New York Law Journal

ANALYSIS

How Treating Data as Property Could Open the Door to More Novel Data Litigation Claims

In 'Calhoun v. Google', the Northern District of California significantly expanded a "growing trend across courts … to recognize the lost property value" of data and affirmatively held that people have a "property interest in their personal information."

May 09, 2022 at 11:00 AM

6 minute read

Big Data

By Annmarie Giblin

An emerging line of case law could pave the way for a whole new generation of cyber negligence cases. In *Calhoun v. Google*, 526 F. Supp. 3d 605 (N.D. Cal. 2021), the Northern District of California significantly expanded a "growing trend across courts … to recognize the lost property value" of data and affirmatively held that people have a "property interest in their personal information." Id. at 635. This holding solidifies many arguments that plaintiffs in both data breach and privacy litigation have been advancing for years. Also, it provides a more direct path for future plaintiffs to assert negligence as a cause of action in various types of litigation involving data. While the reach of this holding is broad, the more immediate changes may be seen in data breach

litigation, which has historically contended with various procedural hurdles.

As cyber incidents and data breaches became more common, commentators anticipated that litigation stemming from such incidents would explode. Yet, while the number of lawsuits stemming from cyber incidents and data breaches did indeed increase, various procedural hurdles, such as establishing standing to bring suit and proving damages necessary to seek recovery, have slowed or ended these cases before they could fuel the runaway train that had been feared.
The *Calhoun* decision significantly weakens some of these procedural hurdles and opens a more direct path forward for future litigants in these cases to assert negligence as a viable cause of action.

Significance of 'Calhoun'

Calhoun is a privacy—not a data breach—case and centers on the alleged illegal collection of the plaintiffs' personal information by the defendant. The plaintiffs in *Calhoun* initially asserted 16 causes of action in their complaint. After the court directed the parties to select 10 claims out of the 16 to litigate, the defendant moved to dismiss the action. The remaining 10 claims included a claim for statutory larceny. *Calhoun*, 526 F. Supp. 3d 605, 617 (N.D. Cal. 2021).

The defendant asserted several arguments in support of its motion to dismiss, but with respect to the statutory larceny claim, it specifically argued that the claim failed because the personal information alleged to have been stolen was "not property." Id. at 635. In support of this argument, defendant cited a 2012 case, *Low v. LinkedIn*, 900 F. Supp. 2d

1010, 1030 (N.D. Cal. 2012), which held that a person's "'personal information' does not constitute property."

In rejecting this reasoning, the court in *Calhoun* noted that the more recent trend in cases involving data was moving away from the holding in *Low* and instead was finding that the "lost value" of a person's data was sufficient to establish an injury to such plaintiffs. The court in *Calhoun* also noted that many courts have taken this trend a step further and started to recognize the "lost property value" of a person's personal information, and also that courts in California "have also acknowledged that users have a property interest in their personal information" *Calhoun*, 526 F. Supp. 3d at 635 (citing *CTC Real Estate Servs. v. Lepe*, 140 Cal. App. 4th 856, 860 (2006) (internal parenthetical omitted)). Thus, the *Calhoun* court concluded that the statutory larceny claim could proceed as the "[p]laintiffs have adequately alleged that they were deprived of a property interest." Id. at 635. The court declined to reconsider this holding when asked by the defendant in *Brown v. Google*, 2021 U.S. Dist. LEXIS 244695, (N.D. Cal. 2021), in which different plaintiffs asserted similar arguments against the same defendant.

One procedural hurdle that this decision immediately affects is the application of the economic loss doctrine, which in some jurisdictions has prevented data breach plaintiffs from alleging negligence as a cause of action. "Under the economic loss doctrine, 'purely economic losses are not recoverable in tort.' In the absence of personal injury, physical damage to property, a special relationship between the parties, or some other common law exception to the rule, recovery of purely economic loss for negligence is foreclosed. *In re Ambry Genetics Data Breach Litig.*, 2021 U.S. Dist. LEXIS 204358, *14 (C.D. Cal. Oct. 18, 2021) (quoting *NuCal*

Foods v. Quality Egg, 918 F. Supp. 2d 1023, 1028 (E.D. Cal. 2013) (citation omitted) (citing *J'Aire Corp. v. Gregory*, 24 Cal. 3d 799, 803-04, (1979)).

Thus, depending on the specific elements of that jurisdiction's version of the economic loss doctrine (which can vary from state to state), in certain jurisdictions, plaintiffs bringing suit over a data breach have been unable to assert negligence as a cause of action unless they were able to establish a special relationship between the parties or some other common law exception to the rule. See *Zoll Med. v. Barracuda Networks*, 2021 U.S. Dist. LEXIS 180761, *7-10 (D. Mass. Sept. 21, 2021). Now, in light of the holding in *Calhoun*, plaintiffs may no longer have to jump through these procedural hoops in order to bring a negligence cause of action as they can now legally assert that their data, which has been held to be their property, has been damaged as a result of the data breach.

Additionally, the *Calhoun* decision could also impact insurance coverage cases, depending on the terms of the policy at issue. If insurance policies that cover property damage define the term "property" broadly or do not define it at all, then the *Calhoun* decision could be used as a basis to argue that "damage" to personal information, whether in a cyber incident or data breach, constitutes covered property damage under the policy.

Conclusion

These arguments are fresh and, as of this writing, are not known to have been tested in other courts. However, the *Calhoun* decision is only a year old, and it remains to be seen how broad the impact of its novel holding will be. What is certain is that lawsuits and claims involving data, especially those involving compromised personal information, are rapidly evolving and starting to embrace unique and novel legal theories

in response to unique and novel fact patterns. Thus, this holding that data is property likely heralds the approach of the long-anticipated data litigation train.

Annmarie Giblin *is a partner at Hinshaw & Culbertson, where concentrates her practice on the legal issues surrounding cybersecurity, privacy, and insurance. She provides proactive cyber legal defense, third-party vendor legal risk management, cyber incident response legal services, and legal support and advice on emerging technologies, such as artificial intelligence. Annmarie also advises clients on best practices and compliance with privacy and cyber laws and regulations, and related contract issues, including drafting unique contract language to address emerging and novel legal issues.*