
These three significant and long-awaited government reports provide new insights into how regulators on both sides of the Atlantic view privacy challenges and the extent to which those views may be converging. In fact, many observers were surprised by the extent to which the three reports overlap.

For example, all three reports are prompted by similar issues and address similar problems—mainly, that current approaches to data protection have become ineffective in response to the rapid expansion in information technologies and applications.

All three reports explicitly recognize the tension between innovation and intrusion and acknowledge both the value and risks of information flows. Notice and choice, particular hallmarks of US privacy protection, but also found in European laws, come in for special (and well-deserved) criticism, especially in the EU and FTC reports. All three reports stress the importance of not over-focusing on notice and choice and ensuring that, when presented, notices are clear, concise, and simple to use.

The reports also recognize the importance of industry responsibility, self-regulation, and international cooperation in enforcement. All three focus new attention on accountability, rather than mere compliance, as a principled basis for data protection. And all three reports were issued in draft form and specifically invited public comment, reflecting the fundamental importance of individual and industry participation in formulating workable privacy policies.

These and other similarities appear to reflect growing convergence in transatlantic thinking about data protection issues. In fact, elements of each report sound themes historically associated with regulators on the other side of the Atlantic.

The EU report reflects concerns about the burden of complying with data protection laws, the tension between protecting privacy and not stifling innovation, inconsistency among member state laws, and the practicality of current restrictions on international transfers of data—concerns that seasoned privacy observers might find more reminiscent of US regulators.

Meanwhile, the FTC and Commerce reports expand the range of privacy principles to which companies might be held accountable, the data that might raise privacy issues (even if no unique identifiers are involved), and interests that should be protected—all points traditionally associated with European regulators.

The reports are, of course, not the only sign of convergence. The FTC joined with twelve European and other regulators in March 2010 to launch the Global Privacy Enforcement Network to facilitate multinational cooperation in enforcing privacy laws. In October, the FTC was officially admitted to the annual conference of data protection and privacy commissioners. Department of Commerce officials have been
increasingly visible in Europe and in discussions with European regulators, and European Commission Vice President Viviane Reding visited Obama administration officials in July to discuss opportunities for greater cooperation.

To be sure, neither the reports, nor the perspectives they reflect, are identical. The most obvious example is that the European Commission report focuses considerable attention on bringing national government law enforcement and national security activities within the practical scope of data protection law. The FTC report is silent on this subject, reflecting the fact that the FTC has no jurisdiction over government activities, but it is interesting to note that the Commerce report did address government surveillance because of its likely impact on privacy in cloud computing, even though the department also has no jurisdiction in this area. The EU also regards data protection as a fundamental right under human rights law, which approach is largely foreign to the USA.

Convergence, on the whole, is good for both individuals and business. We live and operate in an increasingly multinational world; it is good for law to catch up with that reality. To the extent that convergence leads to harmonization and greater certainty, it is a worthy goal. Moreover, by moving beyond mechanical notice and choice requirements and compliance with often duplicative if not conflicting legal requirements, these reports suggest that stronger, but potentially more rational and meaningful privacy protection, may be on the horizon.

The devil, as they say, is in the details, and while the move towards substantive convergence is real, we aren’t there yet. It remains to be seen whether regulators and politicians will be able to achieve the potential reflected in these reports and produce truly innovative approaches to protecting privacy.

We believe these reports are a promising start. It is good that regulators responsible for privacy and data protection on both sides of the Atlantic are recognizing similar issues, and that they are working positively together and with all stakeholders to craft solutions. We applaud their determination, and hope that the content in this and future issues of *International Data Privacy Law* will help inform their efforts.


*Advance Access Publication 24 February 2011*