wiley

NEWSLETTER

The Risks of De-Identified Health Data Sharing: An Update on Potential State Privacy Claims and Standing

September 2020

Privacy in Focus®

On September 4, the U.S. District Court for the Northern District of Illinois issued a memorandum opinion and order in a closely watched privacy case in which the plaintiff brought suit based on a university's alleged disclosure of de-identified health information to a third party, but did not allege re-identification or any tangible harm. The case, *Dinerstein v. Google*, which we have previously written about here and here, has broader implications because re-identification of data is arguably easier in the world of big data and machine learning. In addition, the case raises the question of whether plaintiffs can bring suit under state law for alleged health privacy violations, even without a private right of action under the Health Insurance Portability and Accountability Act (HIPAA) or its implementing rules. In this case, the court granted the motion to dismiss, but the decision was mixed: While the court ultimately dismissed the plaintiff's purported privacy claims under state law, it endorsed a capacious view of Article III standing doctrine in privacy cases where plaintiffs fail to show tangible harm. Accordingly, this decision will do little to stem litigation seeking to squeeze amorphous and speculative privacy claims into unrelated state law claims.

Plaintiff's Theory in *Dinerstein*

The plaintiff ("Plaintiff") in *Dinerstein* brought a class action lawsuit arguing that the University of Chicago ("the University") breached its privacy obligations to hospital patients. According to Plaintiff, the University signed a deal with a third-party technology platform

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Boyd Garriott
Associate
202.719.4487
bgarriott@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

wherein it agreed to share de-identified health care data – including Plaintiff's health data. The crux of Plaintiff's argument was that this sharing constituted a privacy violation because – although the shared data was de-identified – the platform allegedly had so much data on individuals like himself that it could determine the subject of the health data if it so desired. However, Plaintiff did not allege that the platform actually identified any data subjects.

While Plaintiff's identity was apparently never associated with any health data, Plaintiff alleged three theories of injury to satisfy Article III standing – a jurisdictional bar that requires plaintiffs to show an "injury in fact" to seek relief in federal court. *First*, Plaintiff argued that the University injured him when it breached its contractual promise to keep patients' medical records confidential. *Second*, he argued that the sharing of medical information was an invasion of privacy, sufficient to establish injury in fact. *Third*, he argued that the University injured him by stealing the commercial value of his medical information.

The Court's Holding

The court accepted the first two theories of standing, rejected the third, and then dismissed all surviving claims on state law grounds.

First, the court agreed that "breach[ing] an express contract" – even without allegations of actual damages – "is sufficient for Article III standing purposes." The court first noted that common law authority and U.S Supreme Court Justice Thomas' concurrence in *Spokeo v. Robins* supported the proposition that breaches of contract – even breaches that do not result in tangible harm – are sufficient to establish injury in fact. It then analyzed the "conflicting precedent" on this issue and concluded that most – but not all – courts had come to the same conclusion. Lastly, the court cautioned that standing "is not dispensed in gross" and limited its grant of standing to only Plaintiff's breach of contract claim and closely related tortious interference of contract claim.

Second, the court found that Plaintiff's invasion of privacy theory was sufficient to establish Article III standing to assert a common law privacy tort. In particular, the court found the Seventh Circuit's opinion in *Bryant v. Compass Group* – a case we have previously discussed here – dispositive. In *Bryant*, the Seventh Circuit allowed a privacy lawsuit based on technical violations of a state statute to proceed without a showing of "tangible consequences" because the claim was based on a personal – rather than "public" – harm. Following this approach, the *Dinerstein* court reasoned that Plaintiff's allegation of wrongful disclosure alleged "a violation of his own rights" and was thus sufficient to establish Article III standing.

The court's invasion of privacy analysis, however, goes further than the Seventh Circuit in *Bryant*. Indeed, the *Dinerstein* court recognized that the facts before it "differ[ed] from *Bryant* and others cited" because those cases "involved statutes that created private rights of action." By contrast, *Dinerstein* held that disclosing "private information" to a third party – *independent of a statutory private right of action* – creates injury in fact, even without an allegation of tangible harm. The court relied upon this free-standing theory of privacy harm to find that Plaintiff had standing to assert an intrusion-upon-seclusion claim.

Third, the court rejected Plaintiff's argument that he was deprived of the value of his medical data. The court first found that the Plaintiff failed to establish that any statute or contract provided him a legal interest in his medical information. The court then noted that, even if he *did* have a property interest in this information, "his allegations d[id] not support an inference that the value of that property ha[d] been diminished by the [Defendants'] actions." That is, even if the Defendants gained a benefit from the information, Plaintiff did not lose anything.

Finally, while the court found that Plaintiff satisfied Article III standing for several theories, it subsequently dismissed each of them for failure to state a claim. In particular, the lack of economic damages for the alleged contract action – a hurdle that Plaintiff overcame for Article III standing – proved fatal to the contract claim under state law. And the court – again applying state law – held that adverse case law foreclosed Plaintiff's intrusion-upon-seclusion claim. The court also declined to "break new ground in state law" by recognizing Plaintiff's related breach of confidentiality claim in Illinois. Finally, the court dismissed Plaintiff's unjust enrichment claims, finding that they were derivative of other claims the court had already dismissed. Accordingly, the *Dinerstein* court found for the Defendants on every count and dismissed Plaintiff's complaint.[1]

Conclusion and Takeaways

Despite this victory, in finding that Plaintiff had a cognizable standing theory to bring a claim, the *Dinerstein* decision leaves the door open for future privacy lawsuits in which plaintiffs may attempt to shoehorn abstract privacy harms into state common law claims. Plaintiffs using similar theories have brought a deluge of claims based on amorphous theories of harm – with mixed success. This remains a risk in the area of sharing de-identified health data, which is typically governed under HIPAA rules that do not provide a private right of action.

Until Congress (via a preemptive federal privacy law) or the U.S. Supreme Court (via a case clarifying the Article III standing requirements for privacy suits) takes action, organizations must continue to evaluate their privacy practices and related contracts in light of risks associated with private litigation for alleged privacy violations.

---

[1] Though the court granted Plaintiff leave to file an amended complaint on or before October 15, 2020.