Versatile Defense Strategy Is Best For Privacy Class Actions

By **Adam Fox, Kristin Bryan and Katy Spicer** (July 7, 2020)

Adam Fox

Kristin Bryan

Katy Spicer

"Privacy means people know what they're signing up for, in plain language, and repeatedly. I believe people are smart. Some people want to share more than other people do. Ask them."

— Steve Jobs

After checking the rear-view mirror to reexamine the way in which courts have responded to privacy litigation for decades, it is time to greet the nationwide class action phenomenon raising privacy concerns.

An examination of the intersection between emerging technologies that threaten privacy and new lawmaking that seeks to protect it reveals an unchanging, fundamental truth: The immediate and aggressive response to a lawsuit often leads to resolution of the controversy before costly and time-consuming litigation.

In consumer privacy cases, this response most frequently involves a multifaceted strategy, including:

- Identifying and asserting rights to arbitrate if they exist;
- Employing motion practice to challenge the plaintiffs' standing and identifying implausible claims for prompt dismissal; and
- Using all available tools to defeat class certification and thereby minimizing the enterprise exposure of the threatened lawsuit.

Below, we examine in greater detail some of these tactics.

Is there an agreement to arbitrate?

One particularly effective strategic option for countering prospective class actions since AT&T Mobility LLC v. Concepcion,[1] has been the enforcement of agreements to arbitrate.

In Concepcion, the U.S. Supreme Court held that the Federal Arbitration Act preempts state laws intended to prohibit contracts from disallowing class-wide arbitration, prompting one commentator to characterize the decision as a "tsunami that is wiping out existing and potential consumer and employment class actions."[2]

The waves of that decision continue to crash down on putative class actions, as exemplified by the Supreme Court's decision last term in Lamps Plus Inc. v. Varela.[3] In that case, the court held that a party could compel an individual arbitration even if a written agreement to arbitrate does not clearly surrender the right to arbitrate a class action.

Varela is also especially important to privacy litigation because it presented an employee's claims arising from a data breach and thus underscores the conclusion that privacy issues are not immune from Concepcion and its progeny. Apart from the data breach context, arbitration issues have also emerged in statute-specific contexts including under the Illinois Biometric Information Privacy Act and the California Consumer Privacy Act.

Thus, the invocation of an available arbitration agreement provides a particularly effective option for defeating prospective privacy class actions. To avoid any question of waiver, the availability of arbitration should be examined at the commencement of litigation and pursued with aggressive early motion practice.

Is there a concrete injury?

In Spokeo Inc. v. Robins,[4] the Supreme Court confronted a putative class action alleging violations of the Fair Credit Reporting Act because the defendant's online profile of people, including the named plaintiff, reflected false information.

Although both lower courts deemed the particularized description of the plaintiff's alleged injury sufficient to confer standing to proceed, the Supreme Court explained that the U.S. Constitution also "requires a concrete injury even in the context of a statutory violation." The court elaborated that "a bare procedural violation, divorced from any concrete harm," fell short of satisfying the constitutional requirement for a concrete injury.

Despite the apparent simplicity of this principle, lower courts have since grappled with the requirement for a concrete injury, particularly in the context of other data privacy statutes. Illustrative is the recently decided Bryant v. Compass Group USA Inc.,[5] in which a putative class action brought in a state court alleged that the plaintiff's employer had violated Illinois' Biometric Information Privacy Act by failing to obtain her written, informed consent prior to collecting her fingerprint.

After the defendant removed the case, the plaintiff succeeded in persuading the trial court to remand the case on the basis that she lacked the concrete injury required for federal subject matter jurisdiction. The U.S. Court of Appeals for the Seventh Circuit reversed, explaining that the plaintiff's assertion of "a violation of her own rights — her fingerprints, her private information" was enough "to show injury-in-fact without further tangible consequences."

As such, the plaintiff had Article III standing to pursue some of her BIPA claims in federal court. The U.S. Court of Appeals for the D.C. Circuit also recently ordained that "the loss of a constitutionally protected privacy interest itself would qualify as a concrete, particularized, and actual injury in fact."[6]

In contrast, the U.S. Court of Appeals for the Second Circuit has imposed a standard that draws a sharper distinction between bare statutory violations and concrete injuries resulting from them.[7] The Second Circuit concluded that the plaintiffs' alleged BIPA notice violations, even "if true, presents a material risk that their biometric data will be misused or disclosed," and therefore did not suffice for purposes of Article III.

Likewise, with regard to the plaintiffs' claims regarding a failure to follow BIPA's data security provisions, the Second Circuit ruled that they had not alleged "a material risk that their biometric data will be improperly accessed by third parties" and therefore "have failed to show a "risk of real harm" sufficient to confer an injury-in-fact."

This split in authority suggests that the Supreme Court may speak to the subject once again, keeping the defense alive even in circuits having already rejected it.

Does personal jurisdiction embrace a nationwide class?

Although it is not a class action case itself, Bristol-Myers Squibb Co. v. Superior Court[8] may provide another avenue to attack data privacy class actions. In that case, the Supreme Court confronted a California mass action in which the defendant, over which the trial court lacked general personal jurisdiction, challenged the court's personal jurisdiction over claims brought by plaintiffs who likewise did not reside and had not made purchase or been injured in the state.

Following the defendant's success with this argument at Supreme Court, "the overwhelming majority of federal courts that have considered it ... have held that Bristol-Myers applies to claims brought by named plaintiffs in class actions."[9]

In contrast, the two federal appellate courts to address the issue have either rejected this notion or deferred its resolution to the consideration of class certification.[10] Again, the uncertainty should at least encourage defendants to challenge personal jurisdiction where it presents the potential of defeating a nationwide class.

These strategies are just part of the toolkit a litigator can use when confronted with a data privacy class action. While new technologies continue to emerge (and face challenges in the courts), these strategies when combined with other approaches and statute-specific considerations provide an efficient path toward resolution.

Adam Fox is a partner, and Kristin Bryan and Katy Spicer are senior associates, at Squire Patton Boggs LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] AT&T Mobility v. Concepcion, 563 U.S. 333 (2011).

[2] Sternlight, Jean, Tsunami: AT&T Mobility LLC v. Concepcion Impedes Access to Justice, 90:3 Oregon L. Rev. 703, at 704.

[3] Lamps Plus, Inc. v. Varela, 139 S. Ct. 1407 (2019).

[4] Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016).

[5] Bryant v. Compass Grp. USA, Inc., No. 20-1443, 2020 U.S. App. LEXIS 14256 (7th Cir. May 5, 2020).

[6] In re United States OPM Data Sec. Breach Litig., 928 F.3d 42, 55 (D.C. Cir. 2019).

[7] See Santana v. Take-Two Interactive Software, Inc., 717 F. App'x 12, 18 (2d Cir. 2017).

[8] Bristol-Myers Squibb Co. v. Superior Court, 137 S. Ct. 1773, 198 L. Ed. 2d 395 (2017).

[9] Goldstein v. GM LLC, No. 3:19-cv-01778-H-AHG, 2020 U.S. Dist. LEXIS 64851, *14 (S.D. Cal. Apr. 13, 2020) (collecting cases).

[10] See Mussat v. IQVIA, Inc., 953 F.3d 441, 447 (7th Cir. 2020) (rejecting the application of Bristol-Meyers to decline personal jurisdiction over a nationwide TCPA class action).