O'Melveny

Alerts & Publications

Privacy Reforms on the Horizon: A Primer on Pending E.U. and U.S. Privacy Proposals

December 16, 2010

For global companies that collect, broker, or use consumer data, the first several months of 2011 may prove critical. Both the European Union and the United States have announced plans to revise their data-protection laws or policies and those changes could, of course, require alterations in current business practices. Thus, the potential implications of new privacy requirements are great—both jurisdictions contemplate reforms that will affect broad categories of entities and that could affect companies around the world. To take one example, the FTC's discussion of a new "Do Not Track" mechanism has already sparked debate over its potential impact on advertising-supported business models.

Moreover, the EU and the US approaches to privacy reform appear to be different in important respects, thus increasing the risk of business disruption. Accordingly, rapidly-approaching comment periods offer companies a critical opportunity to advocate for data-protection policies that will work best in a global economy, while creating a record for further governmental action or review.

Three key proposals form the basis for the anticipated changes in data-protection legislation and enforcement in Europe and the U.S. The European Commission issued a White Paper outlining its "approach for modernizing the EU legal system for the protection of personal data" on November 4, 2010.[1] Next, on December 1, 2010, the Federal Trade Commission proposed for comment its own "normative framework for how companies should protect consumers' privacy" based on the three core principles of privacy by design, consumer choice, and transparency.[2] Finally, the U.S. Department of Commerce today released its "Green Paper" in which it "provides an initial set of recommendations to help further the discussion and consider new ways to create a stronger commercial data privacy framework."[3] Of particular note is its recommendation of a new entity—The Privacy Policy Office.

As a starting point, this Client Alert notes several key similarities and differences between the proposals.

Key Similarities:

• Balancing Priorities: All three proposals balance increased consumer protection against the benefits of data collection, such as innovation, job creation, and economic growth.[4]

• "Privacy By Design": The proposals all support the notion of "privacy by design"—that companies should adopt certain best practices for protecting consumer data as an inherent part of the creation of their products and services. The FTC proposal, for example, suggests that "[c]ompanies should incorporate substantive privacy and security protections into their everyday business practices and consider privacy issues systemically, at all stages of the design and development of their products and services."[5] These protections might include adopting reasonable security for consumer data,

collecting only the data needed for a specific purpose, retaining data only as long as necessary to fulfill that purpose, and implementing reasonable procedures to promote data accuracy.[6] The European Commission White Paper, similarly, notes that the Commission plans to further explore the possibility of "concrete implementation of the concept of 'Privacy by Design.'"[7] The Commerce Department, meanwhile, suggests that a newly-established Privacy Policy Office (PPO) would help stakeholders implement industry standards and best practices, which could draw on the Privacy by Design approach.[8]

• Increased Transparency: All three issuing bodies agree that companies should increase transparency with regard to the ways in which they collect and use consumer data, part of what the Commerce Department referred to as a "Privacy Bill of Rights".[9] To improve transparency, the proposals recommend:

o shorter, clearer, and more standardized privacy policies;[10]

o increased consumer access to the information held about them;[11]

o increased efforts to educate consumers about data collection and use;[12] and

o simplified consumer choice mechanisms.[13]

Key Differences:

• Legislation vs. Self-Regulation: The proposals all recommend different levels of legislative involvement in privacy reforms:

o The European Commission will seek proposed privacy legislation in 2011,[14] although it also notes the potential for certification schemes to help prove individual data controllers' fulfillment of privacy obligations.[15]

o The FTC has publicly declared that "self-regulation of privacy **has not** worked adequately and **is not** working adequately for American consumers."[16] And, while it does not actively recommend legislative action, the FTC seeks comment on whether it should recommend legislation requiring an "effective uniform choice mechanism" such as a "Do Not Track" program if the private sector does not do implement one voluntarily.[17]

o The Commerce Department recognizes that "in certain circumstances . . . more than self-regulation is needed," but still recommends "that the United States Government recognize a full set of Fair Information Practice Principles (FIPPs), as a foundation for commercial data privacy."[18] The report acknowledges the popular call for baseline privacy legislation, but also cautions against the danger of "locking-in outdated rules that would fail to protect consumers and stifle innovation."[19] The report also notes that any legislation should provide "safe harbor" to companies "that adhere to voluntary, enforceable codes of conduct."[20] Thus, the Green Paper expressly favors the creation of "voluntary codes of conduct" created by the private sector.[21] The newly-recommended Privacy Policy Office would help convene stakeholders and work with the FTC to help create these voluntary, but enforceable codes of conduct. Still, the Secretary of Commerce's statement released in conjunction with the Green Paper said that, "Self-regulation without stronger enforcement is not enough."[22] The Department also asks for consideration of a

new Federal commercial data security breach law. In addition, the Department is focused on updating existing legislation. It recommends, for example, that the Obama Administration review the Electronic Communications Privacy Act to address privacy protection in cloud computing and location-based services. [23]

• Enforcement: The proposals also differ in the way that privacy policies will be enforced:

o The European Commission expresses a continued support for the Data Protection Authorities (DPAs) as the primary enforcers of data protection principles, and the Article 29 Working Party as the entity to ensure "the uniform application of EU data protection rules at a national level."[24] The White Paper advocates for a stronger role for the DPAs and increased cooperation between DPAs where cross-border transactions are involved.[25]

o The FTC report suggests that the Commission will continue to rely on its existing authority under Section 5 of the Federal Trade Commission Act to continue its privacy enforcement efforts.[26]

o The Commerce Department concedes that the FTC "should remain the lead consumer privacy enforcement agency for the U.S. Government," but asks whether the FTC should be given any additional rulemaking authority if voluntary enforceable codes are not developed.[27] Moreover, the Department asks whether state attorneys general should be given authority to enforce national privacy legislation.[28]

Extraterritorial Impact:

The proposals also all contemplate that domestic privacy policies will have extraterritorial impact, in various ways. The European Commission notes that "the fact that the processing of personal data is carried out by a data controller established in a third country should not deprive individuals of the protection to which they are entitled."[29] The Commission addresses this concern in part by suggesting the adoption of uniform rules for assessing the level of data protection in a third country, and the "development and promotion of international legal and technical standards for the protection of personal data."[30] The FTC proposal does not make any direct recommendations regarding international privacy policies, but notes the FTC's participation in international initiatives, including the Global Privacy Enforcement Network (GPEN).[31] And the Commerce Department calls for "global interoperability" of privacy laws and policies, recognizing that "[w]hile the privacy laws across the globe have substantive differences, these laws are frequently based on the same fundamentals."[32] The Department thus recommends that the U.S. look to the Asia-Pacific Economic Cooperation (APEC) Data Privacy Pathfinder project as a model for identifying common privacy principles among countries with diverging legal frameworks.[33] The Secretary of Commerce's statement today expressly called for "steps to bridge the different privacy approaches among countries, which can help us increase the export of U.S. services and strengthen the American economy."[34]

***

The proposals explicitly cover fairly broad categories of entities, but their potential impact is even more far-reaching. The European Commission notes that the EU Data Protection Directive "applies to all personal data processing activities in Member States in both the public and private sectors," and proposes that data protection rules be extended further to cover police and judicial cooperation in criminal matters.[35] The FTC proposal limits its coverage to "online and offline **commercial** entities that collect, maintain, share, or otherwise use consumer data that can be reasonably linked to a specific consumer, computer or device."[36] The Commerce Department report does not

identify the scope of its coverage, but emphasizes its focus on a "comprehensive national framework for commercial data privacy."[37] Regardless of the scope of any of the proposals' direct coverage, however, it is clear that any entity that collects, brokers, or uses consumer data may be affected by the upcoming privacy reforms.[38]

Still, much remains to be decided. All three reports represent only proposed frameworks, guidelines and recommendations. The FTC proposal, for example, "is intended to inform policy makers, including Congress, as they develop solutions, policies, and potential laws governing privacy, and guide and motivate industry as it develops more robust and effective practices and self-regulatory guidelines."[39]

The timeframe for public input and comment, however, is short and the deadlines are fast approaching. The EU has a **January 15, 2011** deadline in place. Similarly, the FTC seeks comments on each component of its proposed framework by **January 31, 2011** and plans on releasing a final report later next year. And today's Commerce Department report requires that comments be submitted by **January 28, 2011**.

Accordingly, and in light of the approaching deadlines for comment, companies in every sector should consider whether they will be affected by any of the proposed privacy reforms and whether such potential impact warrants direct participation in the public comment process.

[1] Commission Proposal for a Comprehensive Approach on Personal Data Protection in the European Union, COM (2010), 609/3 (Nov. 11, 2010), at p. 5, *available* at http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf(hereinafter "EC Proposal").
[2] Preliminary FTC Staff Report, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers" (Dec. 1, 2010), *available* at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (hereinafter "FTC Report").
[3] Report of the Department of Commerce Internet Policy Task Force, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework" (Dec. 16, 2010), *available* at http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf(hereinafter "Commerce Dept. Report").
[4] FTC Report at iv; EC Proposal at 2; Commerce Dept. Report at 3.
[5] FTC Report at 44.
[6] FTC Report at 44-48.
[7] EC Proposal at 2.2.4.
[8] *See* Commerce Dept. Report at 45-47.
[9] Press Release, US Department of Commerce, Commerce Department Unveils Policy Framework for Protecting Consumer Privacy Online While Supporting Innovation: Calls for consideration a new set of principles—A "Privacy Bill of Rights," (Dec. 16, 2010) *available* at http://www.commerce.gov/news/press-releases/2010/12/16/commerce-department-unveils-policy-framework-protecting-consumer-priv(hereinafter "Commerce Dept. Press Release").
[10] *See* EC Proposal at 2.1.2; FTC Report at 70-72; Commerce Dept. Report at 31-34.
[11] FTC Report at 72-76; EC Proposal at 2.1.3.
[12] FTC Report at 78-79; EC Proposal at 2.1.4.
[13] FTC Report at 69; Commerce Dept. Report at 31-32.
[14] EC Proposal at 3.
[15] EC Proposal at 2.2.5.
[16] Jon Leibowitz, Chairman, Fed. Trade Comm'n, Preliminary FTC Staff Privacy Report: Remarks

of Chairman Jon Leibowitz as Prepared for Delivery (Dec. 1, 2010), *available* at http://www.ftc.gov/speech
[17] FTC Report at 69.
[18] Commerce Dept. Report at iv, 4.
[19] Commerce Dept. Report at 29.
[20] Commerce Dept. Report at 41.
[21] Commerce Dept Report at 5.
[22] Commerce Dept. Press Release
[23] Commerce Dept. Report at 63.
[24] EC Report at 2.5.
[25] EC Report at 2.5.
[26] FTC Report at viii.
[27] Commerce Dept. Report at 72-73.
[28] Commerce Dept. Report at 74.
[29] EC Report at 2.2.3.
[30] EC Report at 2.4.1-2.4.2.
[31] FTC Report at 18.
[32] Commerce Dept. Report at 6-7.
[33] Commerce Dept. Report at 56-57.
[34] Commerce Dept. Press Release
[35] EC Report at 2.3.
[36] FTC Report at v (emphasis added).
[37] Commerce Dept. Report at 22.
[38] See FTC Report Appendix C at C-1.
[39] FTC Report at i.