wiley

NEWSLETTER

Health Care Privacy Lawsuit Tees Up Next Standing Battleground in Privacy Cases – With Implications for Use of De-Identified Data

May 2020

Privacy in Focus®

In *Dinerstein v. Google* – a pending case in the Northern District of Illinois that we have previously covered – a plaintiff alleges that the University of Chicago and its Medical Center (collectively "the University") are liable for sharing de-identified electronic health records (EHRs) of patients with a third party. The plaintiff argues that this sharing violated a contract between himself and the University, as well as a state statute and common law, and a key part of the case involves applicability of the de-identification safe harbors within the Health Insurance Portability and Accountability Act (HIPAA) regulations. But the court will have to first decide whether the plaintiff has Article III standing to bring a case for disclosure of de-identified data – even when subject to a contract prohibiting re-identification – under a theory that it *could* potentially be re-identified at a later date. The answer to that question could have broad-ranging implications for the use and disclosure of de-identified data moving forward, which is a particularly critical issue when it comes to dealing with use of de-identified health data to help combat the ongoing COVID-19 pandemic.

In *Dinerstein*, the plaintiff alleges that the University improperly shared his EHRs with a third party. The plaintiff argues that although the University de-identified the data before sharing it with the third party, the third party would be able to re-identify the plaintiff with the EHRs using other information to which it allegedly has access. The plaintiff asserts several causes of action in connection with this alleged sharing: (1) breach of the plaintiff's health care contract with

Authors

Bruce L. McDonald
Senior Counsel
202.719.7014
bmcdonald@wiley.law

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Boyd Garriott
Associate
202.719.4487
bgarriott@wiley.law

Practice Areas

Privacy & Data Protection

Privacy, Cyber & Data Governance

the University, which allegedly incorporates compliance with HIPAA; (2) violations of the Illinois Consumer Fraud and Deceptive Business Practices Act; and (3) common law "intrusion upon seclusion" and unjust enrichment claims. Ultimately, however, the court may not need to address the merits of these claims because there is no actual allegation that the defendant re-identified – or is even contemplating re-identifying – the information. Indeed, the agreement under which the information was disclosed expressly prohibits re-identification.

Both defendants – the University and the third party – moved to dismiss for lack of Article III standing, among other grounds. Under U.S. Supreme Court standing doctrine, plaintiffs must show a concrete and particularized injury for a court to assert jurisdiction. The plaintiffs here argue that they showed four such injuries: (1) the economic value of the information that the University shared; (2) loss of privacy; (3) a breach of contract; and (4) an "overpayment" theory, i.e., that the plaintiff would not have paid for the University's health care services if he had known that it would disclose his health information. The defendants challenged each theory of injury in turn.

First, the defendants argued that the economic value of the plaintiff's personal information does not constitute a cognizable injury, citing a bevy of case law for the proposition that individuals typically lack a legal or monetary interest in their personal information. *Second*, defendants argued that the loss of privacy theory was insufficient to establish standing because (1) loss of privacy – without more – is too abstract a harm to constitute injury in fact, and (2) any harm beyond loss of privacy was too speculative to establish standing because the plaintiff did not allege that the third party with which the University shared information had made any attempt to de-identify the information.

Third, the defendants argued that breach of contract itself is not an adequate injury to establish standing under *Spokeo v. Robins*, which held that "a bare procedural violation, divorced from any concrete harm" is not a cognizable injury in fact. *Fourth*, the defendants argued that the "overpayment" theory of standing has generally been limited to breach of an express promise. They thus contended that the plaintiff's complaint was deficient because it failed to allege that the plaintiff was expressly promised privacy guarantees that the University failed to uphold.

The court has not yet ruled on these standing arguments, but the Ninth Circuit issued a decision involving many similar issues last month. In *In re Facebook, Inc. Internet Tracking Litigation*, the Ninth Circuit found that plaintiffs had standing to make a number of novel privacy claims based on (1) legal interests conferred by state and federal statutes, and (2) a theory of injury based on "unjust enrichment, even where an individual has not suffered a corresponding loss." Seizing on the second standing theory, the *Dinerstein* plaintiff has moved to cite the Ninth Circuit's opinion as a supplemental authority for his argument that the "medical records [at issue] have commercial value which has been unjustly taken by the University and given to" a third party.

As private plaintiffs have attempted to bring novel privacy claims under state law theories, Article III standing has been, and will continue to be, a key battleground for privacy litigation. Congress has seen many proposals on federal privacy legislation that would provide greater clarity on applicable law, but has thus far shown little progress toward reaching consensus on a final bill.[1] For its part, the Supreme Court has been reluctant to address standing in privacy cases since its 2015 opinion, *Spokeo v. Robins*, leaving these issues to be resolved in the lower courts.

The *Dinerstein* court's ultimate resolution of the pending motions in this case will not be the last word on these critical Article III standing issues. But particularly for companies dealing with de-identified personal data, the question of whether this kind of class action can move forward past its initial stages will be an important consideration for their business practices and approach to litigation.

---

[1] However, Congress has shown renewed interest in privacy issues in light of the recent pandemic.