Daniel's Law: the next wave in privacy litigation

By Philip N. Yannella, Esq., and Tim Dickens, Esq., Blank Rome LLP

MARCH 20, 2024

Privacy litigation remains one of the fastest growing areas of litigation in the U.S. Plaintiff's privacy attorneys have a well-developed playbook for asserting new claims, a pillar of which is to identify new website technologies that allegedly violate older privacy laws that provide for liquidated damages. The recent surge in litigation alleging that the use of Meta Pixel, a tracking technology, violates state wiretap laws and/or the Video Privacy Protection Act (VPPA) is a prime example of this approach.

The latest boomlet in privacy litigation may be happening in New Jersey, where over 140 lawsuits have been filed in February alone against data brokers, alleging violations of New Jersey's "Daniel's Law."

Similarly, plaintiff's lawyers have creatively advanced new theories of liability under the Illinois Biometric Information Privacy Act (BIPA) based on website "try-on" and identity verification technologies. Another common trend is to target companies that allegedly profit off the sale of personal information, such as data brokers and online look-up services.

The latest boomlet in privacy litigation may be happening in New Jersey, where over 140 lawsuits have been filed in February alone against data brokers, alleging violations of New Jersey's "Daniel's Law." This law prohibits the posting or disclosure of address and telephone information of certain New Jersey public officials, including judges, prosecutors and law enforcement. The suits allege the data brokers and look-up services did not take down protected contact information that had been posted on public sites within the proper time frame as required under the law.

Daniel's Law may be enforced through an assignable private right of action with liquidated damages equal to the higher of actual damages or $1,000 per violation of the act. Like other kinds of privacy litigation, one problem for companies defending claims under Daniel's Law is the expansive nature of the law, which broadly defines key concepts, such as who qualifies as a "covered person" and what constitutes a disclosure.

Overview of the law

New Jersey Statute § 56:8-166.1, better known as "Daniel's Law," (https://tinyurl.com/yzxh9pn3) was passed in 2020 in response to the fatal shooting of Daniel Anderl, the son of a federal judge, by a disgruntled attorney who was able to find the home address of the judge on the internet. The law covers current and former judicial officers, law enforcement officers, prosecutors, and related officials as well as "the immediate family members" of any such persons.

Daniel's Law prohibits any person from posting, reposting, or otherwise making available the home address or unpublished telephone number of any "covered person" with the intent to expose that person to harassment or risk of harm to life or property or with reckless disregard to the possibility.

The law provides a 10-day cure period, triggered by receipt of a "written notification" from, or on behalf of, a covered person. Failure to remove or delete any such post within this 10-day window opens the door to a private right of action for the greater of actual damages or statutory damages of at least $1,000 per violation, as well as attorney fees and punitive damages.

Importantly, Daniel's Law specifically permits covered persons to authorize a third party to assert the covered person's rights on their behalf as an "authorized person."

Daniel's Law does not create liability for telephone directories or directory assistance *unless* the covered person requested to be removed from the relevant directory prior to the applicable publication deadline. The law provides an exception for news media organizations for failure to remove information from previously printed content.

The statutory definition of a "covered person" includes any "active, formerly active, or retired judicial officer, law enforcement officer, or child protective investigator in the Division of Child Protection and Permanency or prosecutor" as well as any *immediate family member* residing in the same household. "Immediate family member" in turn includes any family member related by blood. Another seemingly

open-ended term is the phrase "otherwise make available," which could cover a broad range of online and offline activities.

Importantly, Daniel's Law specifically permits covered persons to authorize a third party to assert the covered person's rights on their behalf as an "authorized person." This express permission of authorized parties has facilitated the mass organization and sending of deletion requests by potential plaintiffs and their counsel. These template requests, reminiscent of similar template requests sent under state comprehensive data protection laws, allow plaintiffs to select from a broad range of data brokers who may have posted or sold their information.

Details of the complaints

Attorneys representing Atlas Data Privacy Corporation, a New Jersey company, filed 142 complaints under Daniel's Law in February 2024 alone. Atlas functions as an assignee of claims from police officers asserting that the defendant companies refused requests to remove online postings containing their protected information. The primary target of these complaints has been large online data brokers that create and disseminate consumer profiles and online lookup services.

The complaints allege that plaintiff judges or police officers were harmed because of the publication of their home addresses, detailing violent threats made to individual plaintiffs, threatening notes left at plaintiffs' properties, and thwarted attacks on plaintiffs.

According to the complaints, plaintiff's claims were assigned to Atlas, which sent deletion requests to defendants. The defendants allegedly did not remove the information within the 10-day window, the complaint states. The complaints allege that Atlas Data Privacy Corporation has amassed a list of nearly 1,000 potential brokers, meaning future waves of litigation may be soon to follow.

As of this writing, none of the defendants in these cases have filed answers to the complaints.

Moving forward

Daniel's Law litigation is still in its infancy, and no court has yet ruled on a motion to dismiss or opined on key definitions under the law, such as who qualifies as a "covered person."

In the short term, entities that have implemented data subject request tools or procedures for responding to data subject requests under state privacy laws, such as the California Consumer Privacy Act, must be careful to ensure they do not miss the 10-day deletion window. Procedures that anticipate a 45-day response timeline, as generally required under U.S. privacy laws, may cause entities to miss the 10-day deletion window required under Daniel's Law.

Finally, more states may begin to move forward in passing laws reminiscent of Daniel's Law, creating new avenues of liability. For example, the Maryland Legislature (https://tinyurl.com/4zxmyaf9) is considering a similar bill with a private right of action following the murder of Judge Andrew F. Wilkinson outside of his home.

About the authors

Philip N. Yannella is a partner and co-chair of the privacy, security and data protection group at **Blank Rome LLP**. He has counseled and represented clients in a wide array of privacy and data security litigations. He is the author of "Cyber Litigation" (Thomson Reuters 2021). **Tim Dickens** is an associate in the privacy, security and data protection group at the firm. He regularly counsels organizations on compliance with domestic and international privacy and data security laws. The authors are based in Philadelphia.

This article was first published on Reuters Legal News and Westlaw Today on March 20, 2024.