District of Columbia v. Facebook: General Consumer Protection Statute can serve as vehicle for state attorney general seeking redress for data privacy violations

Litigation Alert

12 June 2019
By: Matthew P. Denn

On May 31, 2019, the District of Columbia Superior Court rejected Facebook's request to dismiss data privacy litigation brought by the District of Columbia Office of the Attorney General based on its alleged role in the Cambridge Analytica scandal, concluding that the DC Superior Court had jurisdiction over the case and the complaint sufficiently alleged violations of the District of Columbia Consumer Protection Procedures Act (CPPA).[i]

The order demonstrates that general state consumer protection statutes can serve as a viable weapon in the arsenal of State Attorneys General who wish to challenge the reasonableness of entities' data privacy practices and disclosures. The order also demonstrates that Internet-based companies are not immune to jurisdiction in a foreign venue even when general personal jurisdiction does not exist.

Background

Following reports arising from the Cambridge Analytica scandal, the District of Columbia Office of the Attorney General

(DC OAG) filed suit under the District's Consumer Protection Procedures Act (CPPA). Although a number of State Attorney General offices publicly announced in 2018 that they were either investigating or seeking additional information regarding potential state law violations arising from the Cambridge Analytica incident, the DC OAG was the first state AG to file any formal action.[ii]

The DC complaint alleged that Facebook permitted third-party developers to access consumers' personal data and data concerning consumers' digital behavior in connection with offering mobile applications to Facebook users.[iii] Citing the Cambridge Analytica incident, where a researcher used a third-party application to harvest Facebook consumers' data and then sold the data to a political consulting firm, the complaint alleged that Facebook had (1) failed to effectively oversee and enforce its consumer protection policies, (2) failed to take reasonable steps to protect consumers' privacy by ensuring that the data was accounted for and deleted from Cambridge Analytica's databases once the incident was known to Facebook, and (3) failed to alert the public of the sale of users' data to Cambridge Analytica.[iv]

Facebook moved to dismiss the complaint, arguing that the court lacked jurisdiction to hear the DC OAG's claims and the DC OAG failed to state a claim for relief. Alternatively, Facebook argued that the court should stay the case pending the resolution of a related multi-district litigation and the FTC investigation.

In denying Facebook's motion, the court specifically found that it was permitted by the federal Due Process Clause to exercise personal jurisdiction over Facebook and that the facts alleged by the DC OAG established that Facebook had made statements regarding its handling of personally identifiable information that could be reasonably interpreted by a consumer as misleading. The court also denied Facebook's request to stay the action.

Jurisdictional challenge

Although the court agreed with Facebook that it did not have general jurisdiction over Facebook, it found that exercising specific personal jurisdiction over Facebook would comport with the federal Due Process Clause.

The court acknowledged that "the relationship between a defendant's online activity and its susceptibility to suit in a foreign jurisdiction remains ill-defined," and that the personal jurisdiction issue was a "novel" one.[v] It also reaffirmed that the mere fact that a DC resident had access to Facebook's website did not allow for the court to exercise specific personal jurisdiction over Facebook. Nevertheless, the court concluded that personal jurisdiction existed because Facebook's online accessibility and transactions with the forum satisfied DC's minimum contacts standard.

First, the court concluded that **Facebook's website qualified as a "storefront" in DC because Facebook engaged in continuous and systemic business activities with DC residents**, which included its collection of DC residents' data, use of that data to target advertising to DC residents, harvesting of that data for third parties, filings with DC regulatory authorities, operation of an office in the District of Columbia, and acquiring substantial revenue from consumers in the District of Columbia .

The court also concluded that Facebook's conduct had an effect in DC because Facebook regularly made regulatory filings in the forum and allegedly allowed Cambridge Analytica to collect the personal data of 340,000 DC residents.[vi]

Application of the District of Columbia's General Consumer Protection Statute

Although the Federal Trade Commission's statutory authority to apply Section 5 of the Federal Trade Commission Act (FTCA) – a general consumer protection statute – to data security issues was confirmed by the Third Circuit Court of Appeals in 2015,[vii] the applicability of state general consumer protection statutes to data privacy and security issues has been relatively untested in the state courts. The *DC v. Facebook* decision is **one of the first to conclude that a state general consumer protection statute *can* be applied to a data privacy issue**.

In the complaint, the DC OAG alleged that Facebook had violated three subsets of the CPPA, which generally forbids any person from "engag[ing] in an unfair or deceptive trade practice," including specifically:

"(e) misrepresent[ing] as to a material fact which has a tendency to mislead;

(f) fail[ure] to state a material fact if such failure tends to mislead;

(f-1) [u]s[ing] innuendo or ambiguity as to a material fact, which has a tendency to mislead[.]"

Although the DC CPPA generally forbids both unfair and deceptive practices, the DC OAG's complaint focused on specific

provisions of the CPPA that involve deception. In doing so, the DC OAG avoided a parallel to the continuing debate taking place in the federal courts as to the scope of the FTC's authority to sanction "unfair" (as opposed to deceptive) conduct with respect to data security.[viii]

In its order, the court found that the DC OAG had pled facts sufficient to withstand a motion to dismiss. *First,* the court concluded that the DC OAG had sufficiently alleged a "misrepresentation as to a material fact which has a tendency to mislead" in violation of subsection (e). In reaching this conclusion, the court relied on the complaint's allegations that **Facebook's general statements that it would protect the privacy of consumers' personal information and require the same of third parties were misleading** because Facebook did not provide consumers with a clear explanation of how much responsibility Facebook undertook to protect consumers' personal data from third parties. The court also relied on the complaint's allegation that Facebook's statement that it may share some users' personal information with partner companies could lead a reasonable consumer to believe that the information obtained by those partner companies would be limited to data that users had opted to share in their privacy settings, which the DC OAG alleged had not been the case with respect to the data shared with Cambridge Analytica.

Second, with respect to subsection (f) (failure to state a material fact when the failure has a tendency to mislead), the court found that two failures to disclose alleged by the Attorney General were sufficient to withstand a motion to dismiss: (i) **Facebook's alleged failure to adequately warn its users** that their personal data was improperly obtained, harvested, and used by third parties without the consumers' knowledge or consent, and (ii) Facebook's alleged failure to disclose to users that **it allowed certain companies to override users' privacy settings and access consumers' personal data without their knowledge or consent**. The court noted that the DC OAG had cited a series of cases finding that "fine print and obscurely placed disclosures, even if contained within a privacy policy, may be insufficient to give consumer reasonable notice that their personal information may be shared with third parties." Although the court did not indicate that it was relying on these cases in reaching its conclusion, the cases were likely cited in response to Facebook's argument that (in the court's words) "'every policy' contested by the DC OAG was disclosed to users in Facebook's Statement of Rights and Responsibilities and Data Use Policy."

Finally, with respect to subsection (f-1) (use of innuendo or ambiguity as to a material fact, which has a tendency to mislead), the court found that four separate statements or omissions by Facebook, as alleged in the complaint, served as a basis to allow the claim to proceed:

- Facebook's failure to explain to consumers how to control how information is shared with third-party applications and how to change privacy settings with respect to apps
- Facebook's representations to consumers that it would protect the privacy of their personal information
- Facebook's representation to consumers that it requires apps and third-party developers to respect the privacy of consumers' personal information, and
- Facebook's representation to consumers that consumers' agreements with third-party apps would control how those apps used consumer data.[ix]

Central to the court's decision was the fact that the decision was being made at the pleading stage, where the allegations are assumed true. Whether Facebook engaged in the alleged conduct and whether that conduct was deceptive is a question for a later day.

Lessons and implications

Although the District of Columbia Superior Court's opinion involved the application of some specific statutory provisions to a set of unique alleged facts, the case should be carefully examined by entities that collect data for a number of reasons.

1. Although the case was decided under District of Columbia law, it provides a good example of the deferential standard that may be applied by some courts at the pleading stage to data privacy claims brought by State Attorneys General.
2. The case also demonstrates how an error by a data collector can give rise to a consumer protection claim even in those instances where it does not violate a data privacy-specific statute. The court found that Facebook's after-the-fact failure to promptly notify consumers of the Cambridge Analytica incident might constitute an actionable failure to state a material fact under the consumer protection statute. Thus, businesses in states having similar general consumer protection statutes should consult with counsel about whether, even in the absence of a specific statutory obligation, they have a duty to notify consumers of data privacy issues.
3. The case supports the proposition that in the data privacy/data security context even an express disclosure to

consumers of a data sharing practice by a data collector may not be sufficient to defeat a claim under a consumer protection statute if the court finds that the disclosure is so unclear or inconspicuous that the full disclosure is rendered deceptive.

4. The case is a reminder to businesses that if they are going to make affirmative claims to consumers that they will protect the privacy of the consumers' personal information, they should consult with counsel to ensure that they have not overstated those claims and have clearly articulated any exceptions to them.
5. Finally, the case demonstrates that Internet-based companies can become susceptible to a court's jurisdiction by targeting advertising to residents of foreign venues.[x]

To learn more about the implications of this case, please contact either of the authors. You may also be interested in learning more about our State Attorney General practice.

---

[i] The opinion can be found online at https://tinyurl.com/yya8t5jy.

[ii] The District of Columbia is not currently a state, but its Attorney General is treated as a State Attorney General by his peers and is the Vice President of the National Association of Attorneys General.

[iii] The summary of the complaint is drawn from the court's summation of the allegations in its May 31, 2019 Order.

[iv] The complaint also alleged more broadly that Facebook knew of other third-party applications that also improperly sold or used consumer data, that Facebook also failed to tame reasonable measures to enforce its policies in connection with those other third-party applications, and that Facebook failed to disclose to users when their data was improperly used by those other third-party applications Complaint at ¶ 43·

[v] Facebook has asked for an interlocutory appeal of the court's decision regarding personal jurisdiction.

[vi] The court separately found that application of the District of Columbia long-arm statute was met under all four prongs of that statute.

[vii] *Federal Trade Commission v. Wyndham Worldwide Corporation*, 799 F.3d 236 (3d. Cir. 2015).

[viii] See, *eg, Federal Trade Commission v. D-Link Systems, Inc.*, 2017 WL 4150873 (N.D. Cal. 2017) (Court dismisses FTCA fairness claim against router and camera manufacturer while allowing deception claims to proceed).But see *Veridian Credit Union v. Eddie Bauer LLC,* 295 F. Supp. 3d. 1140 (W.D. Wash. 2017) (allowing a data breach claim to proceed under the "unfairness" prong of Washington state's CPPA).

[ix] The court also declined to stay the case pending the outcome of ongoing multi-district litigation and an FTC investigation.

[x] *Gullen v. Facebook.com, Inc.*, 2016 WL 245910 (N.D. Ill. 2016).

AUTHORS

Matthew P. Denn
Partner
Wilmington | T: +1 302 468 5700
matthew.denn@dlapiper.com