Thompson & Knight Impact®

ATTORNEYS AND COUNSELORS

Client Alert *August 13, 2013*

TIME TO TUNE-UP YOUR PRIVACY POLICY?
FTC, STATES INCREASE ENFORCEMENT OF PRIVACY AND DATA SECURITY POLICIES

The Federal Trade Commission ("FTC") and state attorneys general are escalating their consumer privacy enforcement efforts. In the last three years alone, the FTC has brought 32 enforcement actions against organizations for violating consumers' privacy rights or for misleading consumers by failing to maintain security for sensitive consumer information. Increased enforcement in this area is no coincidence—newly instated FTC chair, Edith Ramirez, has insisted that data privacy and protection are top priorities for the Commission and will continue to be priorities for the foreseeable future. These increased enforcement efforts by the government are forcing businesses to take a serious look at their privacy policies and implementation, as compliance is the best risk management tool available for avoiding the costs of an enforcement action and potential civil penalties.

The FTC enforces consumers' privacy rights through Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce, and more than 30 other laws, rules, and guides concerning consumers' privacy. The FTC has brought charges against companies with inadequate privacy practices and companies that materially change their privacy policies without notifying (and in some cases without obtaining consent from) users. Recently, the FTC has taken particular interest in companies that do not adhere to their existing privacy and data usage policies. The FTC has held that businesses who do not adhere to their privacy policies are violating the FTC Act by committing deceptive acts.

The FTC's aggressive stance is shown by its recent enforcement actions. In 2012, Google settled with the FTC for alleged privacy violations and made history by receiving the largest fine ever assessed for the violation of an FTC consent order—$22.5 million. In November, a management services company paid a fine and was required to implement a data security program with independent third-party audits for the next 20 years. More recently, mobile device manufacturer, HTC, agreed to settle FTC charges with respect to HTC's mobile device software. The settlement requires HTC to develop and release software patches to fix vulnerabilities found in millions of HTC devices, to establish a comprehensive security program designed to address security risks, and to undergo independent security assessments every other year for the next 20 years.

The FTC also monitors adherence to privacy policies when companies undergo a change of control or sell assets that include consumer information. In the Borders Group bankruptcy proceeding (and sale of assets to Barnes & Noble), the FTC recommended that any transfer of personal information only take place with consent of Borders' customers or with significant restrictions on the transfer and use of the information. Ultimately, Borders was required to provide its customers with e-mail notification of the sale and 15 days to opt-out of the transfer.

More recently, states have also jumped on the privacy policy enforcement bandwagon. So far, California has led the way in privacy policy and data protection enforcement. California has created a Privacy Enforcement and Protection Unit to focus on protecting consumer and individual privacy through civil prosecution of state and federal privacy laws. This unit has been active in policing companies' privacy practices. Last year, Attorney General Kamala D. Harris sent notices to up to 100 providers of mobile apps claiming that their apps do not comply with California's privacy laws. For example, in December 2012, California filed suit against a major airline carrier for failure to display a privacy policy on its mobile application.

These enforcement actions illustrate the agencies' increasingly aggressive stance regarding consumer data protection. The FTC and state attorneys general are pushing for companies to be more diligent in protecting sensitive consumer information, instating privacy and data handling policies, and making sure that companies follow those policies.

In light of the increased enforcement activity in this area, companies may wish to review their current privacy and data handling practices to: (1) ensure that the privacy and data policies are up to date; (2) identify the information collected by the company, whether related to customers, employees, or third parties; (3) identify when the company shares information collected by the company; (4) identify any restrictions on the transfer of such data; and (5) confirm that the privacy and data policies are actually being practiced.

If you have any questions about the information contained in this Client Alert, please contact the Thompson & Knight attorney with whom you regularly work or one of the attorneys listed below for more information.

CONTACTS:

Stephen E. Stein
214.969.1209
Stephen.Stein@tklaw.com

Ira L. Herman
212.751.3045
Ira.Herman@tklaw.com

Deborah L. Lively
214.969.1767
Deborah.Lively@tklaw.com

Craig Carpenter
214.969.1154
Craig.Carpenter@tklaw.com

Mackenzie S. Wallace
214.969.1404
Mackenzie.Wallace@tklaw.com