Twitter, FTC Battle Puts Advertisers on Alert About Privacy

7/13/2022

By Oscar Shine, *partner*; **Jacob Maiman-Stadtmauer**, *associate*; **Denae Kassotis**, *former associate*

(This article was originally published by Bloomberg Law. Reproduced with permission. Published July 12, 2022. Copyright 2022 The Bureau of National Affairs, Inc. 800-372-1033)

When companies acquire consumers' personal data, they also acquire legal obligations to disclose to those consumers how the data will be used. As illustrated by a recent complaint against Twitter—brought pursuant to the Federal Trade Commission Act (FTCA), as well as a related civil litigation, companies may face repercussions for misrepresenting how they use consumer data.

Federal agencies have shown willingness to pursue companies that misuse consumer information, but consumers still face substantial obstacles to bringing private lawsuits to vindicate privacy interests.

In May, the US Department of Justice brought an action against Twitter for the company's purported misrepresentations concerning its use of consumer data. According to DOJ, Twitter represented to users that it sought their phone numbers and email addresses solely to secure their accounts, but then used that information for targeted advertising by matching Twitter's list of user data to advertisers' existing lists.

DOJ alleged that Twitter's recent conduct violates both the FTCA and a 2011 Commission Order, in which the FTC specifically prohibited Twitter from making misrepresentations regarding the security of "nonpublic consumer information." Twitter ultimately settled with DOJ, agreeing to pay $150 million in fines, inform users of the alleged misappropriation, and implement and report new systems to ensure it protects consumers' information.

The FTCA grants federal agencies broad investigative and enforcement powers, but it does not provide a private right of action to a wronged consumer. Nor is there a clear path to relief under federal or state law for a consumer whose personal data ends up in the hands of an advertiser without their knowledge.

However, the efficacy of existing state law in these circumstances is currently being tested; Twitter is facing a class-action lawsuit in California for the allegedly deceptive practices flagged by DOJ.

As the class action against Twitter remains in its infancy, this article explores possible avenues for redress under New York and California law, as well as hurdles that plaintiffs may face in bringing such suits.

New York: Consumer Protection Law

If a company fails to disclose to a consumer the ways in which it will use their personal data, that company may be liable under New York's General Business Law. The NYGBL requires a consumer to establish they were injured by a company's "materially misleading" and "consumer-oriented" conduct.

New York courts interpret injury in this context broadly to include the exposure of personal and private information. Nevertheless, while New York courts have found that consumers' browsing history and Social Security numbers are "private," it is unclear if courts will find the exposure of phone numbers or email addresses sufficient to qualify as a statutory injury.

An NYGBL plaintiff faces other challenges. For instance, if a plaintiff cannot show actual damages (which is difficult where the injury is informational in nature) the NYGBL caps damages at $550 per violation.

California: Unjust Enrichment

In California, a consumer can allege unjust enrichment as a cause of action by asserting that the defendant unjustly retained a benefit at their expense. An unjust enrichment plaintiff need not suffer economic harm.

In a recent class action against The Weather Channel, users alleged that TWC comprehensively tracked and sold their geolocation data to advertisers, despite representing that such data would only be used to enhance the app's accuracy. The court allowed the case to proceed to the merits on the theory that the consumers "did not receive the benefit of [their] bargain" and could recover TWC's ill-gotten gains.

The road to recovery, however, is not smooth. While California courts have found that geolocation data and Facebook users' comprehensive browsing history are sufficiently personal to constitute injury for unjust enrichment, it remains an open question whether phone numbers and email addresses will be treated similarly.

Indeed, the California Consumer Privacy Act—the strictest data-privacy law in the nation—does not permit a private action for unauthorized access to phone numbers or email addresses (unless accompanied by users' passwords). This may indicate courts' hesitancy to hold Twitter liable for unjust enrichment, which is, at bottom, an equitable remedy.

Disclosure As a Liability Shield

The now-settled DOJ case and pending class actions against Twitter are premised on Twitter's alleged misrepresentations about how it intended to use consumers' data. Twitter would not be facing legal exposure had it disclosed to consumers its intent to use their data for targeted advertising. But what qualifies as adequate disclosure?

Most jurisdictions merely require that a company provide notice regarding their use of consumers' data, even if such notice is buried in a platform's "Terms of Service."

Some states, like Virginia, require consumers to affirmatively consent to the disclosure of certain categories of "sensitive data." But these requirements are the exception, not the rule. Even the CCPA recognizes a hyperlink at the bottom of a webpage as sufficient disclosure of data collection practices.

As the law stands—absent flagrant misrepresentation—companies are unlikely to be held liable for misusing data if they provide some notice to consumers, regardless of whether consumers affirmatively consent to, or have actual knowledge of how their data will be used.

Nevertheless, as public backlash against perceived misappropriations of user data grows, state legislatures may fill this gap by enacting more robust laws that require companies to affirmatively request that a user consent to sharing their data.

Likewise, courts may interpret state law in a such a way as to provide recourse to consumers—like the 140 million Twitter users—who were allegedly deceived about what Twitter would do with their phone numbers and email addresses.

This article does not necessarily reflect the opinion of The Bureau of National Affairs, Inc., the publisher of Bloomberg Law and Bloomberg Tax, or its owners.

Author Information

Oscar Shine is a partner at Selendy Gay with experience in complex commercial disputes, internal investigations, and government enforcement matters.

Denae Kassotis is an associate at the firm, handling a broad range of complex litigation.

Jacob Maiman-Stadtmauer is a summer associate at the firm.

Attorneys

- Oscar Shine
- Jacob Maiman-Stadtmauer