LegalBytes

BAKER & McKENZIE

Special Edition

February 2014

Print Version

For more information, please contact:

Brian Hengesbaugh
Partner, Chicago
Tel: +1 312 861 3077
Brian.Hengesbaugh@bakermckenzie.com

Amy de La Lama
Of Counsel, Chicago
Tel: +1 312 861 2923
Amy.deLaLama@bakermckenzie.com

U.S. Federal Trade Commission is serious about enforcement of the U.S.-EU Safe Harbor Framework

The U.S. Federal Trade Commission ("FTC") announced on January 21, 2014 that 12 companies from a wide array of industries handling a variety of categories of personally identifiable information ("PII") agreed to settle charges that they violated the U.S.-EU Safe Harbor Framework regarding the collection, use, and retention of PII from EU member countries ("Safe Harbor"). Specifically, the FTC alleged that the companies deceptively claimed in their privacy policies or by their use of the Safe Harbor certification mark that they were in compliance with the Safe Harbor. The settlement agreements, or "consent orders," which are effective for 20 years, require, among other things, that the companies not misrepresent their association with any government sponsored privacy or security program and submit a report detailing the manner and form of compliance with the order and all documents relating to compliance with the order. As is explained in more detail below, these terms could have far-reaching consequences for the signing organizations and illustrate how the FTC has come to exercise its privacy enforcement authority.

EC Report Trust-Building Recommendations

The announcement of these 12 consent decrees closely follows a recent report by the European Commission ("EC") setting forth specific recommendations, including a call for greater enforcement, to enhance trust in Safe Harbor and could be viewed as a direct response to these recommendations. Following the Edward Snowden surveillance incident, the surrounding media attention and member country concerns prompted the EC to evaluate the functioning of Safe Harbor. In November 2013, the EC issued its Safe Harbor Report, which reaffirmed the continued commercial significance of Safe Harbor and outlined 13 recommendations to enhance trust in the framework. Among the recommendations, greater enforcement is a consistent theme. In particular, the EC recommends the investigation of false claims of Safe Harbor certification to avoid weakening the credibility of the Safe Harbor. The Safe Harbor Report also calls for *ex officio* investigations of a percentage of Safe Harbor participants to ensure compliance and continued investigation of non-compliance findings one year after such findings. The combination of the recent enforcement activity coupled with

Karen Sewell
Associate, Chicago
Tel: +1 312 861 8228
Karen.Sewell@bakermckenzie.com

Brandon Moseberry
Associate, Chicago
Tel: +1 312 861 8265
Brandon.Moseberry@bakermckenzie.com

Lothar Determann
Partner, San Francisco
Tel: +1 650 856 5533
Lothar.Determann@bakermckenzie.com

Michael Egan
Associate, Washington, D.C.
Tel: +1 202 452 7022
Michael.Egan@bakermckenzie.com

this emphasis on enforcement by the FTC suggests an uptick on enforcement related to Safe Harbor in the coming months and years.

Increasing FTC privacy enforcement through consent decrees

This latest group of consent decrees is consistent with broader privacy enforcement actions by the FTC in the last few years. The trend has been for the FTC to primarily settle privacy actions rather than take them to trial. However, these ever-growing number of consent decrees are creating a type of federal privacy common law that can be instructive beyond the settling parties. For the settling parties, the consent decrees, which have a term of 20 years, could be better viewed as marking the start of heightened FTC privacy oversight rather than as a capstone to a privacy investigation. The fact is that the consent decrees provide the FTC with greater enforcement authority over settling parties than is available to the FTC at law.

Although originally founded for purposes of enforcing antitrust laws, the FTC has evolved over time to focus more generally on consumer protection issues. The FTC has relied on its consumer protection mandate to create a federal common law of privacy along with enforcing several specific privacy statutes, such as the CAN-SPAM Act and Children's Online Privacy Protection Act. It also is specifically charged with enforcing Safe Harbor along with the Department of Commerce.

Sections 5 and 6 of the FTC Act gives the FTC the authority to investigate "unfair or deceptive acts or practices." 15 U.S.C. §§ 45(a)(1), 46(a)-(b). In exercising its Sections 5 and 6 authority, the FTC takes the position that misrepresenting why information is being collected from consumers or how the information will be used constitutes a deceptive practice. The FTC may investigate and enter an enforcement action against an organization it believes has failed to keep its privacy promises and, thus, committed a deceptive practice. Although FTC enforcement actions could lead to a trial, recently the more common result, as with the recent Safe Harbor cases, has been settlement through consent decrees and accompanying consent orders.

The terms of a consent decree vary depending on the violation, but typically detail what remedial actions the organizations must take and what practices they are prohibited from engaging in for the 20-year term of the decree. To ensure compliance with the terms of the consent decree, organizations often agree to be subject to third-party audits of their privacy and security practices. The scope of these audits is not limited to just the privacy practice that prompted the settlement with the FTC but reaches all of the organization's data privacy and security practices. Most importantly, although the FTC does not have authority to directly levy fines for deceptive privacy practices, any violation of the terms of the consent decree could trigger civil penalties of up to $16,000 per violation per day. 15 U.S.C. § 45(m)(1)(A); 16 CFR § 1.98(d). In sum, by entering into a consent decree, organizations may avoid

admitting fault, but sign up for an individualized privacy regime and terms that are far from a “light touch”.

Given this increased focus on enforcement, it is an especially critical time for companies to ensure they have their data privacy, and particularly their Safe Harbor “house” in order. To reduce the risk of an enforcement action and the resulting burdens of 20 years of third-party audits and risk of civil penalties that accompany a consent decree, companies should prioritize data privacy compliance and develop appropriate safeguards at every relevant portion of their business.