protection, including models based on data use, risk, and accountability.

I wish you success in these critical endeavors. Thank you.

Fred H. Cate is a Distinguished Professor and C. Ben Dutton Professor of Law at the Indiana University Maurer School of Law, and the director of Indiana University's Center for Applied Cybersecurity Research. He also serves as a senior policy advisor at the Centre for Information Policy Leadership at Hunton & Williams LLP. He may be reached at fcate@indiana.edu.

Notes

1. Committee of Ministers of the Organization for Economic Cooperation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, O.E.C.D. Doc. (C 58 final) (Oct. 1, 1980), available at http://www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html.
2. *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (Eur. O.J. 95/L281), arts. 25-26, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf and http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf.
3. See, e.g., Fred H. Cate, *Provincial Canadian Geographic Restrictions on Personal Data in the Public Sector*, Submitted to the Trilateral Committee on Transborder Data Flows, Sept. 2008, available at http://www.hunton.com/files/tbl_s47Details/FileUpload265/2312/cate_patriotact_white_paper.pdf.
4. U.S.-European Union Safe Harbor Framework (2000), available at <http://www.export.gov/safeharbor/>.
5. Asia-Pacific Economic Cooperation, *APEC Privacy Framework*, 2004/AMM/014rev1 (Nov. 2004), at 12, available at http://www.apec.org/apec/news_media/2004_media_releases/201104_apecminsendorseprivacyfrmwk.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/ministerial/annual/2004.Par.0015.File.v1.1