Bloomberg BNA

Electronic Commerce & Law Report™

Privacy

Attorneys Offer Tips for Avoiding FTC Privacy Investigations and Responding to Inquiries

Companies can take specific steps to avoid privacy investigations by the Federal Trade Commission, including ensuring that they adopt privacy-by-design principles and live up to privacy and security promises made to consumers, panelists said March 9.

Businesses should also be aware of sources that trigger FTC scrutiny, including media coverage, congressional interest, consumer-filed complaints, and the FTC's own ''top 10'' list of consumer complaints, Alysa Z. Hutnik, partner at Kelley Drye & Warren LLP, in Washington, said at the International Association of Privacy Professionals Global Privacy Summit.

In addition, companies should take a Civil Investigative Demand (CID) or access letter from the FTC seriously, attorneys advised

One enforcement theme that is emerging is the ''ecosystem,'' or whether each party that handles data is fulfilling its consumer protection duties, Hutnik said. She added that mobile devices will continue to attract more FTC enforcement attention.

Investigation 'Triggers' to Avoid. Hutnik listed five ''privacy triggers'' to avoid:

1. a material misrepresentation in a privacy policy;

2. inadequate safeguards for personally identifiable information (PII);

3. inadequate consumer choices or control over the use of PII;

4. inadequate disclosures about the sharing of PII; and

5. unauthorized access to PII by third parties.

The FTC likes to find ''low-hanging fruit,'' added Benita A. Kahn, partner at Vorys, Sater, Seymour and Pease LLP, in Columbus, Ohio. ''Don't be a low-hanging fruit and become a poster child for an issue,'' she advised.

She emphasized understanding what has been important to the FTC in the past, discussing the agency's enforcement actions against Google (16 ECLR 1779, 10/26/11),Twitter, and Facebook (16 ECLR 1983, 12/7/11).

Hutnik added that the Google enforcement action highlights the ''silo effect,'' or the lack of coordination between a company's legal department and its technology and engineering teams.

It is not just big companies that are receiving the FTC's attention, Kahn said. ''Don't assume that because you're small you're safe,'' she advised.

Avoiding Becoming a Target. The speakers offered three tips to avoid becoming the target of an FTC investigation:

1. ''Bake It In'' or privacy-by-design;

2. empowering consumer choice; and

3. ''say what you do and do what you say.''

Hutnik said that companies need to address their privacy programs in ''a thoughtful, comprehensive way instead of as an afterthought.'' Conducting a data risk assessment is one of the hardest things to do, she commented, and it is bubbling up to be a key issue in investigations.

Kahn added that the FTC is broadening its definition of PII with each consent order.

The process of selecting service providers is also important, Hutnik said. The FTC looks for a due diligence process in place before a company hires a service provider, as well as a monitoring, she said.

Empowering choices for consumers involves simplifying choice and providing opt-out provisions, according to the speakers' presentation materials.

The last tip, ''say what you do and do what you say,'' involves transparency as well as disclosures and consent to any new or additional sharing of data, Kahn explained.

What to Do When You Receive a Letter. ''Time matters'' when a company receives a CID or access letter from the FTC, Hutnik said, explaining that a ''20-day clock'' begins ticking. The first steps a company should take include reviewing the letter, hiring expert counsel, and identifying an internal team with knowledge of the situation, she added.

The next step, the speakers explained, involves assessing the scope of the investigation and CID, including crafting a letter to the FTC that identifies which requests are an unreasonable burden on the company. Petitions to limit or quash requests for information from the FTC must be filed no later than 20 days after service of the CID unless the FTC provides a written extension, according to the panel presentation materials.

Immediately prepare and distribute a legal hold memo to preserve relevant information, Hutnik advised. She also said to suspend auto-delete features in email. ''Keep in mind that the FTC is very technologically savvy,'' Kahn added.

The next steps include producing responsive documents, filing a privilege log, and negotiating with the

FTC staff attorney concerning the items in the log, Hutnik said. She added that a proposed revision to the FTC Rules of Practice requires a detailed log and mandates that the parties meet and confer on privilege issues 10 days after process is received or before the deadline for filing the petition to quash, whichever comes first.

Telling Your Side of the Story. Start following up and telling your side of the story at the moment you receive an FTC letter, Kahn said.

Hutnik advised providing a ''white paper,'' or a written narrative, before the FTC staff makes a recommendation on the case.

Ensure that privacy protections are built-in, Hutnik advised, and request a meeting with staff to discuss the case.

''Don't be shy about making remedial changes during the investigation,'' Hutnik added.

BY KATIE W. JOHNSON

Further information on the International Association of Privacy Professionals is available at https://www.privacyassociation.org/.

  ECLR ISSN 1098-5190