WILMERHALE

FTC Settles Deception Charges Relating to Privacy Program Claims

FEBRUARY 22, 2017

On February 22, 2017, the FTC settled charges with three companies that, according to the FTC, deceptively claimed that they participated in the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (APEC CBPR). The proposed consent orders would prohibit each company from making any misrepresentations regarding its participation in a government or self-regulatory privacy program and impose compliance and reporting obligations on each company. The proposed orders are open for public comment for 30 days.

APEC's CBPR system and TRUSTe are but two examples of voluntary privacy programs sponsored by governmental or self-regulatory bodies. APEC's CBPR system is designed to facilitate data flows among APEC member countries in a privacy-respecting way. Companies that choose to participate in the CBPR must develop privacy policies that follow the APEC Privacy Framework, which rests on nine principles: preventing harm; notice to individuals; limited collection of personal information, limited use of personal information and individual choice, information integrity; security safeguards; access and correction; and accountability. Companies that seek to participate in the APEC CBPR system must undergo a review by an APEC-recognized accountability agent, which certifies companies that meet the standards. The three companies, however, were not and had never been certified, according to the complaints.

Companies may participate in such programs to gain consumer confidence or so they can more easily transfer data internationally. Additionally, regulators may view self-regulation as a nimbler approach to privacy protection than enforcement actions. As then-FTC Commissioner Thomas Rosch explained in 2009, self-regulation "can offer flexibility and timeliness that may not always be present in enforcement actions" and leverage the judgment and experience of industry participants. But as the FTC's actions of February 22, 2017, indicate, if the FTC believes that a company claims it complies with a voluntary privacy program when, in fact, it doesn't, the FTC may level deception charges under Section 5 of the FTC Act.

The three companies targeted in these enforcement actions were Sentinel Labs, Inc., which provides network security software; SpyChatter, Inc., which provides a private messaging app; and Vir2us, Inc., which provides cybersecurity software. According to the FTC, Sentinel One's privacy

policy stated that its policies complied with the CBPR system. According to the FTC, that statement was false. Similarly, the FTC alleged that both SpyChatter and Vir2us claimed in their privacy policies that they followed the CBPR system, when in fact they were never CBPR certified.

These are not the first Section 5 deception charges brought against companies that, in the FTC's view, falsely claimed they were certified by a governmental or self-regulatory privacy program. For example, before it was struck down by the European Court of Justice, the US-EU Safe Harbor framework facilitated data transfers from the European Union to the United States. Between 2009 and 2015, the FTC brought 39 actions based on alleged misrepresentations about participation in the Safe Harbor. Some of these companies allegedly never participated in Safe Harbor, while others were Safe-Harbor certified but did not renew their certification.

Even though some privacy programs may be voluntary, they are not toothless. The FTC will likely continue to take action against companies that claim they participate in voluntary privacy programs when, in fact, they do not. This includes claiming to be certified under the new US-EU Privacy Shield Program, which replaced the Safe Harbor last year.