THE RECORDER

Data Privacy Across State Lines

'In re Blackbaud' and beyond: As state law-focused data privacy litigation gains momentum, Baker Botts' Cynthia Cole and Nicholas Palmieri highlight some of the issues that are taking shaping in the gap between these new laws and litigation on the ground.

October 08, 2021

By Cynthia Cole and Nicholas Palmieri

As more states create data privacy laws, plaintiffs face an increasingly complicated litigation landscape for privacy redress, and companies must mount even more complicated defense strategies. One such example is the ongoing multidistrict litigation proceeding against Blackbaud, Inc. in the District of South Carolina. *In re Blackbaud*, No. 3:20-mn-02972 (D.S.C. filed April 2, 2021), where plaintiffs from 20 states filed a single Consolidated Class Action Complaint. This case provides instructive initial issues for companies to take into consideration as they drive their data-driven practices.

Blackbaud was hit with a ransomware attack between February and May 2020. Blackbaud, ultimately, complied and paid the ransom, but not before data had allegedly been breached. From July 2020 through January 2021, Blackbaud notified its customers and other data subjects who had been affected, and according to the plaintiffs, contained conflicting information on exactly the type of data that was affected.

In response, a number of putative class actions were filed across the country, eventually being consolidated into the present MDL litigation. The consolidated complaint, spanning 427 pages, alleges causes of action under the laws of all 50 U.S. states—as well as the District of Columbia, Puerto Rico, and the U.S. Virgin Islands—though only a subset of those are specifically related to data privacy.

Surviving Motions To Dismiss

Blackbaud submitted a motion to dismiss under Rule 12(b)(6) alleging that the plaintiffs failed to state a claim under the laws of California, Florida, New Jersey, New York, Pennsylvania, and South Carolina. This motion met with limited success, with the court granting the motion with respect to the claims under certain laws in Pennsylvania, South Carolina, New Jersey, Florida, and California. (Note that not all claims for each of these states were dismissed, but only select ones. See Order Granting in Part and Denying in Part Defendant's Motion to Dismiss under Rule 12(b)(6), *In re Blackbaud*, No. 3:20-mn-02972, ECF No. 143 (D.S.C. filed Aug. 12, 2021).

As would be expected, this motion focused heavily on specific statutory language, specifically California, South Carolina and New York.

California Consumer Privacy Act (CCPA)

Blackbaud alleged in its motion that is was not a "business" under the CCPA, but rather a "service provider" which does not fall under the scope of the CCPA. The court did not find this argument convincing. Specifically, the court emphasized that the CCPA calls for the act to "be liberally construed to effectuate its purposes." To that end, they recognized that while Blackbaud may be a "service provider" under the CCPA, they may also qualify as a "business" and thus, this claim survives the motion.

South Carolina Data Breach Security Act (SCDBA)

South Carolina's Data Breach Security Act covers any person "owning or licensing" data with personally identifying information. In its motion, Blackbaud alleged that it does not "own or license" data. The court agreed on this point. Specifically, the complaint merely "suggests" that *Blackbaud* processes or otherwise hosts information that it receives. However, at no point in the complaint, according to the court, do the plaintiffs assert (or provide any evidence) that *Blackbaud* has any ownership interest in the data it may process. While possession of the data is a prerequisite to ownership, according to the court, that alone does not establish ownership.

New York General Business Law (GBL)

Under New York's General Business law, plaintiffs must show that the accused practice (1) was consumer oriented; (2) was misleading in a material way; and (3) the plaintiff suffered an injury. Blackbaud's motion focused on only the first element, alleging that their practices were not consumer oriented. The court, though, disagreed, and instead took a broad view of the term "consumer oriented" and viewed the plaintiff's allegations that Blackbaud's actions affected "a broad segment of New York consumers" as sufficient to overcome the motion. Interestingly, the court also appeared to endorse the concept of "diminished data value" as a viable damage to qualify under the statute. (This broad damage reading is also a very different view than the Supreme Court took in *TransUnion v. Ramirez*, where the court refused to acknowledge potential future harm as sufficient to provide standing under the statute at issue. 594 U.S. __ (2021) See Order and Opinion Denying Blackbaud's Motion to Dismiss for Lack of Subject Matter Jurisdiction, *In re Blackbaud*, ECF No. 121 (D.S.C. filed July 1, 2021).)

Privilege in Data Breach

Beyond multiple state statutory interpretation, this case may also implicate other, fundamental issues, especially: (1) Attorney-Client Privilege and (2) Attorney Work Product.

As discovery evolves, the plaintiffs may seek certain documents that were prepared by Blackbaud (or by vendors hired by Blackbaud) which provide details of the security incident itself and Blackbaud's handling of it. One such document, known as the "Kroll Summary" has already been provided, sealed for containing personal information, though it appears to have been produced to the plaintiffs without issue.

However, Blackbaud may wish to assert either the attorney-client privilege or attorney work product as grounds not to release other similar documents or reports. While these privileges are powerful, the protections are not absolute. Recently, in Pennsylvania, a defendant tried to assert that a report detailing a cybersecurity breach (ironically also prepared by Kroll Cyber Security) should not be disclosed, under both the attorney-client privilege and the work-product doctrine. (See Order re Discovery, *In re Rutter's Data Security Breach Litigation*, ECF No. 95 (M.D. Penn. Filed July 22, 2021).

The court, though, did not find their argument convincing, deciding that (1) the report hadn't been prepared "in anticipation of litigation" as it had been prepared before the litigation had commenced and (2) the report was not prepared to provide legal advice, since no one involved in its creation had a legal degree.

Conclusion

State data privacy litigation under these new consumer-focused laws are still in the making. Pressure from plaintiffs and the federal courts unwillingness to take up the issues keeps these matters squarely in state courts for now.

From what we see, state courts will rely heavily on statutory precision. Companies must plan very carefully how they define what they do with respect to data collection, whether they own the data they process (versus use only) and how they protect the processes and procedures they have in place with respect to keeping the data secure.

Cynthia Cole *is a partner at Baker Botts Palo Alto office. Her practice focuses on corporate, strategic and technology transactions and data privacy.*

Nick Palmieri *is an associate at Baker Botts New York Office. His practice focuses on a wide range of intellectual property issues, as well as data privacy.*