Articles + Publications | May 23, 2024

Maryland Enacts the Judge Andrew F. Wilkinson Judicial Security Act: Are More Daniel's Laws on the Horizon?

WRITTEN BY

Timothy J. St. George | Alan D. Wingfield | Robert Austin Jenkin, II | Angelo A. Stio III | Laura Hamady

Maryland has joined the growing list of states to pass a law — the Judge Andrew F. Wilkinson Judicial Security Act — that allows current and former members of the Maryland judiciary to request certain of their personal information not be made available to the public. The act is named after former Washington County Circuit Court Judge Andrew F. Wilkinson, who was senselessly murdered by an individual involved in a divorce proceeding over which Judge Wilkinson was presiding. The act passed the Maryland House and Senate unanimously and will take effect on June 1, 2024.

Maryland's act follows the onset of litigation involving New Jersey's "Daniel's Law," and passage of the federal law that seeks to protect the safety of members of the judiciary by allowing persons protected by the laws to limit public access to their personal information. So far in 2024, 37 states have begun considering or adopted similar privacy-based legislation designed to protect members of the judiciary and, in some states, other government officials involved in law enforcement.

"Protected Individuals" Under the Act

The act applies to "protected individuals," which are defined as current or retired: (i) Maryland judges or justices; (ii) federal judges domiciled in Maryland; (iii) Maryland magistrates; (iv) federal magistrates domiciled in Maryland; and (v) commissioners of the District Court of Maryland, as well as their children, spouses, or other dependents who reside in the same household.

"Personal Information" Under the Act

The act defines "personal information" as: (i) a home address; (ii) a home telephone number; (iii) a mobile telephone number; (iv) a personal email; (v) a social security number; (vi) a driver's license number; (vii) a federal tax identification number; (viii) a bank account number; (ix) a credit or debit card number; (x) a license plate number or unique identifier of a vehicle; (xi) a birth or marital record; (xii) a child's name; (xiii) a school or daycare; (xiv) a place of worship; or (xv) a place of employment for a spouse, child, or dependent of a "protected individual."

Publications Covered by the Act

The act prevents a person from publishing the personal information of a protected individual and defines "publish"

as “to post or otherwise make available to the general public on the internet, social media, or social networks.”

Invoking the Act

A “protected individual” must submit or have the Office of Information Privacy (OIP) submit on their behalf, a written request to have an online publication removed under the act. The act notes that a written request can be sent by mail or email and must “adequately identify the document, posting, or other publication containing the personal information.”

The written request must also provide “sufficient information” confirming the requesting party’s status as a “protected individual,” unless the request is made by the OIP on the requester’s behalf.

Notably, while the act empowers a “protected individual” to preemptively request that a governmental entity “not publish the protected individual’s information,” the act does not provide that authority against private persons. The act only allows a “protected individual” to request that private persons remove information that has been “published.”

Exemptions to the Act

The act contains two notable exemptions. It excludes from the definition of “personal information”: (i) information that has been publicly disclosed with the consent of the protected individual; and (ii) “information that is relevant to and displayed as part of a news story, commentary, editorial, or any other speech on matters of public concern.”

Compliance Period

An entity or person receiving a request under the act must comply with the request within 72 hours of receipt. Once complied with, the entity or person must notify the requestor of the removal by certified mail or e-mail.

Enforcement

A protected individual or the OIP can bring an action against a governmental entity for failure to comply with the act. The act authorizes awards of declaratory relief, injunctive relief, and reasonable attorney’s fees and costs, but does not provide for the recovery of statutory damages.

The act also allows for a protected individual or the OIP to bring an action against a private person for failure to comply with the act. It authorizes awards of declaratory relief, injunctive relief, damages incurred as result of the noncompliance and reasonable attorney’s fees. The act further authorizes the award of punitive damages in cases of willful noncompliance.

Criminal Actions

The act also made it a misdemeanor for an individual to knowingly publish “personal information” on a “protected individual” when the publishing of that information results in an assault, harassment, trespass, or malicious destruction of property.

Creation of the Judicial Address Confidentiality Program

The act also created the Judicial Address Confidentiality Program, managed by the OIP. A protected individual may apply to join the program, which requires the individual to prove their protected individual status. Once proven, the OIP may request that a person or governmental agency use a substitute address designated by the OIP as the protected individual's address, request the shielding of real property records showing the protected individual's ownership interest in the real property, or request the shielding of the protected individual's actual address from public inspection in a record maintained by a government entity.

The act further provides that a person may not knowingly disclose a program participant's actual address, and that the participant, or the OIP, may bring an action for declaratory relief, injunctive relief, and reasonable attorney's fees for a violation of this section. This section of the act does not authorize actions against governmental agencies.

Maryland Law vs. New Jersey Law

There are significant differences between the act and New Jersey's Daniel's Law. As an initial matter, the laws differ in whose information they protect and what information is protected. The Maryland act only applies to "personal information" of current and former members of Maryland's judiciary. Daniel's Law, on the other hand, applies not only to New Jersey's judiciary, but also to law enforcement officers, child protective investigators in the Division of Child Protection and Permanency, and prosecutors. As for the information protected, Maryland's law is significantly broader. The act defines "personal information" to include: (i) a home address; (ii) a home telephone number; (iii) a mobile telephone number; (iv) a personal email; (v) a social security number; (vi) a driver's license number; (vii) a federal tax identification number; (viii) a bank account number; (ix) a credit or debit card number; (x) a license plate number or unique identifier of a vehicle, (xi) a birth or marital record, (xii) a child's name; (xiii) a school or daycare; (xiv) a place of worship; or (xv) a place of employment for a spouse, child, or dependent of a "protected individual." Daniel's Law only protects three of those 15 categories: (i) home address; (ii) unlisted home telephone number; and (iii) unlisted mobile telephone number.

The laws also greatly differ in their enforcement mechanisms and remedies. First, while both laws require the provision of written notice requesting the nondisclosure of certain information, Daniel's Law does not define or describe what constitutes sufficient "written notice" under the law. Conversely, Maryland expressly requires that the written notice be: (i) sent by certified mail or by e-mail; (ii) "provide sufficient information to confirm the requester is a 'protected individual'" (unless the notice comes from the OIP); and (iii) "adequately identify the document, posting, or other publication containing the personal information." Second, under Daniel's Law, a "covered person" can assign their right to bring a civil action for a violation of the statute. The act does not contain a similar assignment provision. Third, Daniel's Law requires that a court award "actual damages, but not less than liquidated damages computed at the rate of $1,000 for each violation," while the act only provides for actual damages against persons found to have violated the act.

Perhaps most notably, the act and Daniel's Law differ significantly in terms of who they can be enforced against and whether enforcement can be preemptive. Under Daniel's Law, a "covered person" can prevent a "person, business, or association" from "disclos[ing] or re-disclos[ing]" their home address or unpublished home telephone number. Conversely, under the act, a "protected individual" can only demand that a "person who has published

the Protected Individual's personal information remove the Protected Individual's Personal Information from publication." Therefore, the act, unlike Daniel's Law, does not apply to businesses and associations, and does not allow for preemptive requests for the nondisclosure of "personal information" pertaining to a "protected individual."

Lastly, the laws differ in their compliance periods. Perhaps because the act is purely a remedial statute when applied against a private party, it only provides a person 72 hours to comply with a written request. This is a much shorter compliance period than the 10 business days provided under Daniel's Law.

The laws do have some similarities. Both provide for an award of punitive damages against a private party found to have willingly violated the statute. Likewise, both have an exception for newspapers articles published before the enactment of the laws. Though it should be noted that the act's exception is much broader in that it includes any "information that is relevant to and displayed as part of a news story, commentary, editorial, or any other speech on matters of public concern" and is not limited to publications pre-dating the act's enactment.

The below chart provides a high-level comparison of the act with Daniel's Law, as well as the Daniel Anderl Judicial Security and Privacy Act of 2022 (the Anderl Act) which is the federal version of Daniel's Law.

Final Takeaway

With the act's passage and effective date of June 1, and other states continuing to consider similar legislation, it is important that entities be aware of these laws and review their policies for potential compliance with requests sent by individuals demanding non-disclosure under applicable state and federal law.

	Anderl Act	Daniel's Law	Maryland Act
Who is protected?	"At-risk individuals," which includes: (i) active, senior, recalled, and retired federal judge, justice, or magistrate; (ii) a spouse, parent, sibling, or child of an active, senior, recalled, or retired federal judge, justice, or magistrate; and (iii) an individual living in the household of an active, senior, recalled, or retired federal judge, justice, or magistrate.	"Covered persons" which includes an active, formerly active, or retired: (i) judicial officer; (ii) law enforcement officer; (iii) child protective investigator in the Division of Child Protection and Permanency; (iv) prosecutor; and (v) any immediate family member residing in the same household as an individual that satisfies categories (i-iv).	"Protected individuals" which includes: (i) current or retired Maryland justice or judge; (ii) current or retired federal judge domiciled in Maryland; (iii) current or retired Maryland magistrate; (iv) current or retired federal magistrate domiciled in Maryland; (v) current or retired commissioner of the District Court of Maryland; and (vi) a spouse, child, or dependent residing in the same household as an individual that satisfies categories (i-v).
Allows assignment of claims?	No.	Yes.	No.

Who can issue takedown notices?	A written takedown request sent to a business must be made by the at-risk person.	A written takedown request can be sent to a business by: (i) the covered person; (ii) a designee of the U.S. Marshals Service or the clerk of any U.S. District Court filing a notice on behalf of a federal judge; (iii) a designated trustee, estate executor, or power of attorney acting on behalf of a covered person who is deceased or incapacitated; and (iv) the parent or legal guardian acting on behalf of an immediate family member.	A written takedown request may be sent to a person by the protected individual or the OIP.
What constitutes a valid notice by an agent?	Notice must "be in writing and contain information necessary to ensure compliance with this section, including information expressly referencing the prohibition on the posting or transfer of covered information, information regarding redress and penalties for violations provided in subsection (f), and contact information to allow the recipient to verify the accuracy of any notice or request and answer questions by the recipient of the notice or request."	Unclear.	A takedown request to a person must be: (i) in writing; (ii) sent by certified mail or e-mail; (iii) provide sufficient information to confirm the requestor is a protected individual (unless sent by the OIP); and (iv) adequately identify the document, posting, or other publication containing the personal information.
Allows private causes of action/enforcement?	First resort: "the director of the Administrative Office of the U.S. Courts, or the designee of the director, may file an action seeking injunctive or declaratory relief in any court of competent jurisdiction, through the Department of Justice." Only if a defendant knowingly or willfully violates such order or injunction may a private party	Yes, as a first resort.	Yes, as a first resort.

	institute an action for damages.		
Damages	Actual damages.	Actual damages, liquidated damages, attorney's fees, costs, and punitive damages (if willfulness is found).	Actual damages, reasonable attorney's fees, and punitive damages (if willfulness is found).
Who do restrictions apply to?	**Data brokers**: With or without a takedown request, data brokers may not "knowingly sell, license, trade for consideration, transfer, or purchase covered information of an at-risk individual or immediate family members." **Other persons and businesses**: may not "publicly post or publicly display on the internet covered information of an at-risk individual or immediate family member if the at-risk individual has made a written request."	A **business**, **person**, or **association** "shall not disclose or re-disclose on the Internet or otherwise make available" covered information.	Persons.
What data is covered?	"Covered information" which includes: (i) a home address, including primary residence or secondary residences; (ii) a home or personal mobile telephone number; (iii) a personal email address; (iv) a social security number or driver's license number; (v) a bank account or credit or debit card information; (vi) a license plate number or other unique identifiers of a vehicle owned, leased, or regularly used by an at-risk individual; (vii) the identification of children of an at-risk individual under the age of 18; (viii) the full date of birth; (ix) information regarding current or future school or day care attendance, including the name or address of the school	Home address or unpublished home or cell phone number.	"Personal information" which includes: (i) a home address; (ii) a home telephone number; (iii) a mobile telephone number; (iv) a personal email; (v) a social security number; (vi) a driver's license number; (vii) a federal tax identification number; (viii) a bank account number; (ix) a credit or debit card number; (x) a license plate number or unique identifier of a vehicle; (xi) a birth or marital record; (xii) a child's name; (xiii) a school or daycare; (xiv) a place of worship; or (xv) a place of employment for a spouse, child, or dependent of a protected individual.

	or day care, schedules of attendance, or routes taken to or from the school or day care by an at-risk individual; and (x) information regarding the employment location of an at-risk individual, including the name or address of the employer, employment schedules, or routes taken to or from the employer by an at-risk individual.		
Who is a "data broker"?	"[A]an entity that collects and sells or licenses to third parties the personal information of an individual with whom the entity does not have a direct relationship." **Exclusions**: the definition does not include a commercial entity engaged in the following activities: (i) engaging in reporting, news-gathering, speaking, or other activities intended to inform the public on matters of public interest or public concern; (ii) providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier; (iii) using personal information internally, providing access to businesses under common ownership or affiliated by corporate control, or selling or providing data for a transaction or service requested by or concerning the individual whose personal information is being transferred; (iv) providing	Undefined.	Undefined.

	publicly available information via real-time or near-real-time alert services for health or safety purposes; (v) a consumer reporting agency subject to the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); (vi) a financial institution subject to the Gramm-Leach-Bliley Act (Public Law 106-102) and regulations implementing that title; (vii) a covered entity for purposes of the privacy regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d-2 note); or (viii) the collection and sale or licensing of covered information incidental to conducting the activities described in clauses (i) through (vii).		
Exceptions	The restriction on "**other persons and businesses**" does not apply to: (i) the display on the internet of the covered information of an at-risk individual or immediate family member if the information is relevant to and displayed as part of a news story, commentary, editorial, or other speech on a matter of public concern; (ii) covered information that the at-risk individual voluntarily publishes on the internet after the date of the act's enactment; or (iii) covered information lawfully received from a federal government source (or from an employee or agent of the	A defendant **can disclose information in the ordinary course of business** if they are providing the information to: (i) a title insurance company, a title insurance agent, or an approved attorney; (ii) a mortgage guarantee insurance company; (iii) a mortgage loan originator; (iv) a registered title search business entity; (v) a real estate broker, a real estate salesperson, a real estate broker-salesperson, a real estate salesperson licensed with a real estate referral company, or a real estate referral company; or (iv) an individual or business that	The Act **excludes from the definition** of "personal information": (i) information that has been publicly disclosed with the consent of the protected individual; and (ii) information that is relevant to and displayed as part of a news story, commentary, an editorial, or any other speech on matters of public concern.

federal government).

The restriction on **data brokers** does not: “prohibit information sharing … to a Federal, State, Tribal, or local government, or any unit thereof.”

There is **no restriction** on: “(i) the lawful investigation or reporting by the press of any unlawful activity or misconduct alleged to have been committed by an at-risk individual or their immediate family member or (ii) the reporting on an at-risk individual or their immediate family member regarding matters of public concern.”

has made or received an offer for the purchase of real estate and real property, or any portion thereof, to or from a covered person whose address is subject to redaction or nondisclosure.

The law **exempts from nondisclosure**: (i) records and documents, including Uniform Commercial Code filings and financing statements, maintained by the Division of Revenue and Enterprise Services in the Department of the Treasury; (ii) petitions naming candidates for office; (iii) records evidencing any lien, judgment, or other encumbrance upon real or other property; (iv) assessment lists subject to inspection pursuant to R.S.54:4-38 when inspected in person; and (v) property that is presumed abandoned under the “Uniform Unclaimed Property Act.”

RELATED INDUSTRIES + PRACTICES

- Consumer Financial Services
- Privacy + Cyber