Proskauer

Plaid Federal Electronic Surveillance Claims Dropped, Privacy Claims Survive

New Media and Technology Law Blog on **May 11, 2021**

On April 30, 2021 a California district court trimmed various federal privacy-related claims, including the Computer Fraud and Abuse Act (CFAA) claim, from a highly-visible, ongoing putative class action against fintech services company Plaid Inc. ("Plaid"), but allowed other state law privacy claims to go forward. The lawsuit involves Plaid's alleged collection and use of consumers' banking login credentials and later processing and selling of such financial transaction data to third parties without adequate notice or consent (*Cottle v. Plaid Inc.*, No. 20-3056 (N.D. Cal. Apr. 30, 2021).

The court's decision did not delve deeply in the merits of the CFAA claim, as it was dismissed on procedural grounds; similarly, resolution of the major issues of the case about invasion of privacy and the adequacy of consent to access consumers' bank accounts and collect/aggregate data was not achieved at this early stage of the litigation. Thus, this case is just beginning and is certainly one to watch to see how the unsettled areas of mobile privacy and CFAA "unauthorized access" are further developed.

Plaid is a fintech services company that offers applications that provide account linking and verification services for various fintech apps that consumers use to send and receive money from their bank accounts. The plaintiffs claim that Plaid's banking authentication system, which is embedded into various fintech apps, included a user interface that mimicked the login screens of an individual user's financial institution such that users were uninformed that they were not actually logging in via the bank's own platform. Instead, according to plaintiffs, consumers would unwittingly give Plaid their financial institution login credentials and that Plaid would retain access to their credentials and use them to mine, aggregate and then sell users' financial transaction data to third parties (including to the fintech apps that use its services) for purposes unrelated to the plaintiffs' use of the fintech payment apps. In sum, plaintiffs' complaint asserts that at no time were users ever given conspicuous notice or meaningfully prompted to read through Plaid's privacy policy indicating that Plaid receives and retains access to their financial institution account login credentials or uses their credentials to collect and sell their banking information.

Based on the allegations, plaintiffs advanced a number of claims, including, among others, violations of the CFAA (and state computer trespass law) and the federal Stored Communications Act (SCA), as well as a number of state privacy and consumer protection claims (including violation of the California Anti-Phishing Act of 2005). In response, Plaid moved to dismiss on several grounds, with mixed results.

The court first ruled that the plaintiffs had Article III standing because they sufficiently pled an injury-in-fact.. The court found that plaintiffs' allegations – that Plaid does not disclose to users that they are interfacing with Plaid rather than their banks, that Plaid does not meaningfully disclose the extent of its data collection practices, that Plaid deemphasizes the link to its privacy policy, and that Plaid uses the consumer login information to obtain banking data regardless of whether it relates to the transfer of money via the finech apps – sufficiently show that Plaid's data collection practice would "cause harm or a material risk of harm" to their interest in controlling their personal information to satisfy Article III standing requirements.

Regarding the federal claims, the court dismissed both of them. The CFAA prohibits various computer crimes, the majority of which involve accessing computers without authorization or in excess of authorization, and then taking certain forbidden actions. Plaid moved to dismiss the CFAA claims on several grounds, including that plaintiffs had not alleged facts supporting the requisite $5,000 amount of "damage or loss" required under the statute ("damage" generally refers to harm to availability or integrity of data and information; "loss" means reasonable costs to respond to a network intrusion or conduct damage assessments, or damages incurred because of an interruption in service). On this procedural matter, the court dismissed the CFAA claim and ruled that plaintiffs did not adequately explain how to value the alleged "loss of use and control" of their financial information and offered no authority that such a loss is cognizable for purposes of the CFAA. The court also dismissed the state computer trespass claims (Comprehensive Computer Data Access and Fraud Act (CDAFA), finding that although the CDAFA does not contain a specific monetary threshold for loss related to violations of the statute, plaintiffs offered no support for their theories that the loss of the right to control their own data or the loss of the value of their data is "damage or loss" within the meaning of the CDAFA.

The court also dismissed the plaintiffs' SCA claim. Under the SCA, a plaintiff may bring an action against anyone who "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage." As the court stated, plaintiffs' argument that their financial institutions meet the SCA definition of "facility through which an electronic communication service is provided" is unsupported by the SCA. Also, the court found that the complaint did not plausibly allege that Plaid accessed an electronic communication while it was "in electronic storage," as there was no allegation that plaintiffs' financial institutions store their "electronic banking communications" for the purpose of providing backup protection.

While Plaid was successful in eliminating the federal claims, the court declined to dismiss the core state privacy-related claims, including a claim for invasion of privacy. Plaid had argued that plaintiffs could not plausibly assert a reasonable expectation of privacy because they chose to link their accounts to the fintech apps and Plaid's privacy policy disclosed the information it collects. Thus, according to Plaid, the allegations do not evince an "egregious" breach of social norms required to bring a successful claim. The court declined to dismiss the state privacy claims because the issue of whether plaintiffs had received notice and consented to Plaid's data collection was a "key factual dispute," as was whether such collection was "egregious" enough to be actionable.

Interestingly, the court also declined to dismiss the creatively-pled claim under California's Anti-Phishing Act of 2005. That statute prohibits, in part, "any person, by means of a Web page, electronic mail message, or otherwise through use of the Internet, to solicit, request, or take any action to induce another person to provide identifying information by representing itself to be a business without the authority or approval of the business." Cal. Bus. & Prof. Code § 22948.2. In its complaint, the plaintiffs had claimed that Plaid had induced users to provide their banking login credentials by representing itself to be the user's financial institution without the authority or approval of the financial institution. Plaid had argued that the law's intent was to combat phishing schemes that facilitate identity theft and that it hadn't "tricked" plaintiffs into disclosing their login credentials. However, the court refused to dismiss the claim at this stage, concluding that the complaint had put forward a plausible claim and the plain language of the statute imposed no requirement that the defendant act with the goal of facilitating identity theft (though, the court admitted that neither the parties nor the court could locate any cases analyzing the statute). Interestingly, the court rejected Plaid's argument that it had acted with the approval of plaintiff's financial institutions when it accessed plaintiffs' account data, citing the existence of another ongoing lawsuit against Plaid brought by a financial institution that includes allegations about Plaid's intentionally "misleading" user interface that mimics the bank's own screens.

The results of Plaid's motion to dismiss are not surprising, given a prior February 2021 ruling in a similar consumer data privacy action against financial data aggregator Yodlee Inc. ("Yodlee"). (*Wesch v. Yodlee Inc.*, No. 20-05991 (N.D. Cal. Feb. 16, 2021)). According to the complaint in that suit, Yodlee is one of the largest financial data aggregators in the world and through its software platforms, which are built into various fintech products offered by financial institutions, it aggregates financial data such as bank balances and credit card transaction histories from individuals in the United States. As we wrote about last year, the crux of the suit is that Yodlee collects and then sells access to such anonymized financial data without meaningful notice to consumers, and stores or transmits such data without adequate security, all in violation of California and federal privacy laws. In ruling on the Yodlee's motion to dismiss the original complaint, the California district court examined similar claims as those advanced in the *Plaid* action and allowed several state privacy-related claims to go forward, but dismissed the federal SCA and CFAA claims Note: the *Yodlee* court dismissed the CFAA claims on similar procedural grounds as the *Plaid* court, but did find that plaintiffs' allegations that Yodlee stored their banking login information and accessed their account transaction history on an ongoing basis for purposes unrelated to facilitating fintech payment transactions were sufficient to allege access that "exceeds" Yodlee's authorization under the CFAA.)

With the major mobile platforms tightening their developer policies and privacy notification requirements in recent years and more and more actions being filed with respect to mobile data collection practices, data privacy (including the collection of location data and financial transaction data) has garnered more scrutiny. There has also been a fair amount of coverage of these issues in the media and fairly intense debate in Washington. We will be watching these cases closely as they may lend some clarity to the contours of appropriate data sharing practices in the fintech area.

View Original

Related Professionals

- **Jeffrey D. Neuburger**
  Partner