NORTH CAROLINA JOURNAL of
LAW & TECHNOLOGY
Volume 27, Issue 3 2026

ARTICLE

JUDICIAL SECURITY IN THE DATA ECONOMY

Anthony M. Ciolli†

The murder of Daniel Anderl, the son of U.S. District Judge Esther Salas, exposed the ease with which publicly available personal data can be weaponized against members of the judiciary. In response, Congress enacted the Daniel Anderl Judicial Security and Privacy Act, and several states adopted analogous statutes—commonly known as "Daniel's Laws"—to restrict the dissemination of judges' home addresses and other sensitive personal information. Critics have argued that these laws violate the First Amendment by restricting the publication of truthful information, and at least one federal court has invalidated portions of a state statute on that basis. This Article contends that such criticisms rest on a fundamental misunderstanding of what these statutes regulate. Properly understood, the federal and state Anderl Acts do not restrict speech on matters of public concern but instead regulate the commercial dissemination of highly sensitive personal data—an area long subject to legislative regulation. By examining the structure of the federal statute and key state analogues, as well as the recent judicial decisions evaluating them, this Article argues that these laws should be upheld under rational basis or, at most, intermediate scrutiny. Far from threatening press freedom, judicial privacy legislation represents a narrowly tailored response to a modern threat to judicial independence in the data economy.

† Practicing Faculty, St. Mary's University School of Law; Past President, Virgin Islands Bar Association; Special Assistant to Hon. Rhys S. Hodge, Chief Justice of the Virgin Islands. The views expressed herein are solely my own and not those of the Judicial Branch of the Virgin Islands, the Virgin Islands Bar Association, or any of their officers or employees.

Table of Contents

I. Introduction

On July 19, 2020, a gunman impersonating a delivery driver arrived at the home of Esther Salas, a judge of the United States District Court for the District of New Jersey, murdered her twenty-year-old son, Daniel Anderl, and critically wounded her husband, Mark Anderl.[1] The gunman—a self-described "men's rights lawyer"—had apparently targeted Judge Salas for her decisions in a case he had brought challenging the all-male draft, and had plans to target other judges as well, including the Chief Judge of the New York Court of Appeals.[2] The shooter was able to obtain Judge Salas's home address and other personal information through publicly accessible online directories.[3]

The attack on Judge Salas's family is, unfortunately, one of the latest in a long line of instances in which judicial officers have been targeted at their homes. In 2015, a gunman shot Julie Kocurek, a judge

1. Debra Cassens Weiss, *Federal Judge's Son Killed, Her Lawyer Husband Wounded in Shooting at Their Home*, A.B.A. J. (July 20, 2020, at 10:35 ET), https://www.abajournal.com/news/article/federal-judges-son-is-killed-her-lawyer-husband-wounded-in-shooting-at-their-home [https://perma.cc/J8LF-A74N].
2. Debra Cassens Weiss, *Men's Rights Lawyer, Now Dead, is Suspect in Fatal Shooting at Federal Judge's Home*, A.B.A. J. (July 21, 2020, at 13:36 ET), https://www.abajournal.com/news/article/mens-rights-lawyer-now-dead-is-suspect-in-fatal-shooting-at-federal-judges-home [https://perma.cc/6RY4-4NPY].
3. Eric Levenson, *New Jersey Federal Judge Whose Son Was Killed Details His Last Words*, CNN, https://www.cnn.com/2020/08/03/us/federal-judge-esther-salas [https://perma.cc/HL7E-9G46 (staff-uploaded)] (last updated Aug. 3, 2020).

in Travis County, Texas, for presiding over his criminal trial.[4] In 2005, a dissatisfied litigant arrived at the home of Joan Lefkow, a judge of the United States District Court for the Northern District of Illinois, and fatally shot her husband and mother.[5] U.S. District Judge John Wood was assassinated in front of his home in 1979, as was U.S. District Judge Richard Daronco in 1988. Robert Vance, a judge of the U.S. Court of Appeals for the Eleventh Circuit, was assassinated by a mail bomb sent to his house.[6]

At the state level, Texas,[7] Illinois,[8] and New Jersey[9] responded to the attacks in their states by enacting legislation to provide current and former judges with such privacy protections.[10] Yet most jurisdictions still lack such legislation. Not surprisingly, an informal survey conducted by the National Judicial College reported that the vast majority of judges fear for their safety and believe more should be done to protect themselves and their families at home.[11]

Despite these attacks, the attempts at state-level legislation, as well as literally thousands of threats against judges nationwide,[12] Congress hesitated to enact national legislation to protect the home addresses or other personal contact or identifying information of current or

---

4. *Man Who Shot Judge Kocurek Sentenced to Life in Prison*, KXAN, https://www.kxan.com/news/local/austin/man-who-shot-judge-kocurek-sentenced-to-life-in-prison/ [https://perma.cc/8FTQ-U2PK (staff-uploaded] (last updated Oct. 3, 2018).

5. Matt Reynolds, *An Attack on a Judge's Family is Putting Judicial Security Center Stage*, A.B.A. J. (Oct. 1, 2020), https://www.abajournal.com/web/article/attack-on-judges-family-puts-judicial-security-center-stage [https://perma.cc/L4HW-H7H7 (staff-uploaded)].

6. *Id.*

7. *See* Judge Julie Kocurek Judicial and Courthouse Security Act of 2017, 2017 Tex. Gen. Laws 356–63.

8. *See* Judicial Privacy Act of 2012, 705 Ill. Comp. Stat. Ann. 90/1-1 to 90/4-99 (2012).

9. *See* Daniel's Law, N.J. Stat. Ann. § 56:8–166.1 (West 2019); *see also Gov. Murphy Signs Daniel's Law After Son of Judge Esther Salas Killed in Home Ambush*, CBS N.Y. (Nov. 20, 2020, at 18:10 ET), https://newyork.cbslocal.com/2020/11/20/daniels-law-ester-salas-daniel-anderl-phil-murphy-new-jersey/ [https://perma.cc/59FK-XB6K] (providing details on the passage of Daniel's Law).

10. Reynolds, *supra* note 5.

11. *Id.*

12. *Id.*

former judges from public disclosure. The Judicial Conference of the United States held an emergency meeting after the attack on Judge Salas's home, and on August 14, 2020, approved a measure requesting that Congress adopt legislation to, among other things, enhance the protection of judges' personally identifiable information, as well as monitor the public availability of such information.[13] On September 24, 2020, a bipartisan group of representatives and senators introduced the Daniel Anderl Judicial Security and Privacy Act of 2020 in both houses of Congress, which, if enacted, would implement the recommendations of the Judicial Conference.[14] However, no hearing was ever held on either bill, and it ultimately died upon the adjournment of the 116th Congress when the U.S. Senate did not pass it by unanimous consent.[15]

It would take more than two years for Congress to eventually pass the federal Anderl Act, which only passed the Senate in the 117th Congress after its sponsors attached it to the annual defense authorization bill.[16] Then-Director of the Administrative Office of United States Courts, Judge Roslynn R. Mauskopf, hailed the legislation as an "important step to protect federal judges and their families," and as one that preserves democracy, which "depends on judges who are free to make decisions without fear of reprisal or retribution."[17]

The federal Anderl Act, however, was certainly not met with universal acclaim. As one might expect, the Reporters Committee for Freedom of the Press noted the potential chilling effects on journalists

13. *Judicial Conference Approves Measures to Increase Security for Federal Judges*, U.S. CTS. (Aug. 14, 2020), https://www.uscourts.gov/news/2020/08/14/judicial-conference-approves-measures-increase-security-federal-judges [https://perma.cc/P8XN-SHVE].

14. *See* S. Res. 4711, 116th Cong. (2020); H.R. Res. 8591, 116th Cong. (2020).

15. *See Important Updates for FJA Members Re: the Daniel Anderl Judicial Security and Privacy Act 2020*, FED. JUDGES ASS'N, (Dec. 18, 2020), https://federaljudgesassoc.org/important-updates-for-fja-members-re-the-daniel-anderl-judicial-security-and-privacy-act-2020/ [https://perma.cc/M2XW-DALZ].

16. *Congress Passes the Daniel Anderl Judicial Security and Privacy Act*, U.S. CTS. (Dec. 16, 2022), https://www.uscourts.gov/data-news/judiciary-news/2022/12/16/congress-passes-daniel-anderl-judicial-security-and-privacy-act [https://perma.cc/73JZ-9H9Y].

17. *Id.*

who cover the federal courts.[18] Thomas A. Berry, the Director of the Robert A. Levy Center for Constitutional Studies at the libertarian-leaning Cato Institute, recognized the measure as "well-intentioned," yet characterized the federal act as well as the various state-level acts that mirror it as unconstitutional under the First Amendment to the United States Constitution.[19]

Such concerns, however, are not limited only to trade groups or free speech absolutists. The progressively-aligned advocacy group, Fix the Court, perhaps most well-known for lobbying for term limits and "new and robust ethics rules" for U.S. Supreme Court Justices,[20] asserted that portions of the federal Anderl Act "are so broadly drawn" that "it would preclude certain reporting on potential bad actors in the judiciary" and at worst "open a reporter or a watchdog organization to civil liability for alerting the public" or at a minimum "encourage self-censorship by media companies and nonprofits."[21]

In the three years since passage of the federal Anderl Act, the Administrative Office of the United States Courts has aided federal judges in obtaining its protections. For instance, the Administrative Office has partnered with DeleteMe, "a third-party data broker monitoring and removal service" to "assist judges with the removal of covered information under the Daniel Anderl Act."[22] To date, however, there have been no publicized lawsuits or other enforcement actions taken under the federal Anderl Act.

---

18. Grayson Clary, *Bill to Conceal Judges' Personal Information Raises First Amendment Concerns*, REPS. COMM. FOR FREEDOM OF THE PRESS (Oct. 20, 2022), https://www.rcfp.org/judicial-security-first-amendment [https://perma.cc/JDL7-DY9W].

19. Thomas Berry, Opinion, *Government Can't Censor the Truth About Judges*, WALL ST. J. (Dec. 26, 2021), https://www.wsj.com/opinion/government-cant-censor-the-truth-about-judges-legislation-law-free-speech-adresses-phone-numbers-11640533446 [https://perma.cc/9T4E-G8W6 (staff-uploaded, dark archive)].

20. *About Us*, FIX THE CT., https://fixthecourt.com/about-us/ [https://perma.cc/2HFG-MCK7] (last visited Jan. 24, 2026).

21. *Beware a "Judicial Security" Bill that Flouts the First Amendment*, FIX THE CT. (Nov. 12, 2020), https://fixthecourt.com/2020/11/beware-judicial-security-bill-flouts-first-amendment/ [https://perma.cc/C4RU-WU5L].

22. Paul Gamble, *Memorandum to All United States Judges*, ADMIN. OFF. CTS. 2 (Apr. 20, 2023), https://ncbj.org/wp-content/uploads/2024/08/Daniel-Anderl-Judicial-Security-and-Privacy-Act-removal-of-PII.pdf [https://perma.cc/9Q72-Q5ET].

Yet the same cannot be said for the state-level Anderl Acts. In Judge Salas's home state of New Jersey, where the Governor signed "Daniel's Law" nearly four months to the day of the murder, a flurry of lawsuits—as many as 100 in one month alone—have been filed in New Jersey state courts under the law.[23] Many of these lawsuits, however, were often not brought by judges or other persons covered by Daniel's Law, but "by 'assignees' of covered persons" who "allege that the defendants failed to comply with take-down requests" under the law and seek relief "for hundreds of thousands of violations" for "thousands of covered persons."[24] Notably, such lawsuits were spurred not by the original Daniel's Law, but later-enacted amendments that expressly permitted assignment of claims.[25] Similar lawsuits were brought in West Virginia, where a retired law enforcement officer brought class action lawsuits against several data brokers that allegedly continued to publish addresses and phone numbers of thousands of covered persons.[26]

The flurry of lawsuits filed under the New Jersey and West Virginia state-level Anderl Acts has resulted in inconsistent adjudications. In June 2025, the New Jersey Supreme Court expressly rejected a journalist's First Amendment challenge to the state's Daniel's Law on grounds that it did not constitute a prior restraint on speech and "as written is narrowly tailored to achieve the state interest of the highest order: protection of certain public officials from harm and the threat of harm so that they can perform their public duties without fear of reprisal."[27] Yet, two months later, in September 2025, a judge of the United States District Court for the Northern District of West

23. *See Daniel's Law and the Explosion of Privacy Claims Impacting Real Estate and Tech Platforms*, THOMPSON HINE (Mar. 12, 2024), https://www.thompsonhine.com/insights/daniels-law-and-the-explosion-of-privacy-claims-impacting-real-estate-and-tech-platforms/ [https://perma.cc/N4SU-DDY7].

24. *Id*.

25. *See Amended Daniel's Law Sparks Litigation and Business Implications*, MORGAN LEWIS (Oct. 25, 2024), https://www.thompsonhine.com/insights/daniels-law-and-the-explosion-of-privacy-claims-impacting-real-estate-and-tech-platforms/ [https://perma.cc/Z27Q-3MVY].

26. *See* Suzanne Smalley, *West Virginia Law Enforcement Sues Data Broker for Publishing Personal Information Online*, RECORD (Sep. 6, 2024), https://therecord.media/west-virginia-law-enforcement-sues-broker [https://perma.cc/E9AS-35KV].

27. Kratovil v. City of New Brunswick, 336 A.3d 201, 218 (N.J. 2025).

Virginia declared portions of that state's Daniel's Law unconstitutional under the First Amendment, concluding that they "cannot survive strict scrutiny because it is not narrowly tailored" and "far from the least restrictive means of achieving West Virginia's undeniably compelling interest in protecting its public servants from harassment and violence."[28] Unlike the New Jersey lawsuit, the West Virginia case arose in the context of a class action seeking monetary damages on behalf of "thousands of . . . judicial and law enforcement officers whose information is displayed on defendants' 'people search' websites."[29]

This Article posits that the federal- and state-level Anderl Acts are constitutional under the First Amendment, at least when properly understood. These laws do not impose novel restrictions on speech but rather regulate the commercial dissemination of highly sensitive personal data—something which numerous other federal and state laws already do. They do not suppress public scrutiny of judges and their decisions, restrict reporting on matters of public concern, or impose any prior restraints. The very recent split between the Supreme Court of New Jersey and the U.S. District Court for the Northern District of West Virginia does not necessarily reflect different views on the constitutional questions but rather illustrates this misunderstanding and confusion.

II. Federal- and State-Level Daniel Anderl Acts

What, exactly, do these Anderl Acts do? While their opponents have asserted a line of evils, such as a purported chilling effect on journalists, these fears are entirely unfounded and rest on a fundamental misunderstanding of what federal- and state-level Anderl Acts regulate. Properly understood, they do not prohibit speech but instead regulate the dissemination of certain narrowly-defined categories of personal information by commercial data brokers—in the same manner other federal and state laws have done for decades.

28. Jackson v. Whitepages, Inc., 798 F. Supp. 3d 583, 611 (N.D.W. Va. 2025).
29. *Id.* at 587.

A. The Federal Act

The federal Anderl Act, adopted as part of Public Law 117-263 but not yet codified in the United States Code,[30] is a surprisingly simple piece of legislation given its scope and purpose. At its core, the federal Anderl Act prohibits "government agencies" and "data brokers" from disseminating "covered information" about an "at-risk individual." The Act defines an "at-risk individual" as

> (A) a Federal judge;
>
> (B) a senior, recalled, or retired Federal judge;
>
> (C) any individual who is the spouse, parent, sibling, or child of an individual described in subparagraph (A) or (B);
>
> (D) any individual to whom an individual described in subparagraph (A) or (B) stands in loco parentis; or
>
> (E) any other individual living in the household of an individual described in subparagraph (A) or (B).[31]

"Covered information," meanwhile, refers to

> (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;

30. *See* Daniel Anderl Judicial Security and Privacy Act of 2022, Pub. L. No. 117–263, 136 Stat. 2395, 3458 (2022).

31. 136 Stat. at 3459–60.

> (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 or day care, schedules of attendance, or routes taken to or from the school or day care by an at-risk individual; or
>
> (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.[32]

However, it "does not include information regarding employment with a government agency."[33]

As noted above, the federal Anderl Act primarily places restrictions on government agencies and data brokers. Government agencies, with limited exceptions, possess an affirmative duty to "not publicly post or display publicly available content that includes covered information of an at-risk individual or immediate family member," and to remove any such information "not later than 72 hours" after "receipt of a written request" by the at-risk individual or assignee.[34] The government agency may still maintain the records, but must "mark as private their covered information" once it receives written notice.[35]

With respect to data brokers, the Act generally provides that "[i]t shall be unlawful for a data broker to knowingly sell, license, trade for consideration, transfer, or purchase covered information of an at-risk individual or immediate family members."[36] The Act defines "data broker" as "an entity that collects and sells or licenses to third parties the personal information of an individual with whom the entity does

---

32. 136 Stat. at 3460.
33. *Id.*
34. 136 Stat. at 3462.
35. *Id.*
36. 136 Stat. at 3464.

not have a direct relationship."[37] However, it also provides a long list of exclusions from this general definition:

> The term 'data broker' 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 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 . . . .
>
> (vi) A financial institution subject to the Gramm-Leach-Bliley Act . . . 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 . . . .

37. 136 Stat. at 3460.

> (viii) The collection and sale or licensing of covered information incidental to conducting the activities described in clauses (i) through (vii).[38]

Moreover, the general prohibition on the knowing sale, trade, and so forth of an at-risk individual's covered information by data brokers, shall 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 enactment of this Act; or
>
> (III) covered information lawfully received from a Federal Government source (or from an employee or agent of the Federal Government).[39]

Consistent with the requirement that the data broker act "knowingly,"[40] the Anderl Act imposes a notice-and-take-down regime in which, after receiving written notice from the at-risk individual or assignee, the data broker must "remove" the covered information "within 72 hours" and also "ensure that the information is not made available on any website or subsidiary website controlled by that person, business, or association and identify any other instances of the identified information that should also be removed."[41] In addition, the data broker cannot thereafter "transfer the covered information . . . to any other person, business, or association, through any medium."[42] That prohibition on subsequent transfers, however:

---

38. 136 Stat. at 3460–61.
39. 136 Stat. 3464–65.
40. 136 Stat. 3464.
41. 136 Stat. 3465.
42. *Id.*

shall not apply to-

> (I) the transfer of the covered information of the 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 or immediate family member voluntarily publishes on the internet after the date of enactment of this Act; or
>
> (III) a transfer made at the request of the at-risk individual or that is necessary to effectuate a request to the person, business, or association from the at-risk individual.[43]

Some aspects of the Anderl Act, however, do apply to "other persons and businesses" besides data brokers. Most notably, the Act provides that

> no person, business, or association shall 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 to that person, business, or association not to disclose or acquire the covered information of the at-risk individual or immediate family member.[44]

But like other prohibited conduct, the Act provides for broad exclusions. In this case, the prohibition

> shall 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,

43. *Id.*
44. 136 Stat. 3464.

> 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 enactment of this Act; or
>
> (III) covered information lawfully received from a Federal Government source (or from an employee or agent of the Federal Government).[45]

Moreover, the rules of construction for the Act specify that

> [n]othing in this subtitle shall be construed-
>
> (1) to prohibit, restrain, or limit-
>
> (A) 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
>
> (B) the reporting on an at-risk individual or their immediate family member regarding matters of public concern;
>
> (2) to impair access to decisions and opinions from a Federal judge in the course of carrying out their public functions;
>
> (3) to limit the publication or transfer of covered information with the written consent of the at-risk individual or their immediate family member; or
>
> (4) to prohibit information sharing by a data broker to a Federal, State, Tribal, or local government, or any unit thereof.[46]

45. 136 Stat. 3464–65.
46. 136 Stat. at 3468–69.

The Anderl Act further provides for scaling remedies for violations. However, it does not provide for a private right of action—rather, actions may only be brought by the Director of the Administrative Office of the United States Courts (or the Director's designee) or, for certain Article I courts, the chief judge of the court.[47] If covered information is made public in violation of the Act, the Director or chief judge "may file an action seeking injunctive or declaratory relief in any court of competent jurisdiction, through the Department of Justice."[48] However, if the defendant "knowingly violates an order granting injunctive or declarative relief," the court may at that point award damages in "an amount equal to the actual damages sustained by the at-risk individual or their immediate family" (or, if the defendant is a government agency, "a fine not greater than $4,000") as well as "court costs and reasonable attorney's fees."[49]

B. State-Level Acts

As indicated earlier, several states have enacted laws similar to the federal Anderl Act. However, in the interests of brevity, this Article will examine the two state-level Anderl Acts that resulted in judicial opinions scrutinizing them under the First Amendment: the state-level Anderl Acts passed by New Jersey and West Virginia, both titled "Daniel's Law."

1. The New Jersey Daniel's Law

New Jersey passed its Daniel's Law nearly four months to the date of Daniel Anderl's murder, more than two years before Congress enacted the federal Anderl Act. The legislation enacted by New Jersey bears the general structure of the federal Anderl Act, but with several significant differences. Perhaps most notably, a "covered person" under the New Jersey Act is not limited only to judges and their families, but

> [m]eans an active, formerly active, or retired judicial officer, law enforcement officer, or child protective investigator in the Division of Child Protection and Permanency . . . or prosecutor and any immediate

47. 136 Stat. at 3466.
48. *Id.*
49. *Id.*

> family member residing in the same household as such judicial officer, law enforcement officer, child protective investigator in the Division of Child Protection and Permanency, or prosecutor.[50]

Yet while the definition of "covered person" is exceptionally broader, the information that may not be disclosed is limited only to "the home address or unpublished home telephone number of any covered person."[51] This prohibition, however, extends to any "person, business, or association" and not just data brokers like the federal Anderl Act.[52]

And like the federal law, the New Jersey Daniel's Law establishes a notice-and-take-down regime where a covered person (or someone acting with the covered person's authorization) "shall provide written notice" which requests "that the person cease the disclosure of the information and remove the protected information from the Internet or where otherwise made available," within the person needing to do so within 10 business days.[53] Importantly, "Daniel's Law imposes no obligation on a person in possession of the covered person's home address or unpublished home telephone number who has not received the notice that the statute requires."[54] And like the federal Anderl Act, it contains several exceptions, including one for the news media.[55]

But New Jersey's Daniel's Law differs from the federal law both in terms of who can seek redress under the law and what remedies a court can provide. While the federal Anderl Act authorizes only the U.S. Department of Justice to bring an enforcement action at the request of the Director of the Administrative Office of the United States Court or certain Article I chief judges, Daniel's Law authorizes "the covered person or the covered person's assignee" to "bring a civil action in the Superior Court."[56] In addition to allowing a private right of

---

50. N.J. STAT. ANN. § 56:8-166.1(d) (West 2023).
51. *Id.* § 56:8-166.1(a)(1).
52. *Id.*
53. *Id.* § 56:8-166.1(a)(1)–(2).
54. Kratovil v. City of New Brunswick, 336 A.3d 201, 209 (N.J. 2025).
55. N.J. STAT. ANN. § 56:8-166.1(e)–(f) (West 2023).
56. *Id.* § 56:8-166.1(b).

action, the New Jersey Daniel's Law does not provide for a sliding scale remedy, instead:

> The court shall award:
>
> (1) actual damages, but not less than liquidated damages computed at the rate of $1,000 for each violation of this act;
>
> (2) punitive damages upon proof of willful or reckless disregard of the law;
>
> (3) reasonable attorney's fees and other litigation costs reasonably incurred; and
>
> (4) any other preliminary and equitable relief as the court determines to be appropriate.[57]

Considering the breadth of these private remedies for a cause of action that appears relatively easy to prove, it should perhaps come as no surprise that hundreds of lawsuits have been filed in New Jersey courts under Daniel's Law.[58]

2. The West Virginia Daniel's Law

The West Virginia Daniel's Law bears some similarities to the New Jersey Daniel's Law. Like New Jersey, West Virginia prohibits disclosure only of home addresses and unpublished telephone numbers and has broadened protection beyond judges to also include prosecutors, public defenders, law enforcement officers, and certain immediate family members and those residing with them.[59] And like New Jersey's Daniel's Law, these individuals may bring a private civil action to enforce their rights under the statute.[60]

But the West Virginia Daniel's Law differs in one very significant aspect: it establishes two different types of causes of action. The first cause of action may be brought against "a person, business, or association" that discloses the address and phone number, but only if

57. *Id.* § 56:8-166.1(c).
58. *See Daniel's Law and the Explosion of Privacy Claims*, *supra* note 23.
59. *See* W. VA. CODE § 5A-8-24 (2021).
60. *Id.*

the disclosure is made "under circumstances in which a reasonable person would believe that providing such information would expose another to harassment or risk of harm to life or property."[61] In such a civil action

> [t]he court may award:
>
> > (A) Actual damages, but not less than $1,000, for each violation of this act;
> >
> > (B) Punitive damages, if applicable . . .
> >
> > (C) Reasonable attorney's fees and other litigation costs reasonably incurred; and
> >
> > (D) Any other preliminary or equitable relief as the court deems appropriate.[62]

Significantly, this portion of the West Virginia Daniel's Law does not create a notice-and-takedown system and does not require that the defendant receive notice and an opportunity to remove the information prior to liability attaching.[63]

The second cause of action created by the West Virginia Daniel's Law does, however, greatly resemble the New Jersey Daniel's Law. Judges and other covered individuals "may request," "in writing," "that the person, business, or association" that has distributed their address or phone number "refrain from that action and remove the information."[64] If the person, business, or association does not do so, "[a] civil action may be maintained" in which "the court may award injunctive or declaratory relief" and, if it does so, "the person, business, or association responsible for the violation shall be required to pay reasonable attorney's fees and other litigation costs reasonably incurred . . . as applicable and appropriate."[65] But unlike the federal Anderl Act and the New Jersey Daniel's Law, the West Virginia

61. *Id.* § 5A-8-24(e) & (e)(1).
62. *Id.* § 5A-8-24(e)(2).
63. Jackson v. Whitepages, Inc., 798 F. Supp. 3d 583, 589 (N.D.W. Va. 2025).
64. W. VA. CODE § 5A-8-24(f)–(h) (2021).
65. *Id.* § 5A-8-24(h)(1)–(2).

Daniel's Law also provides a criminal penalty, in the form of up to a $1,000 fine and six months' incarceration, for "[a] person who willfully refuses to remove information within 24 hours of receipt of the written request."[66]

III. Unwarranted First Amendment Scrutiny

The federal Anderl Act, as well as the New Jersey and West Virginia Daniel's Laws, have had their constitutionality questioned, with a federal court even declaring portions of the West Virginia Daniel's Law unconstitutional as violative of the First Amendment. As noted above, none of these Acts impose any prior restraints. The primary argument, therefore, is that these laws regulate speech, impose content-based regulations, and cannot survive strict scrutiny under the First Amendment.

These concerns, however, are unfounded and are ultimately based on fundamental misunderstandings of the laws. Perhaps the most natural way to frame this analysis is through the lens of the opinion of the United States District Court for the Northern District of West Virginia in *Jackson v. Whitepages, Inc.*,[67] where it held Section E of the West Virginia Daniel's Law unconstitutional.[68] That portion of the statute provides that

> [u]nless written permission is first obtained from the individual, a person, business, or association shall not disclose, redisclose, or otherwise make available the home address or unpublished home or personal telephone number of any active, formerly active, or retired judicial officer, prosecutor, federal or state public defender, federal or state assistant public defender, or law-enforcement officer under circumstances in which a reasonable person would believe that providing such information would expose

66. *Id.* § 5A-8-24(h)(3).
67. 798 F. Supp. 3d 583 (N.D.W. Va. 2025).
68. *Id.* at 611.

> another to harassment or risk of harm to life or property.[69]

The *Jackson* court found this provision unconstitutional under the First Amendment after concluding that it (1) regulated speech; (2) was subject to strict scrutiny review because it regulated speech; and (3) did not satisfy strict scrutiny review because it lacked a notice of requirement.[70]

"Precisely what constitutes speech, and how to approach the delicate balance involved in weighing incursions on purported speech . . . are questions that continue to provoke contentious debate."[71] In holding that Section E of the West Virginia Daniel's Law regulated speech, the district court in *Jackson* relied heavily on the decision of the Supreme Court of the United States in *Sorrell v. IMS Health, Inc.*,[72] where, according to the district court, it "concluded that a Vermont law that banned the sale, transmission, or use of prescriber-identifiable data for marketing or promoting a prescription drug without the consent of the prescriber was an unconstitutional regulation of speech."[73] Relying on several lower court decisions addressing publication of home addresses, dates of birth, Social Security numbers, and the like, the district court declared that "there is no doubt that West Virginia's Daniel's Law regulates speech."[74]

The *Jackson* court greatly misread the Supreme Court's holding in *Sorrell*. Simply put, nothing in *Sorrell* stands for the proposition that aggregated personal data—standing alone—constitutes speech. Significantly, the Supreme Court in *Sorrell* found that the Vermont law only burdened speech to the extent that it imposed "content-and speaker-based restrictions on the sale, disclosure, and use of

---

69. W. Va. Code § 5A-8-24(e) (2021).

70. *Jackson*, 798 F. Supp. 3d at 611.

71. Wayne Batchis, *Reconciling Campaign Finance Reform with the First Amendment: Looking Both Inside and Outside America's Borders*, 25 QUINNIPIAC L. REV. 27, 42 (2006).

72. 564 U.S. 552 (2011).

73. *Jackson*, 798 F. Supp. 3d at 594 (citing *Sorrell*, 564 U.S. at 570–71, 580).

74. *Id.* at 595.

prescriber-identifying information."[75] The Supreme Court characterized the Vermont law:

> The provision first forbids sale subject to exceptions based in large part on the content of a purchaser's speech. For example, those who wish to engage in certain "educational communications," may purchase the information. The measure then bars any disclosure when recipient speakers will use the information for marketing. Finally, the provision's second sentence prohibits pharmaceutical manufacturers from using the information for marketing. The statute thus disfavors marketing, that is, speech with a particular content. More than that, the statute disfavors specific speakers, namely pharmaceutical manufacturers. As a result of these content- and speaker-based rules, detailers cannot obtain prescriber-identifying information, even though the information may be purchased or acquired by other speakers with diverse purposes and viewpoints. Detailers are likewise barred from using the information for marketing, even though the information may be used by a wide range of other speakers. For example, it appears that Vermont could supply academic organizations with prescriber-identifying information to use in countering the messages of brand-name pharmaceutical manufacturers and in promoting the prescription of generic drugs. But [the statute] leaves detailers no means of purchasing, acquiring, or using prescriber-identifying information. The law on its face burdens disfavored speech by disfavored speakers.[76]

In other words, it was not the prescriber-identifying information itself that constituted speech, but rather the transformative use of that data by a speaker to create a message, i.e. marketing communications, that received First Amendment protection.

---

75. *Sorrell*, 564 U.S. at 564–65 (emphasis added).
76. *Id.* at 565.

This, of course, is a stark contrast from the West Virginia Daniel's Law, as well as the federal Anderl Act and the New Jersey Daniel's Law. While some provisions of the federal Anderl Act are directed to data brokers, the general prohibition on the sale, transfer, and so forth of home addresses and unpublished phone numbers of judges and other covered individuals applies to everyone and does so regardless of the message (if any) being conveyed.

Moreover, in the specific case of Section E of the West Virginia Daniel's Law, the prohibition is even narrower: it applies only to disclosures "under circumstances in which a reasonable person would believe that providing such information would expose another to harassment or risk of harm to life or property."[77] This, of course, is a well-established exception to the First Amendment, and can give rise to criminal punishment and not just civil liability. As the United States Court of Appeals for the Ninth Circuit aptly explained

> [t]he first amendment does not provide a defense to a criminal charge simply because the actor uses words to carry out his illegal purpose. Crimes, including that of aiding and abetting, frequently involve the use of speech as part of the criminal transaction. The use of a printed message to a bank teller requesting money coupled with a threat of violence, the placing of a false representation in a written contract, the forging of a check, and the false statement to a government official, are all familiar acts which constitute crimes despite the use of speech as an instrumentality for the commission thereof.[78]

And harassment, of course, has long been considered unprotected by the First Amendment in that it is the conduct—and not the spoken words—which has been made unlawful.[79]

This same principle applies, of course, to aiding and abetting a crime committed by someone else. For instance, the authors of books

---

77. W. VA. CODE § 5A-8-24(e) (2021).

78. United States v. Barnett, 667 F.2d 835, 842 (9th Cir. 1982).

79. *See, e.g.*, Scott v. State, 322 S.W.3d 662, 668–69 (Tex. Crim. App. 2010).

on how to make illegal drugs,[80] commit tax fraud,[81] or hire a hit man[82] have all been held criminally or civilly liable notwithstanding the First Amendment because, despite the use of words, they are "directed to inciting or producing imminent lawless action and . . . likely to incite or produce such action."[83] In other words, it is ultimately not the "content" of the speech that the state disfavors, but rather the "secondary effects."[84]

It is inconceivable that a statute like Section E of the West Virginia Daniel's Law that imposes civil liability on person who disseminates a judge's home address or phone number—again, "under circumstances in which a reasonable person would believe that providing such information would expose another to harassment or risk of harm to life or property"[85]—should not be constitutional for the same reasons. While an address or phone number contains words and/or numbers, the dissemination of this "content" is unlawful "not because the State disagrees with that content, but because [it] is more likely to lead to violent secondary effects."[86]

Because the federal- and state-level Anderl Acts do not regulate speech and "are minimally burdensome and nondiscriminatory," courts should construe them only under rational basis review[87] or—at the very worst—under intermediate scrutiny.[88] Yet regardless of the standard employed, the governmental interest is one of the highest order: "protecting judges, prosecutors, and other law enforcement officers from threats and assassinations."[89] The laws were not enacted as a pretext, but were "based on a very real set of facts": "the attempted assassination of Judge Salas, the murder of her son, and the wounding

80. *Barnett*, 667 F.2d at 843.
81. United States v. Buttorff, 572 F.2d 619, 625 (8th Cir. 1978).
82. Rice v. Paladin Enters., Inc., 128 F.3d 233, 249 (4th Cir. 1997).
83. Brandenburg v. Ohio, 395 U.S. 444, 447 (1969).
84. City of Renton v. Playtime Theatres, Inc., 475 U.S. 41, 47 (1986).
85. W. VA. CODE § 5A-8-24(e) (2021).
86. *Ex parte* Flores, 483 S.W.3d 632, 641 (Tex. App. 2015).
87. *See* Ohio Council 8 Am. Fed. of State v. Husted, 814 F.3d 329, 335 (6th Cir. 2016).
88. *See Renton*, 475 U.S. at 47–48.
89. Atlas Data Priv. Corp. v. We Inform, LLC, 758 F. Supp. 3d 322, 337 (D.N.J. 2024).

of her husband, all of which resulted after an assailant obtained her home address through the Internet."[90] It is so obvious to not require citation that physical violence inherently threatens judicial independence and ultimately undermines democracy, as seen—for instance—"in Latin America, where you see judges living in fear of threats from mobs and drug cartels."[91]

Finally, it is worth noting that the district court in *Jackson* ultimately based the decision to strike down Section E of the West Virginia Daniel's Law "due to its lack of a notice requirement."[92] This, of course, was done in the context of a strict scrutiny analysis[93]—which, as explained in the prior paragraph, was a much higher standard of review than the court should have applied. Nevertheless, applying the demanding strict scrutiny standard, the *Jackson* court found Section E not narrowly tailored because it was purportedly more restrictive than both the New Jersey Daniel's Law and the federal Anderl Act, which utilized a notice-and-take-down regime.[94]

This holding, however, is based on another misunderstanding of the West Virginia Daniel's Law: The failure to recognize that it codifies two *separate* causes of action. As explained earlier, Section E does not utilize a notice-and-takedown regime but instead attaches liability when the pertinent information is disseminated "under circumstances in which a reasonable person would believe that providing such information would expose another to harassment or risk of harm to life or property."[95] This, by its nature, *is* a notice requirement—the person either knows (actual knowledge) or should know (under a reasonable person standard) "that providing such information would expose another to harassment or risk of harm to life or property."[96]

Importantly, Section E has no analogue in the New Jersey Daniel's Law or the federal Anderl Act; rather, it is Section F of the West Virginia Daniel's Law that models those statutes and establishes a

---

90. *Id.* at 338.

91. David F. Levi et al., *Judicial Independence Under Attack*, 105 JUDICATURE 10, 19 (2021) (statement of Allyson Duncan).

92. *Jackson*, 798 F. Supp. 3d at 609.

93. *Id.*

94. *Id.* at 608–10.

95. W. VA. CODE § 5A-8-24(e) (2021).

96. *Id.*

notice-and-takedown regime with liability attaching if one fails to comply after receiving notice.[97] In other words, West Virginia deliberately chose to distinguish between those who distribute covered information unknowingly or without risk of potential harm, who must receive notice and are only held liable if they choose to ignore it, and those who do so with actual or constructive knowledge that their conduct may result in harassment or risk of harm to life or property. It is unclear why the fact that Congress and the New Jersey Legislature—both of whom passed their laws before West Virginia—chose to treat one who intentionally disseminates covered information with the intent to harm a judge the same as a mere innocent distributor should, in any way, limit the authority of West Virginia to improve on the legislation.

IV. Conclusion

The murder of Daniel Anderl and the long history of violence directed at judges outside the courtroom underscores a reality that the law can no longer afford to ignore. In the modern data economy, publicly available home addresses and telephone information serve as a direct conduit to physical harm. The federal- and state-level Anderl Acts represent a measured legislative response to that reality. Properly understood, they do not silence speech, shield judges from criticism, or erode the transparency essential to democratic accountability. Instead, they regulate the (largely commercial) dissemination of narrowly defined categories of sensitive personal data—data whose primary contemporary function is not to inform public debate, but to facilitate targeting.

Much of the constitutional resistance to these statutes has rested on an initial misclassification. Treating the aggregation, sale, and redistribution of judges' home addresses and unpublished contact information as core expressive activity distorts the First Amendment and invites the application of heightened scrutiny where it does not belong. As this Article has shown, neither the federal Anderl Act nor its state counterparts impose prior restraints, discriminate based on viewpoints, or restrict reporting on matters of public concern. They operate in a doctrinal space long occupied by other federal and state

97. *Id.* § 5A-8-24(f).

statutes that regulate the commercial use of personal data in service of compelling governmental interests, such as the Health Insurance Portability and Accountability Act ("HIPAA"),[98] the Family Educational Rights and Privacy Act ("FERPA"),[99] and the Video Privacy Protection Act ('VPRA").[100]

The recent divergence between courts upholding and invalidating state-level Anderl Acts does not reflect an intractable constitutional conflict. Rather, it reflects differing understandings of what these laws regulate and why. When courts focus on the secondary effects of unrestricted data dissemination—rather than on the mere presence of words or numbers—the constitutional analysis becomes considerably more straightforward. Protecting judges from foreseeable threats of violence is not only a legitimate governmental objective; it is a prerequisite for judicial independence and, by extension, for the rule of law itself.

Anderl Acts or Daniel's Laws are not a panacea, nor do they purport to resolve broader debates about data privacy in the digital age. They are instead a narrow, targeted intervention aimed at specific and well-documented harm. In recognizing the constitutionality of such measures, courts need not diminish the First Amendment. They need only to acknowledge that the Constitution does not require the law to remain static and legislatures indifferent when personal data is transformed into a literal weapon to silence "the guardians of humanity's most audacious attempts to achieve true justice"—the judges who ensure our government remains a democracy.[101]

---

98. Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

99. 20 U.S.C. § 1232 (2025).

100. 18 U.S.C. § 2710 (2025).

101. UBS Fin. Servs., Inc. v. Asociacion de Empleados del Estate Libre Asociado de P.R., 419 F. Supp. 3d 266, 287 (D. Mass. 2019).