EmTech Perspectives

Babst | Calland
Attorneys at Law

Ashleigh H. Krick

FTC Investigation of Twitter for Alleged Privacy Violations Reinforces Need for Strong Privacy Policies and Practices

On August 3, 2020, Twitter disclosed in a regulatory filing that it is under investigation by the Federal Trade Commission (FTC) for allegations that the company used user phone numbers and email addresses for targeted advertising in violation of a 2011 Consent Agreement. Twitter estimates that it could face $150 to $250 million in losses due to legal fees and enforcement penalties resulting from this matter.

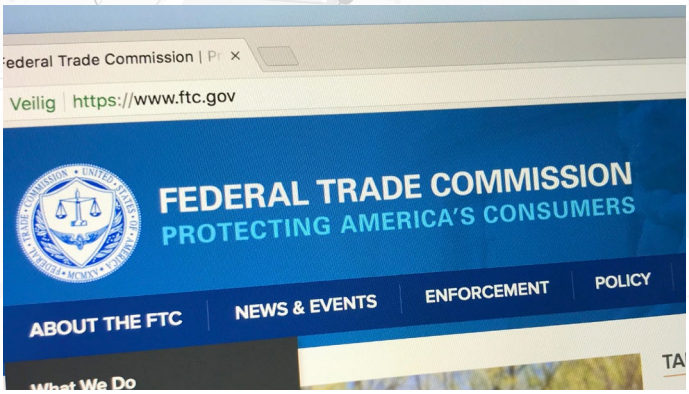
The 2011 Consent Agreement resolved charges that Twitter violated the Federal Trade Commission Act (FTC Act) when hackers obtained administrative control of Twitter allowing them access to non-public user information, private tweets, and the ability to send out fake tweets from any user's account. The FTC found that Twitter's actions neither upheld statements in its privacy policy, nor provided reasonable and appropriate security to prevent unauthorized access to non-public user data and honor the privacy choices of its users.

> ...Both GDPR and CCPA are **intended to require businesses to provide information to consumers** regarding the personal data they collect, how they use or sell that data, and opting-out of data collection.

The 2011 Consent Agreement barred Twitter for 20 years from misleading users about the extent to which it protects the security, privacy, and confidentiality of nonpublic consumer information, and required that the company take administrative controls to prevent unauthorized access. The 2011 Consent Agreement also required Twitter maintain a comprehensive information security program that is subject to review by a third-party auditor.

Although the FTC-Twitter matter will likely remain open for some time, this incident only highlights the importance of establishing strong privacy policies and practices, especially in a time of increased scrutiny surrounding cybersecurity. The FTC is the head federal agency in the United Stated charged with bringing enforcement actions against businesses that engage in unfair or deceptive practices that put consumers' personal data at unreasonable risk. However, recently, domestic and international policymakers and regulators are becoming increasingly involved in establishing requirements for the protection of consumer privacy.

In 2016, the European Union (EU) enacted the General Data Protection Act (GDPR) providing EU residents data protection and privacy rights. Two years later, California enacted a similar law— the California Consumer Privacy Act (CCPA)— providing California residents with enhanced privacy rights and protections and imposing obligations on businesses that collect the personal information of California residents. Both GDPR and CCPA are intended to require businesses to provide information to consumers regarding the personal data they collect, how they use or sell that data, and opting-out of data collection. And, both GDPR and CCPA provide consumers with rights, such as requesting deletion of their personal data, and avenues for submitting complaints and seeking enforcement of their rights. Many other states are likely to follow suit.



As consumer data privacy continues to be a top priority among federal and state legislatures and regulators, businesses must keep up with the increasing legal obligations, best practices, and consumer expectations surrounding privacy and data security. Businesses should evaluate their current privacy policies and practices to determine if sufficient measures and safeguards are in place for privacy protection, even if not subject to a particular privacy law. As the FTC-Twitter matter show cases, the FTC has broad enforcement authority to hold businesses accountable to the statements made in their privacy policies, regardless of any overarching federal or state privacy law. The manner in which businesses handle consumer data privacy and security as compared to industry best practices and their peers will be subject to scrutiny in the years to come as data breaches continue to make headlines and more privacy laws are enacted.

Bottom line: Whether or not your business or organization falls within the scope of the GDPR or CCPA, these laws are only the beginning and businesses should be focused on establishing strong privacy policies and practices now in a manner that is consistent with current guidance and best practices.

> ...this incident only highlights the importance of establishing **strong privacy policies and practices**, especially in a time of increased scrutiny surrounding cybersecurity.

Babst Calland's Emerging Technologies Group has recently created EmTech Law Blog which contains news, articles and legal and regulatory information published by our attorneys in an effort to provide timely legal and business information on issues impacting companies developing or investing in new technologies, new companies, and new ideas.

To subscribe, simply register at EmTech Law Blog and add your e-mail address. Whenever we post information, you'll be notified. We hope that you find our blog posts to be informative and will share them with a colleague or a friend. We look forward to hearing your feedback.

Babst | Calland
Attorneys at Law

Where Trust and Value Meet™

PITTSBURGH, PA I CHARLESTON, WV I HOUSTON, TX I SEWELL, NJ I STATE COLLEGE, PA I WASHINGTON, DC