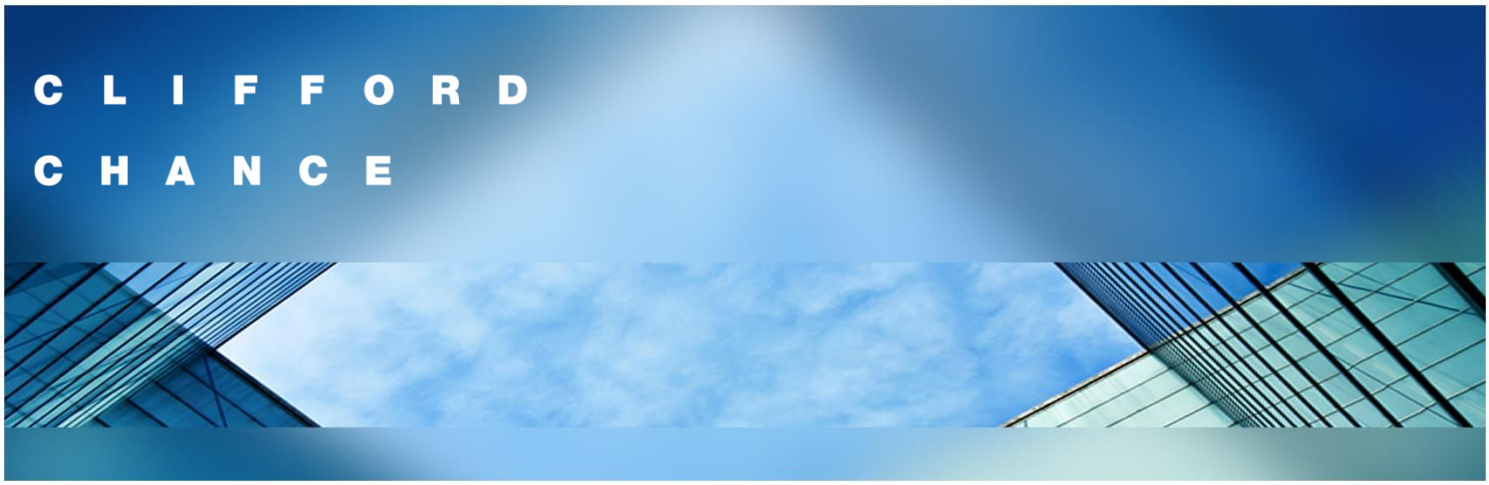

US DATA PRIVACY ENFORCEMENT AFTER FACEBOOK: WHAT TO EXPECT

Earlier this month, Facebook CEO and Founder Mark Zuckerberg testified before Congress regarding Cambridge Analytica's alleged misuse of the data of approximately 80 million US residents with Facebook accounts. During the course of nine hours at two Congressional hearings, Mr. Zuckerberg faced hostile questioning from nearly 100 legislators. Some members of Congress called for new legislation or regulation enhancing the US data privacy system, potentially modeled on the European Union's General Data Protection Regulation ("GDPR").

It is unclear at this time if Congress will pursue new data privacy legislation. Even without new legislation, however, US regulators already have broad authority to investigate and pursue enforcement actions against Facebook and other companies accused of consumer data misuse. Companies holding personal data also face the prospect of private lawsuits from both consumers and investors. It seems clear from the early days of 2018 that businesses entrusted with consumer data should take steps to prepare for further regulatory and media scrutiny of their data privacy and use practices, and not wait for new legislation to implement enhanced data privacy policies and controls.

If Congress does nothing, what exposure do businesses have in the US?

Companies doing business in the United States are subject to oversight and potential enforcement by the US Federal Trade Commission ("FTC") and state regulators, in addition to potential private litigation initiated by consumers and investors.

The Federal Trade Commission

The FTC describes itself as the "leading privacy enforcement agency" in the US and has sought to hold companies accountable for "unfair or deceptive acts or practices in or affecting commerce" under Section 5 of the Federal Trade Commission Act ("FTC Act"). The FTC has already announced that it will investigate the claims against Facebook.

FTC enforcement actions related to data are generally premised on misleading advertising or disclosure. The FTC Act provides that an act or practice is unfair where it:

i. causes or is likely to cause substantial injury to consumers;

ii. cannot be reasonably avoided by consumers; and

iii. is not outweighed by countervailing benefits to consumers or to competition.[1]

Under the FTC's long-standing interpretation of the statute, an act or practice is deceptive when:

i. a representation, omission, or practice is likely to mislead consumers;

ii. the consumer has a reasonable interpretation of the omission, representation, or practice; and

iii. the misleading representation is material.[2]

The FTC brought an enforcement action against Facebook in November 2011 that resulted in a settlement related to allegations that it failed to follow through on promises made to users that their data would be kept private. Facebook agreed to obtain consent prior to sharing consumer information beyond the scope permitted by a user's privacy settings.[3] Although Facebook was not fined, should the FTC find that Facebook violated the terms of the settlement, penalties could be as high as $40,000 for each violation.

Similarly, the FTC previously brought claims against Google in 2012 for misrepresentations to users of Safari – the web browser – regarding the tracking of consumers through the use of "cookies" and the use of targeted advertisements, amongst other things. Google settled the matter with the FTC and paid a $22.5 million fine.[4]

State Regulators

As of July, all US states will have data breach notification requirements, which specify steps that a company must take after a data breach. Where data is stolen by a third party, or potentially, used for a purpose beyond the intended Terms of Service (or similar policies), state data breach laws dictate the types of notifications and remediation that are required. Affected individuals are typically offered identity theft protection and other monitoring services.

---

1 15 U.S.C. § 45(n).
2 FTC Policy Statement on Deception, 103 FTC 174 (1983).
3 *Facebook, Inc.*, 2011 WL 6092532 (F.T.C.)
4 [Proposed] Stipulated Order for Permanent Injunction and Civil Penalty Judgment, *United States of America v. Google, Inc.*, 2012 WL 5833994 (N.D. Cal. 2012) (No. 3:12-cv-04177). *See also* Press Release, FTC, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012) (*available at*: https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented).

Many states have also adopted consumer protection laws prohibiting unfair and deceptive business practices, including the use of false or misleading disclosures to consumers, which apply to statements regarding data privacy and security. These laws empower state regulators to combat insufficient responses to data breaches and deceptive and misleading cybersecurity practices and procedures. For example, numerous state attorneys general have filed complaints against Uber for failing to protect customer information against a recent data breach.

Since the allegations against Facebook and Cambridge Analytica emerged, many state attorneys general have announced that they are considering legal action. On March 26, 2018, forty-one state attorneys general sent Facebook a joint letter demanding information about the company's Terms of Service, oversight of third party applications, use of protective safeguards, and any measures being taken to prevent future misuse of data.

Private Lawsuits

In addition to Federal and state government actions, businesses risk private lawsuits brought by consumers and investors seeking a range of civil remedies, claiming breach of contract, negligence, and fraud. In addition, thirteen states contain a private right of action for violations of data breach notification laws. Data litigants, however, have historically encountered issues successfully asserting that they have "standing" or a definite injury due to the violation. To do so, plaintiffs must show that they have (i) suffered an injury in fact; (ii) that is fairly traceable to the challenged conduct of the defendant; and (iii) that is likely to be redressed by a favorable judicial decision. Until recently, US courts have been reluctant to allow data breach lawsuits to proceed, but this view is changing as some courts have found that the heightened risk of identity theft is an "injury in fact" thus satisfying the standing requirement.[5]

Over a dozen lawsuits have been filed on behalf of Facebook users alleging breach of contract, breach of the implied covenant of good faith and fair dealing, breach of state consumer protection law (e.g., California's Unfair Competition Law), and negligent failure to protect user information. The breach of contract claims allege that Facebook violated its Terms of Service and Privacy Policies, and will require the plaintiffs to establish (i) a contract between the parties; (ii) a breach of that contract by one of the parties; and (iii) an economic loss resulting from the use of their data. Finally, private plaintiffs have filed class action lawsuits on behalf of Facebook investors alleging that Facebook breached its own data privacy policies and made materially false and misleading statements in violation of the federal securities laws. The pending lawsuits against Facebook following the allegations of data misuse will shed light on the extent to which private lawsuits can successfully enforce the rights of consumers and investors against private sector data collectors.

Conclusion

If and how Congress will react to enhance consumer privacy protections following the alleged misuse of consumer data by Facebook and Cambridge Analytica is unclear. One specific proposal that has received considerable attention would require companies like Facebook and Google to receive affirmative "opt-in"

[5] *See Galaria v. Nationwide Mutual Insurance Company,* 2016 WL 4728027 (6th Cir. 2016), *In re Yahoo! Inc. Consumer Data Security Breach Litigation*, 2017 WL 3727318 (N.D. Cal. 2017), *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010).

consent to use, sell, or share consumer data. The proposed legislation would also require such companies to notify users in the event of a breach, supplementing state law notice requirements. The FTC would be empowered to enforce the legislation. While the industry should pay close attention to legislative and regulatory developments we recommend that companies review their current data practices and take affirmative steps to prepare for the inevitable continued focus in this area.

CLIFFORD
CHANCE

CONTACTS

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Steven Gatti
Partner

T +1 202 912 5095
E steven.gatti
@cliffordchance.com

Celeste Koeleveld
Partner

T +1 212 878 3051
E celeste.koeleveld
@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Benjamin Berringer
Associate

T +1 212 878 3372
E benjamin.berringer
@cliffordchance.com

David Rabinowitz
Associate

T +1 202 912 5436
E david.rabinowitz
@cliffordchance.com

Daniel Podair
Associate

T +1 212 878 4989
E daniel.podair
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.