Privacy & Cybersecurity Update

March 2024

Daniel's Law and the Explosion of Privacy Claims Impacting Real Estate and Tech Platforms

In February 2024, over 100 complaints were filed in New Jersey state courts concerning alleged violations of Daniel's Law (codified as amended at N.J.S.A. 56:8-166.1). These lawsuits target organizations that post certain residential addresses and unpublished telephone numbers on the internet and, as could be expected, a significant number of these claims target real estate platforms and similar online services that publish publicly available property records and personal contact data. The law was recently amended to *require* courts to award statutorily defined damages to aggrieved parties. To better avoid litigation costs and reputational harm, organizations should immediately identify whether they are subject to Daniel's Law and ensure they have implemented a comprehensive compliance program.

What Is Daniel's Law?

New Jersey Governor Phil Murphy signed into force Daniel's Law on November 20, 2020. The law is named for U.S. District Court Judge Esther Salas' son Daniel Anderl, who was brutally shot and killed in the family's home in 2020 by a disgruntled former litigant who also severely wounded Judge Salas' husband. The gunman had found Judge Salas' home address on the internet. Daniel's Law was enacted to prevent further acts of violence targeting government officials by prohibiting the disclosure of their personal information (e.g., their residential addresses, unpublished telephone numbers) and that of their close family members.

Who Is a Covered Person?

Daniel's Law primarily protects the personal information of "covered persons," whom the law defines as essentially "an active, formerly active, or retired judicial officer, law enforcement officer, or child protective investigator … , or prosecutor" and their immediate family members residing in the same household.

How Is Personal Information Protected?

Daniel's Law creates a framework in which an "authorized person" can seek to "prohibit the disclosure of the home address or unpublished home telephone number of any covered person." To accomplish this, the authorized person must provide "written notice" to a relevant party stating that they are in fact an authorized person and requesting that the party "cease the disclosure of the information and remove the protected information from the Internet or where otherwise made available." This is often referred to a "take-down" request.

An "authorized person" means either a covered person or any other persons listed in the statute (e.g., certain types of U.S. Marshals Service or U.S. District Court clerk designees, designated trustees, estate executors, and parents or legal guardians).

Am I Subject to Daniel's Law?

Daniel's Law primarily targets individuals, businesses, and associations that disclose on the internet or "otherwise make available" the home addresses or unpublished telephone numbers of covered persons. Accordingly, many real estate platforms and similar online services that provide property-related personal information or other personal contact data can be subject to the law.

What Are the Law's Confidentiality and Compliance Requirements?

Any person, business, or association that receives a take-down request from an authorized person is required, within 10 days, to "not disclose or re-disclose on the Internet or otherwise make available, the home address or unpublished home telephone number of any covered person."

Are There Exceptions to Daniel's Law's Confidentiality Requirements?

Daniel's Law provides several exceptions "to the requirement to redact, and the prohibition against the disclosure of, a home address" otherwise mandated by the law, including:

- Certain types of copies of voter registration files maintained in the statewide voter registration system
- Certain types of documents affecting the title to real property
- Certain records evidencing any lien, judgment, or other encumbrance upon real or other property
- Records related to property that is presumed abandoned under New Jersey law
- Information in any document, record, information, or database shared with or otherwise provided to any other government entity

The law notes that the New Jersey Director of the Division of Taxation "may" issue guidance, guidelines, or rules and regulations necessary to effectuate how these exceptions can be invoked.

Separately, Daniel's Law provides that it must not be construed to impose liability "on the news media for failure to remove information from previously printed newspapers," or "relating to telephone directories or directory assistance unless the covered person has requested to be unpublished in the directory and directory assistance by the applicable publication deadline."

Explosion of Class Action Lawsuits

As noted above, there were over 100 lawsuits filed in February 2024 alone related to Daniel's Law. These claims are often brought by "assignees" of covered persons and allege that the defendants failed to comply with take-down requests. The complaints often claim to represent thousands of covered persons and hundreds of thousands of violations of take-down requests.

Pursuant to Daniel's Law statutory damages, judges are *required* to award damages to aggrieved parties as follows:

- Actual damages, but not less than liquidated damages computed at the rate of $1,000 for *each violation*
- Punitive damages upon proof of willful or reckless disregard of the law
- Reasonable attorney's fees and other litigation costs reasonably incurred
- Any other preliminary and equitable relief as the court determines to be appropriate

The law does not provide for any cure period to resolve disputes of noncompliance (e.g., failure to comply with a take-down request in the designated time frame) prior to filing a complaint.

Risk Mitigation Measures

Organizations should consider implementing and maintaining several measures to better protect themselves from a Daniel's Law-type of lawsuit:

- *Data mapping/inventory.* Organizations should understand and document whether they are collecting, retaining, and posting on the internet the personal information of covered persons. This data "map" or "inventory" should identify the types of personal data the organization collects and how it is used, shared (especially in the online environment), retained, and disposed.
- *Take-down processes*. Similar to requirements under consumer data protection laws, organizations should have clear and readily available processes for intaking, analyzing, and responding to take-down requests.
- *Record of compliance*. Organizations should maintain all records and communications demonstrating their compliance with Daniel's Law, including communications to and from covered persons and evidence of online

resources before and after they comply with a take-down request.

- *Data disposal*. It is important that organizations have documented data purge/deletion processes to ensure that covered personal information redacted from their online resources pursuant to a take-down request cannot be uploaded without appropriate senior-level approval.
- *Data governance*. Organizations should create formal processes and rules for when they are permitted to collect and publicly display personal information and when such activities need approval by senior management or legal counsel.
- *Vendor management*. It is important for organizations to understand whether third-party service providers operate or otherwise host their data online. In such circumstances, these service providers have to be properly vetted to ensure they can comply with take-down requests and that they are contractually liable for failing to adhere to take-down instructions.

Litigation Considerations

The recent surge in class action lawsuits related to Daniel's Law will likely lead to protracted litigation, especially where plaintiffs think they will recover thousands of dollars in damages (if not more). However, the law contains many ambiguities and other clauses that might it make it ripe for facial and constitutional challenges. Also, courts should consider whether they have jurisdiction over real estate and technology platforms that operate nationwide and do not specifically target New Jersey residents. In addition, where these types of class actions are removed to federal courts, plaintiffs may find it difficult to address issues of standing and concrete harm, particularly if an organization subject to a take-down request removes the personal information in question prior to any actual harm or damages impacting a covered person (but perhaps beyond the 10-day take-down window required by law). Finally, as is often seen in the consumer privacy context, many of the plaintiffs' complaints and demand letters are "recycled templates" and lack specificity around individual plaintiffs and claims, which could serve as another potential basis for dismissal.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

Jennifer A. Adler
404.407.3694
Jennifer.Adler@ThompsonHine.com

Robyn Minter Smyers
216.566.5830
614.469.3352
Robyn.Smyers@ThompsonHine.com