February 5, 2014

FTC Settles With Businesses Who Allegedly Misrepresented US-EU Safe Harbor Certification

Beware: Even if your company substantially complies with the Privacy Principles of the US-EU Safe Harbor, failure to annually re-certify can land you in hot water.

Twelve US businesses—ranging from sports teams, to software and consumer product companies, to Internet giants—have recently agreed to settle Federal Trade Commission (FTC) charges that they falsely claimed compliance with the US-EU Safe Harbor, an international privacy framework.

BACKGROUND

The US-EU Safe Harbor is a voluntary, simplified and cost-effective means for US entities to comply with European privacy regulations. The European Commission's Directive on Data Protection[1] prohibits the transfer of personal data to non-European Union countries that do not meet the European Union (EU) "adequacy" standard for privacy protection. The US-EU Safe Harbor framework, developed by the US Department of Commerce in consultation with the European Commission, is a voluntary, streamlined and cost-effective means for US entities to self-certify compliance and be deemed to have "adequate" privacy protection under the EU standard. Such a certification enables US entities to engage in uninterrupted business dealings with the EU and avoid prosecution by EU member state authorities for data transfers to the United States due to the failure of US law generally to meet the "adequacy" requirement. All 28 member states of the EU are bound by the European Commission's finding of "adequacy" for compliant organizations.

To obtain and maintain certification under the Safe Harbor, participating organizations must both (1) comply with the seven Safe Harbor Privacy Principles,[2] and (2) annually self-certify their compliance to the US Department of Commerce.

Participating organizations can highlight their compliance with the US-EU Safe Harbor to consumers by, among other ways, displaying the Safe Harbor mark on their websites or citing their certification in their privacy policies.

Enforcement authority for the Safe Harbor is held by the FTC, certain other US government agencies and/or state authorities, depending on the participating entity's industry sector.

THE FTC SETTLEMENT

The FTC recently filed complaints against 12 US companies for allegedly violating Section 5 of the FTC Act, which bans entities from engaging in unfair or deceptive acts or practices in interstate commerce. According to the complaints, these companies falsely represented that they held current Safe Harbor certifications, through statements in their privacy policies or display of the Safe Harbor certification mark, when their certifications had actually lapsed due to failure to re-certify. Such conduct does not necessarily mean that the companies committed any substantive violations of the Safe Harbor Privacy Principles, only that they misrepresented the status of their certifications.

---

[1] Directive 95/46/EC.

[2] The Safe Harbor Privacy Principles are: (1) notice, (2) choice, (3) onward transfer (transfers to third parties), (4) access, (5) security, (6) data integrity and (7) enforcement.

On January 21, 2014, the FTC announced the parties' intent to enter into settlement agreements regarding the FTC's charges. The proposed settlement agreements prohibit the companies "from misrepresenting the extent to which they participate in any privacy or data security program sponsored by the government or any other self-regulatory or standard-setting organization."[3]

WHAT YOU NEED TO KNOW ON SELF-CERTIFYING COMPLIANCE WITH THE US-EU SAFE HARBOR FRAMEWORK

1. Confirm Eligibility for the Safe Harbor: Any US organization that is subject to the jurisdiction of the FTC, or that is a US air carrier or ticket agent subject to the jurisdiction of the Department of Transportation, may participate in the Safe Harbor.

2. Develop a Safe Harbor-Compliant Privacy Policy Statement: As a prerequisite for submitting a self-certification to the Department of Commerce, develop a Safe Harbor-compliant privacy policy and maintain that privacy policy.

3. Establish an Independent Recourse Mechanism: A self-certifying organization needs to establish, prior to self-certification, an independent recourse mechanism to investigate and remedy disputes between consumers and the organization, and redress problems arising out of the organization's failure to comply with the Privacy Principles.

4. Ensure That the Verification Mechanism Is in Place: A self-certifying organization must have procedures in place for verifying compliance; either self-assessment or third-party assessment verification programs are acceptable.

5. Designate a Safe-Harbor Contact: A self-certifying organization must provide a contact to handle any questions, complaints, access requests or other issues arising under the Safe Harbor.

6. Annually Reaffirm the Commitment to the Safe Harbor Framework: A self-certifying organization must reaffirm—through the Safe Harbor website, by email or by sending a letter—its pre-existing certification on or before the anniversary of the date on which the original self-certification was finalized.

****

For more information, please contact any of the following members of Katten's **Technology Practice**.

Doron S. Goldstein
New York
+1.212.940.8840
doron.goldstein@kattenlaw.com

Leonard A. Ferber
Chicago
+1.312.902.5679
leonard.ferber@kattenlaw.com

Tanya L. Curtis
Chicago
+1.312.902.5593
tanya.curtis@kattenlaw.com

Claudia Callaway
Washington, DC
+1.202.625.3590
claudia.callaway@kattenlaw.com

[3] http://www.ftc.gov/news-events/press-releases/2014/01/ftc-settles-twelve-companies-falsely-claiming-comply.