Michael Best

May 01, 2018

Related Practices

Privacy & Cybersecurity

The Facebook Effect: Today's Changing Data Privacy Regulation Climate

In the words of the Nobel Prize writer Bob Dylan, "The times, they are a-changin.'" Revelations in the press about Facebook's current privacy problems, and a new comprehensive European Union privacy framework that impacts American businesses, may be changing the climate towards more data privacy regulations by United States lawmakers. As technology and uses for data surge ahead at breakneck speed, however, the testimony of Facebook CEO Mark Zuckerberg seemed to highlight both the public's and lawmakers' limited understanding of the impact that dizzying advancement has on individual privacy and on our society at-large. Against these rapidly changing times, the challenge now is for businesses to voluntarily be more transparent and get express consent from data subjects and for lawmakers to create a protective framework against a hazy and unpredictable future.

Facebook and Zuckerberg Testimony

Facebook's most recent publicity nightmare has received scrutiny worldwide because multiple millions of users have accounts on the social media platform. However, the facts underlying the uproar over sloppy privacy practices could happen at any company on a much smaller scale. And, so there are lessons that businesses of all sizes can learn.

What happened? In the summer of 2014, about 300,000 Facebook users agreed to accept a small payment to download a third party application via Facebook, called *This Is Your Digital Life*, which presented them with a series of surveys. The Terms of Service in the application disclosed, in broad scope, that the users were granting permission to the application developer to collect and use data on the profile of those downloading the application – and, data from the profiles of their Facebook friends – if their privacy settings allowed it. This is why the number of Facebook profiles compromised exponentially increased from a mere 300,000 users to that of 87 million users. At the time, this practice was seemingly consistent with Facebook's practice of allowing

outside developers to collect information from the Facebook profiles of users, according to their privacy settings, who downloaded the application.

It was this haphazard business practice that got Facebook (and potentially any company), into its current privacy predicament. Specifically, Facebook did not require its outside developers to provide comprehensive notice and obtain consent for all of the ways for which data from the multiple millions of Facebook profiles would be used. In the case of the profiles downloaded into *This is Your Digital Life*, the data was sold and licensed to Cambridge Analytica for psychographic targeting and marketing of voters based on their "Likes" and other profile data.

Zuckerberg's Testimony. At the heart of questions for Mark Zuckerberg during congressional hearings in Washington, D.C. during the week of April 9, 2018, lawmakers were trying to determine whether these sloppy business habits could be considered a violation of the terms of a Consent Decree, as part of a 2011 settlement with the FTC, to get clear consent from users before sharing their material. During his testimony, Zuckerberg disputes the violation and testified that the Application Developer lied by saying he was gathering the data for research purposes and violated the company's policies by passing the data to Cambridge Analytica.

Although this scenario played out on a grand scale, the lesson all companies can learn is to unambiguously notify data subjects of all uses that will be made of data collected or voluntarily provided – beyond the original purpose it was given – and get their unequivocal consent for such uses.

United States Reaction

Although proposed legislation was swift, it is unlikely to result in immediate federal legislation. The Senate introduced the "Customer Online Notification for Stopping Edge-provider Network Transgressions" or "CONSENT Act," which directs the Federal Trade Commission to promulgate regulations for edge providers requiring them, among other things, to obtain opt-in consent from customers in order to use, share or sell sensitive customer proprietary information. Edge providers broadly include any person that provides a service over the Internet: which requires a customer to subscribe or establish an account; from which customers can purchase without a subscription or account; through which a program searches for and identifies items in a database that corresponds to keywords, or characters; and through which a customer divulges sensitive customer proprietary information. For purposes of the proposed act, "sensitive customer proprietary information" would include financial and health information, information pertaining to children, social security numbers, precise geolocations, content of communications, and web browsing and application usage history. A violation of the CONSENT Act would be considered an unfair or deceptive act or practices under Section 5 of the FTC Act. The introduction of the CONSENT Act is a continuation of legislative dialogue that includes other proposed legislation, including the "Balancing the Rights of Web Surfers Equally and Responsibly (BROWSER) Act," and the Secure and Protect Americans' Data Act.

At the state level, Facebook withdrew its opposition to the proposed California Consumer Privacy Act of 2018. Facebook in a written statement clarified, however, that this action is not a signal that it supports the proposed state law but that it is instead focusing its "efforts on supporting reasonable privacy measures in California." The proposed California law not only provides California consumers with certain rights relating to their personal information, but it gives them a private right of action and minimum statutory damages of $1,000 per violation. It further attempts to alleviate any challenge to standing by specifically setting forth that a violation of the proposed act would automatically be deemed "to constitute

an injury in fact to the consumer who has suffered the violation, and the consumer need not suffer a loss of money or property as a result of the violation in order to bring an action for a violation…."

As other states begin enacting privacy and cybersecurity legislation, it is unclear whether the federal government will intervene with a more comprehensive national law. What is common to the laws proposed at both the federal and state level, however, is a call for more transparency in an organization's collection, use, and sharing of personal information.

European Union Reaction

European regulators are also taking keen attention to these issues. For example, German justice minister Katarina Barley called for an EU-wide investigation into the use of Facebook's data by Cambridge Analytica and other companies. The chair of the Article 29 working party, a collection of national data protection authorities from EU member states, stated that the organization is investigating the incident. These concerns are particularly salient and enhanced in the shadow of the EU's General Data Protection Regulation (GDPR), which strictly requires consent from data subjects for many of the practices that are the subject of the activities at issue here and introduces significant fines and penalties for failures to comply. European authorities will in particular have a keen eye on digital technology and social media companies, as the consent requirements within GDPR go above and beyond what many companies in the industry have in place today and in many cases fresh, more specific permissions will be needed in order to continue current uses and sharing of personal data.

Related People

Adrienne Ehrhardt
Partner
asehrhardt@michaelbest.com
T 608.283.0131

Elizabeth Rogers
Partner
earogers@michaelbest.com
T 512.640.3164

Ryan Sulkin
Partner
rtsulkin@michaelbest.com
T 312.596.5836