5. Data brokers and judicial privacy litigation

By Kayla Bushey, CIPP/US

A new state law aimed at protecting the personal information of state and federal public officials incidentally created a new era of data privacy litigation in the state and federal courts of New Jersey. Data brokers and other consumer-facing businesses now face rising litigation risks under Daniel's Law, exposed to financial and reputational damage, as individuals assert their privacy rights under the law.

Daniel's Law of New Jersey

Daniel's Law provides covered persons the right to request businesses to remove their home addresses and unpublished telephone numbers from public databases and refrain from further publishing this information. Covered persons include federal and state judges, prosecutors, law enforcement officials and their family members. The law passed in 2020 after an assassination attempt on U.S. District Court for the District of New Jersey Judge Ester Salas tragically killed her son Daniel Alder and critically injured her husband.

In 2023, the New Jersey legislature amended the law to allow covered persons to assign their claims to a third party. This has led to hundreds of lawsuits filed against various defendants including "online information services, traditional data brokers, enterprise software companies, real estate websites, and consumer reporting agencies." The law carries fines of USD1,000 per violation.

Upon passage of the 2023 amendment, state and federal courts saw an influx of lawsuits brought under the law. Many of these cases were brought by Atlas Data Privacy Corporation as an assignee of law enforcement officers with claims under the law. By May 2024, Atlas Data Privacy Corporation was the assignee of nearly 20,000 covered persons.

The U.S. Federal District Court of New Jersey consolidated 60 separate lawsuits filed by Atlas after the defendants removed the cases from New Jersey state court to federal court and filed motions to dismiss on First Amendment grounds. Here, defendants argued the law is impermissibly overbroad and infringes their First Amendment rights. They also argued the law placed content-based restrictions on speech that could not survive the U.S. Supreme Court's strict scrutiny standard of review.

In November 2024, U.S. District Court for the Eastern District of Pennsylvania Judge Harvey Bartle III denied the defendant's motion to dismiss the lawsuit after finding strict scrutiny was not the appropriate judicial standard of review. Instead, Bartle concluded Daniel's Law is definitively a privacy law, and therefore, First Amendment challenges must follow the balancing test outlined in Florida Star v. B.J.F.

Under this Supreme Court jurisprudence, the court must balance the right to privacy against the right of free speech using three factors: whether the defendant lawfully obtained information that is of public significance, whether the law "serves a need to further a state interest of the highest order," and whether the law serves the state's purported "significant interest " that is not "underinclusive."

Bartle found the state's interest in protecting public officials' home addresses and telephone numbers were not outweighed by any public significance arguments made by the defendants. Therefore, the court rebuffed the defendant's facial challenges to the law and denied their motions to dismiss.

The defendants in these 60 cases are not the first to challenge the law on First Amendment grounds. A journalist challenged the law in September 2023, arguing it violated his freedom of speech when he was barred from publishing the address of a New Brunswick public official. The state district court ruled against the journalist and a panel of appellate judges affirmed the lower court's finding in April 2024. The plaintiff has petitioned to the New Jersey Supreme Court.

Maryland passed a similar statute after a Maryland judge was killed outside his home in 2023. Georgia, Florida, Idaho, Minnesota, New York and Wisconsin have also passed their own judicial data privacy and security laws. Each of these state laws vary in their scope and available remedies. The Florida, Idaho, Maryland, Minnesota and New York laws are already in effect, while the Georgia and Wisconsin laws will come into effect in July and April 2025, respectively.

Furthermore, Congress passed its own version of Daniel's Law, although it is more limited in scope, with the James M. Inhofe National Defense Authorization Act for the Fiscal Year 2023. This provision of the defense bill prohibits data brokers from sharing the personal information of federal judges. It also allows federal judges to redact information provided by federal agencies.

How can entities comply with Daniel's Law?

Because Daniel's Law mandates the covered information must be removed within 10 days of receiving a proper request, entities that may collect data from covered persons under the law should create streamlined procedures for responding to potential take-down requests.

Businesses and individuals that receive take-down requests can take steps to prepare for compliance with this law. Businesses should maintain comprehensive data mapping or take inventory of existing data to properly map what information they may have. Businesses should also establish and maintain proper data governance within the organization to understand who will process and complete these take-down requests.

This law will also require businesses to sufficiently manage third-party vendors, develop proper data disposal protocols and retain records of compliance with take-down requests received by the organization. Although the existing class-action lawsuits have not reached final decisions on the merits of the law, New Jersey courts have not been persuaded by First Amendment challenges thus far. Barring any new defenses raised by entities subject to Daniel's law, businesses must take steps to respect the rights of covered persons asserted under the law.appoint an authorized representative in the EU in accordance with Article 54.