Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

'Injury In Fact' Standing After Cambridge Analytica

By **Michael Ruttinger** (June 4, 2018, 1:02 PM EDT)

Michael Ruttinger

The Cambridge Analytica scandal that broke in March 2018 shocked the popular consciousness into an awareness of what data brokers, app developers, and consultants have known for years — that in the 21st century, your personally identifiable information is the new hot commodity. Some have even labeled PII "the new oil," underscoring the value that individual information like biometrics, DNA, geolocation history, or internet browsing history holds for those who seek to target individuals or groups of individuals for a variety of reasons, which can range from product marketing to predictive voting models. The public reaction has been predictable — outrage that Facebook allowed millions of its users' "private" PII to be harvested and ultimately sold by the Cambridge Analytica consulting firm.

Over the past few years one of the hottest topics in the field of privacy litigation has been the "injury in fact" standing requirement — specifically, whether unapproved access to your PII (typically because of a data breach) is a sufficiently "concrete and particularized" injury to permit you to bring a lawsuit in federal court. Privacy attorneys are already well familiar with the cornucopia of articles written about the U.S. Supreme Court's Spokeo v. Robins decision and its implications for data breach litigation standing.[1] But if your PII has value — the lesson of Cambridge Analytica — courts may find themselves revisiting the long-marginalized theory that the lost opportunity to profit from your own private data is itself sufficient to show you have been injured.

Cambridge Analytica and the Value of Personally Identifiable Information

The public reaction to the sale of data harvested by Cambridge Analytica is almost ironic because hundreds of millions of internet users give away some personally identifiable information every day, for free. PII has been defined broadly as any information about an individual, such as data that can distinguish or trace an individual's identity (e.g., name, Social Security number, date and place of birth, mother's maiden name, or biometric records), or that is "linkable" to an individual (e.g., medical, educational, financial, and employment information). Thirty years ago, if a consultant wanted to gather your PII there were relatively few accessible sources for doing so beyond conducting a telephone or by-mail survey. But in the 21st century, once-inaccessible private information has been converted into bits and bytes of data that can be transmitted instantaneously across continents via satellite or the internet. Your "person" — your creditworthiness, thoughts, desires, geolocation, biometrics, DNA, shopping habits, business ventures, religious views, political affiliations, or social preferences — can be gathered,

processed, bought, and sold by someone you have never met.

That is the Cambridge Analytica story. As of December 2017, there were over 2.13 billion active monthly Facebook users — a number that equates to more than a quarter of the estimated total global population (about 7.6 billion). In March 2018, Facebook stunned those users by announcing that the data firm Cambridge Analytica had been suspended from the social network for using data it improperly collected from users. Succinctly, Cambridge Analytica harvested the private information of more than 50 million of those users through an app developed by Aleksandr Kogan, a professor at Cambridge University, who then provided the raw profiles to the firm, which in turn profited from that data by providing political consulting services to the 2016 Trump presidential campaign.

Did the Cambridge Analytica scandal injure anyone? It would be hard — if not impossible — to evaluate whether it affected the 2016 presidential election in any meaningful way. Some still think that the disclosure of private information harmed them; allegedly affected Facebook users have sued both Facebook and Cambridge Analytica in a class action complaint filed in the District of Delaware. But putting aside whether those users will be able to establish that they were injured, the lesson Cambridge Analytica teaches about the commoditization of PII could have significant implications for the development of privacy law.

Rethinking Injury in the Cambridge Analytica Aftermath

The extent to which the law gives a remedy to individuals who have had their PII disclosed depends on how we characterize that information. To date, most scholars and practitioners characterize the "injury" as one that sounds in a right to privacy, but others have attempted novel, alternative theories.

For example, some litigants have sought to characterize PII as property; in Intel v. Hamidi[2] the court analogized the unauthorized acquisition of personally identifiable information to a trespass to chattel.[3] Proving such a claim, however, still required the plaintiff to prove a physical trespass — some actual interference with the physical functionality of a computer system.[4]

Meanwhile, others have speculated that unauthorized access to PII may be the basis for a cause of action sounding in the right to the publicity value of one's own personal information, citing the Restatement (Third) of Unfair Competition § 46, which identifies a claim against "one who appropriates the commercial value of a person's identity by using without consent the person's name, likeness, or other indicia of identity for purposes of trade." These causes of action, however, are rarely utilized and remain untested in privacy litigation.

But there is another theory that has been tested, albeit one that has been rejected in most courts outside of the Ninth Circuit. Specifically, data breach victims have previously sued — and in some cases been able to survive a motion to dismiss — based on allegations that the unauthorized access and dissemination of their PII diluted the inherent value of that data, causing a calculable, compensable harm.

The seminal case is Claridge v. RockYou Inc.[5] RockYou was an app publisher that developed apps for use on social networking websites like Facebook. In 2009, RockYou issued a press release and statements acknowledging that it had learned of a security flaw through which at least one confirmed hacker had accessed and copied the email and social networking login credentials of some 32 million users.[6] In the resulting class action, the plaintiff advanced a damages theory that the court itself called "novel" — that RockYou's "role in allegedly contributing to the breach of" the plaintiff's PII "caused

plaintiff to lose the 'value' of" that information "in the form of their breached personal data."[7] The court permitted the claim to survive a motion to dismiss, notwithstanding its skepticism:

On balance, the court declines to hold at this juncture that as a matter of law, plaintiff has failed to allege an injury in fact sufficient to support Article III standing. Not only is there a paucity of controlling authority regarding the legal sufficiency of plaintiff's damages theory, but the court also takes note that the context in which plaintiff's theory arises — i.e., the unauthorized disclosure of personal information via the internet — is itself relatively new, and therefore more likely to raise issues of law not yet settled in the courts.[8]

Most courts have refused to follow RockYou. The decision in Khan v. Children's National Health System[9] is typical; the court succinctly rejected the plaintiff's diminished-value theory by noting "[s]he does not, however, explain how the hackers' possession of that information has diminished its value, nor does she assert that she would ever actually sell her own personal information."[10] This remains the overwhelming trend among the federal courts.[11]

And yet, the RockYou court's novel damages theory remains alive and well within the Ninth Circuit. In 2014, the Ninth Circuit breathed life back into the theory — albeit in a nonprecedential opinion — when it reversed in part the dismissal of claims alleged against Facebook for disclosure of private information. The Ninth Circuit held that the district court erred by dismissing the plaintiffs' state law claims where they alleged "that they were harmed both by the dissemination of their personal information and by losing the sales value of that information."[12] Even though the theory was untested the court held that "[i]n the absence of any applicable contravening state law, these allegations are sufficient to show the element of damages for their breach of contract and fraud claims."[13] Since then, the diminished-value theory has remained viable — if rare — among courts within the Ninth Circuit.[14]

The Diminished Value Theory in the Wake of Cambridge Analytica

The public outcry in the wake of the Cambridge Analytica scandal bolsters one of the key assumptions underlying the diminished-value theory of injury in privacy litigation. Specifically, if your PII is a commodity that can be quantified, then it makes sense that it does have a quantifiable, inherent value. Consequently, it will be fascinating to see whether other courts become more receptive to the novel RockYou theory in the wake of the broader awareness the public has about the uses for their personal data in the wake of the scandal.

Even if courts become more willing to view PII as an inherently valuable, potentially marketable commodity, that does not mean courts will widely embrace the RockYou-style cause of action. A decision from 2013 may presage the better approach to these cases. In the Barnes & Noble Pin Pad Litigation,[15] the Northern District of Illinois acknowledged that "[a]n individual's PII has value, both to the individual and on the black market."[16] But the fact that personal data has value did not mean the diminished-value theory could proceed; as the court explained, the mere allegation of deprivation of value is not sufficient to establish standing. Rather, "[a]ctual injury of this sort is not established unless a plaintiff has the ability to sell his own information and a defendant sold the information."[17]

The Barnes & Noble approach makes sense because it recognizes the fact that PII does have inherent value in the 21st century, but also recognizes that in most instances its unauthorized disclosure will not deprive anyone of a meaningful opportunity to profit from it. Carving out instances of identity theft (no one wants to sell their own PII to a hacker), PII generally carries significant value only once it has been aggregated, so that consulting firms can craft advice based on thousands, or even millions, of users'

data. It is thus hard to imagine any scenario in which an individual would sue for the lost opportunity to sell his or her own PII, which would carry only nominal value. Further, while the Barnes & Noble approach could be a better fit for class actions based on the unauthorized sale of aggregated PII, the requirement that individuals demonstrate an ability to sell their information would be a significant obstacle to class certification.

Conclusion

As the RockYou court itself recognized, the context in which the diminished-value theory arises — "the unauthorized disclosure of information via the internet — is itself relatively new, and therefore more likely to raise issues of law not yet settled in the courts."[18] That fact remains true; even in 2011 when the RockYou court issues its holding, few would have imagined that a scandal like Cambridge Analytica would even be possible, much less that it would dominate news headlines. The law regarding injuries in data privacy litigation remains unsettled and it is only as events like the Cambridge Analytica scandal unfold that we will see the law evolve to match.

Michael J. Ruttinger is counsel at Tucker Ellis LLP.

[1] 136 S.Ct. 1540 (2016).

[2] 71 P.3d 296 (Cal. 2003).

[3] Id. at 1346-47.

[4] Id.

[5] 785 F Supp. 2d 855 (N.D. Cal. 2011).

[6] Id. at 859.

[7] Id. at 861.

[8] Id. at 861.

[9] 188 F. Supp. 3d 524 (D. Md. 2016)

[10] Id. at 533 (citing In re Science Applications Int'l Corp. Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 19 (D.D.C. 2014)).

[11] See, e.g., Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d 735, 755 (W.D.N.Y. 2017) ("Courts have rejected allegations that the diminution in value of personal information can support standing."); Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 659-60 (S.D. Ohio 2014) (rejecting a similar theory of standing because plaintiffs "have failed to allege any facts explaining how their PII [personally identifiable information] became less valuable to them (or lost all value) by the data breach"); see also

In re: Community Health Systems, Inc., No. 15-CV-222-KOB, 2016 WL 4732630, at *8-*9 (N.D. Ala. Sept. 12, 2016) ("This court joins those courts in rejecting the loss of intrinsic value theory to establish standing.").

[12] In re Facebook Privacy Litig., 572 F. App'x 494 (9th Cir. 2014).

[13] Id.

[14] See Svenson v. Google, Inc., No. 13-CV-4080, 2015 WL 1503429, at *2-*3 (N.D. Cal. Apr. 1, 2015) ("In light of the Ninth Circuit's ruling, this Court concludes that Svenson's allegations of diminution in value of her personal information are sufficient to show contract damages for pleading purposes.").

[15] No. 12-cv-8617, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013).

[16] Id. at *2.

[17] Id. at *5.

[18] RockYou, 785 F. Supp. 2d at 861.