

Nos. 25-1555 through 25-1578; 25-1580 through 25-1593; 25-1676;
and 25-1677 (Consolidated)

**IN THE UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT**

ATLAS DATA PRIVACY CORP., *et al.*,
Plaintiffs-Appellees,

MATTHEW J. PLATKIN, in his official capacity as
ATTORNEY GENERAL OF NEW JERSEY,
Intervenor-Appellee.

v.

WE INFORM LLC, *et al.*,
Defendants-Appellants.

On Appeal from the United States District Court for the
District of New Jersey (No. 1:24-cv-4037-HB)

BRIEF OF INTERVENOR-APPELLEE ATTORNEY GENERAL OF NEW JERSEY

MATTHEW J. PLATKIN
Attorney General of New Jersey

JEREMY M. FEIGENBAUM
Solicitor General

MICHAEL L. ZUCKERMAN
Deputy Solicitor General

LIZA B. FLEMING
KASHIF T. CHAND
JOSHUA P. BOHN
PATRICK MISALE
ZACHARY ABOFF
Deputy Attorneys General

Office of the New Jersey Attorney General
R.J. Hughes Justice Complex
25 Market Street, P.O. Box 080
Trenton, NJ 08625
(609) 789-8684
Michael.Zuckerman@njoag.gov
Attorneys for Intervenor-Appellee

TABLE OF CONTENTS

INTRODUCTION	1
STATEMENT OF THE ISSUE.....	3
STATEMENT OF RELATED CASES	3
STATEMENT OF THE CASE.....	4
A. The Right To Privacy And Safety In The Home.	4
B. Growing Threats To Public Servants.	7
C. Daniel’s Law.	9
D. This Litigation.	11
SUMMARY OF ARGUMENT	13
STANDARD OF REVIEW	16
ARGUMENT	16
I. In Seeking Facial Relief, Appellants Face A High Bar.....	16
II. This Facial Challenge Implicates Less-Than-Strict Scrutiny.....	19
A. The Longstanding Coexistence Of Domestic-Privacy Laws And The First Amendment Supports Reduced Scrutiny.....	19
B. Most Applications Impact Only Commercial Speech.....	29
C. Daniel’s Law Is Content Neutral.....	33
III. Daniel’s Law Satisfies Facial Scrutiny.....	35
A. Daniel’s Law Satisfies Facial Scrutiny Under <i>Florida Star</i>	35
B. For Similar Reasons, Daniel’s Law Satisfies Facial Intermediate Scrutiny, Whether Under <i>Central Hudson</i> Or The Standard Test.....	53
C. For Similar Reasons, Daniel’s Law Would Satisfy Even Strict Scrutiny.	55
IV. In The Alternative, Certification Is Appropriate.	55
CONCLUSION	56
COMBINED CERTIFICATIONS.....	57

TABLE OF AUTHORITIES

Cases

<i>Am. Future Sys. v. Penn State Univ.</i> , 752 F.2d 854 (3d Cir. 1984).....	33
<i>Ariix, LLC v. NutriSearch Corp.</i> , 985 F.3d 1107 (9th Cir. 2021)	30
<i>Ayotte v. Planned Parenthood of N. New Eng.</i> , 546 U.S. 320 (2006).....	49
<i>Bank of Hope v. Miye Chon</i> , 938 F.3d 389 (3d Cir. 2019).....	53
<i>Barasch v. Bell Tel. Co. of Pa.</i> , 605 A.2d 1198 (Pa. 1992).....	22
<i>Barr v. Am. Ass’n of Pol. Consultants, Inc.</i> , 591 U.S. 610 (2020).....	27, 49
<i>Bd. of Trustees of State Univ. of N.Y. v. Fox</i> , 492 U.S. 469 (1989).....	33, 54
<i>Boelter v. Advance Mag. Publishers Inc.</i> , 210 F. Supp. 3d 579 (S.D.N.Y. 2016)	18, 30
<i>Boelter v. Hearst Commc’ns, Inc.</i> , 192 F. Supp. 3d 427 (S.D.N.Y. 2016)	30
<i>Borough of Princeton v. Bd. of Chosen Freeholders</i> , 777 A.2d 19 (N.J. 2001).....	42
<i>Bowley v. City of Uniontown Police Dep’t</i> , 404 F.3d 783 (3d Cir. 2005).....	37
<i>Brayshaw v. City of Tallahassee</i> , 709 F. Supp. 2d 1244 (N.D. Fla. 2010)	26, 37, 38, 52
<i>Bruni v. City of Pittsburgh</i> , 824 F.3d 353 (3d Cir. 2016).....	17, 18

<i>Camp Hill Borough Republican Ass’n v. Borough of Camp Hill</i> , 101 F.4th 266 (3d Cir. 2024)	34, 35
<i>Central Hudson Gas & Electric Corp. v. Public Service Commission</i> , 447 U.S. 557 (1980).....	passim
<i>Children’s Health Def., Inc. v. Rutgers</i> , 93 F.4th 66, (3d Cir.)	16
<i>City of Austin v. Reagan Nat’l Advert. of Austin, LLC</i> , 596 U.S. 61 (2022).....	14, 30, 33, 34
<i>Counterman v. Colorado</i> , 600 U.S. 66 (2023).....	49
<i>Cox Broad. Corp. v. Cohn</i> , 420 U.S. 469 (1975).....	36, 37, 38
<i>Dahlstrom v. Sun-Times Media, LLC</i> , 777 F.3d 937 (7th Cir. 2015)	6, 24, 35
<i>Davenport v. Wash. Educ. Ass’n</i> , 551 U.S. 177 (2007).....	14, 20, 23, 34
<i>De May v. Roberts</i> , 9 N.W. 146 (Mich. 1881).....	4, 22
<i>Del. State Sportsmen’s Ass’n, Inc. v. Del. Dep’t of Safety & Homeland Sec.</i> , 108 F.4th 194 (3d Cir. 2024)	16
<i>Dex Media West, Inc. v. City of Seattle</i> , 696 F.3d 952 (9th Cir. 2012)	32
<i>Dirkes v. Borough of Runnemede</i> , 936 F. Supp. 235 (D.N.J. 1996)	22, 26
<i>Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.</i> , 472 U.S. 749 (1985).....	31
<i>Florida Star v. B.J.F.</i> , 491 U.S. 524 (1989).....	passim

<i>Fort Wayne Books, Inc. v. Indiana</i> , 489 U.S. 46 (1989).....	43
<i>Free Speech Coal., Inc. v. Att’y Gen.</i> , 974 F.3d 408 (3d Cir. 2020).....	43
<i>Friedman v. Martinez</i> , 231 A.3d 719 (N.J. 2020).....	4
<i>Frisby v. Schultz</i> , 487 U.S. 474 (1988).....	4, 22
<i>Greater Phila. Chamber of Com. v. City of Philadelphia</i> , 949 F.3d 116 (3d Cir. 2020).....	30, 31, 54
<i>Harris v. Quinn</i> , 573 U.S. 616, 648 (2014).....	31
<i>IMDb.com v. Becerra</i> , 962 F.3d 1111 (9th Cir. 2020)	32
<i>In re Nickelodeon Consumer Privacy Litig.</i> , 827 F.3d 262 (3d Cir. 2016).....	26
<i>Johnson v. NCAA</i> , 108 F.4th 163 (3d Cir. 2024)	16
<i>Kratovil v. City of New Brunswick</i> , No. A-0216-23, 2024 WL 1826867 (N.J. Super. Ct. App. Div. Apr. 26, 2024)	37
<i>Mainstream Mktg. Servs. v. FTC</i> , 358 F.3d 1228 (10th Cir. 2004)	22, 39, 50
<i>Martin v. City of Struthers</i> , 319 U.S. 141 (1943).....	40
<i>Mazo v. N.J. Sec’y of State</i> , 54 F.4th 124 (3d Cir. 2022)	18
<i>Melvin v. Reid</i> , 297 P. 91 (Cal. Ct. App. 1931)	4

<i>Moody v. NetChoice, LLC</i> , 603 U.S. 707 (2024).....	passim
<i>Nat’l Fed’n of the Blind v. FTC</i> , 420 F.3d 331 (4th Cir. 2005)	39
<i>N.J. Repub. State Comm. v. Murphy</i> , 236 A.3d 89 (N.J. 2020).....	44
<i>O’Donnell v. United States</i> , 891 F.2d 1079 (3d Cir. 1989).....	46
<i>Olmstead v. United States</i> , 277 U.S. 438 (1928).....	5
<i>Ostergren v. Cuccinelli</i> , 615 F.3d 263 (4th Cir. 2010)	passim
<i>Paul P. v. Farmer</i> , 227 F.3d 98 (3d Cir. 2000).....	25
<i>Pavesich v. New England Life Ins. Co.</i> , 50 S.E. 68 (Ga. 1905).....	4, 22
<i>Project Veritas v. Schmidt</i> , 125 F.4th 929 (9th Cir. 2025)	34
<i>Publius v. Boyer-Vine</i> , 237 F. Supp. 3d 997 (E.D. Cal. 2017)	52
<i>R.A.V. v. City of St. Paul</i> , 505 U.S. 377 (1992).....	15, 34, 35
<i>Reed v. Town of Gilbert</i> , 576 U.S. 155 (2015).....	55
<i>Romaine v. Kallinger</i> , 537 A.2d 284 (N.J. 1988).....	46, 47
<i>Rowan v. U.S. Post Off. Dep’t</i> , 397 U.S. 728 (1970).....	39

<i>Rubin v. Coors Brewing Co.</i> , 514 U.S. 476 (1995).....	53, 54
<i>S.F. Arts & Athletics, Inc. v. U.S. Olympic Comm.</i> , 483 U.S. 522 (1987).....	54
<i>Saunders v. Hearst Television, Inc.</i> , 711 F. Supp. 3d 24 (D. Mass. Jan. 11, 2024).....	30
<i>Schrader v. District Attorney of York County</i> , 74 F.4th 120 (3d Cir. 2023)	28, 43
<i>Sheehan v. Gregoire</i> , 272 F. Supp. 2d 1135 (W.D. Wash. 2003).....	26, 37, 38, 52
<i>Smith v. Daily Mail Publishing Co.</i> , 443 U.S. 97 (1979).....	28, 37
<i>Snyder v. Phelps</i> , 562 U.S. 443 (2011).....	28, 36, 38
<i>Sorrell v. IMS Health Inc.</i> , 564 U.S. 552 (2011).....	27, 50
<i>Stark v. Patreon, Inc.</i> , 656 F. Supp. 3d 101 (N.D. Cal. 2023)	passim
<i>State v. Burkert</i> , 174 A.3d 987 (N.J. 2017).....	44, 46
<i>State v. Carter</i> , 255 A.3d 1139 (N.J. 2021).....	44
<i>State v. Maldonado</i> , 645 A.2d 1165 (N.J. 1994).....	47
<i>State v. Mrozinski</i> , 971 N.W.2d 233 (Minn. 2022).....	9
<i>State v. Natale</i> , 878 A.2d 724 (N.J. 2005).....	44

<i>State v. Pomianek</i> , 110 A.3d 841 (N.J. 2014).....	47, 48
<i>State v. Ramirez</i> , 284 A.3d 839 (N.J. 2022).....	6
<i>State v. Taupier</i> , 193 A.3d 1 (Conn. 2018)	8
<i>Suter v. San Angelo Foundry & Mach. Co.</i> , 406 A.2d 140 (N.J. 1979).....	46
<i>Time, Inc. v. Firestone</i> , 424 U.S. 448 (1976).....	37
<i>Trans Union Corp. v. FTC</i> , 267 F.3d 1138 (D.C. Cir. 2001).....	31, 37
<i>Turner Broad. Sys., Inc. v. FCC</i> , 520 U.S. 180 (1997).....	53, 55
<i>U.S. Dep’t of Def. v. FLRA</i> , 510 U.S. 487 (1994).....	22, 24
<i>U.S. Dep’t of Just. v. Reps. Comm. For Freedom of Press</i> , 489 U.S. 749 (1989).....	24, 25, 51
<i>United States v. Hansen</i> , 599 U.S. 762 (2023).....	13, 17
<i>United States v. Rahimi</i> , 602 U.S. 680 (2024).....	13, 17, 26
<i>Usachenok v. Department of the Treasury</i> , 313 A.3d 53 (N.J. 2024).....	48
<i>Vidal v. Elster</i> , 602 U.S. 286 (2024).....	passim
<i>Virginia v. Am. Booksellers Ass’n, Inc.</i> , 484 U.S. 383 (1988).....	55

<i>VoteAmerica v. Schwab</i> , 121 F.4th 822 (10th Cir. 2024)	21
<i>Vrdolyak v. Avvo, Inc.</i> , 206 F. Supp. 3d 1384 (N.D. Ill. 2016)	32
<i>Vt. Agency of Nat. Res. v. U.S. ex rel. Stevens</i> , 529 U.S. 765 (2000)	42
<i>Williams-Yulee v. Fla. Bar</i> , 575 U.S. 433(2015)	50
<i>Z.D. v. Cmty. Health Network, Inc.</i> , 217 N.E.3d 527 (Ind. 2023)	46

Statutes

23 Pa. Cons. Stat. Ann. §§ 6701 to 6713	6
47 U.S.C. §227	5
705 Ill. Comp. Stat. Ann. 90/1-10, 90/2-5 (2012)	6, 11
Act of Oct. 18, 1782, 23 J. Continental Cong. 670, 671-72	5
Act of Mar. 3, 1825, ch.64, §21, 4 Stat. 102, 107-08.	5
Act of Mar. 1, 1889, ch.319, §§ 8, 13, 25 Stat. 760.....	5
Cal. Pub. Util. Code §2891.1	44
Colo. Rev. Stat. Ann. §18-9-313 (2002)	6
Daniel Anderl Judicial Security and Privacy Act of 2022, P.L. 117-263, §§ 5931-5938, 136 Stat. 3458-69	7, 11, 54
Del. Code Ann. tit. 10, §§ 1921, 1923	11
Del. Code Ann. tit. 11, §§ 9611 to 9619	6
Haw. Rev. Stat. §§ 92H-1, 92H-2	11
Kan. Stat. Ann. §21-5905 (2010)	6
Md. Code Ann., Cts. & Jud. Proc. §§ 3-2301, 3-2303	11

N.J. Stat. Ann. §1:1-10.....	49
N.J. Stat. Ann. §2A:82-46.....	6
N.J. Stat. Ann. §2C:20-31.1	6, 9, 45
N.J. Stat. Ann. §46:26A-2.....	51
N.J. Stat. Ann. §46:26A-6.....	24
N.J. Stat. Ann. §47:1-5.....	9
N.J. Stat. Ann. §47:1-17.....	9
N.J. Stat. Ann. §47:1A-1.1.....	9
N.J. Stat. Ann. §47:1B-1	10
N.J. Stat. Ann. §47:1B-2	10, 42
N.J. Stat. Ann. §47:1B-3	50, 51
N.J. Stat. Ann. §47:4-1 to -6	6, 24
N.J. Stat. Ann. §56:8-166.1.....	passim
N.J. Stat. Ann. §56:8-166.3.....	9
N.J. Stat. Ann. §§ 56:8-166.4 to -166.19	41
P.L. 2015, ch.226, §1	6
Restatement (Second) of Torts §282 (1965).....	45
Restatement (Second) of Torts §509 (1977).....	46
Restatement (Second) of Torts §519 (1977).....	46
Restatement (Second) of Torts §§ 652A-652E (1977)	5
Texas Gov’t Code §552.117 (1993).....	6
W.Va. Code §5A-8-24	11

Other Authorities

38 Cong. Rec. 7105 (Mar. 26, 1992), https://tinyurl.com/bd7pzj87	6
Chief Justice Roberts, <i>2024 Year End Report on the Federal Judiciary</i> , U.S. Supreme Court, https://tinyurl.com/5ckvnpvs	7
David Flaherty, <i>Privacy in Colonial New England 1630-1776</i> (1972)	4, 21
<i>Fifth Person Charged in Connection to Murder of Cumberland County Detective</i> , NBC10 Phila., (Nov. 6, 2024), https://tinyurl.com/96yt4rtb	8
Jeff Goldman, <i>Pizzas With N.J. Judge’s Murdered Son’s Name on Them Being Sent To Intimidate Other Judges</i> , NJ.com (Apr. 15, 2025), https://tinyurl.com/bdefpu8j	8
<i>Judges Fear for Their Safety Amid a Wave of Threats</i> , N.Y. Times (Mar. 19, 2025), https://tinyurl.com/2ftt3pm4	8
Samuel Warren & Louis Brandeis, <i>The Right to Privacy</i> , 4 Harv. L. Rev. 193 (1890)	4
U.S. Marshals Service, 2022 Judicial Security Fact Sheet (Feb. 17, 2022), https://tinyurl.com/4r3rb6ym	7
William Blackstone, <i>Commentaries on the Laws of England</i> (1772)	4

Rules

Fed. R. Civ. P. 4	40
N.J. Ct. R. 1:38-3	6
N.J. Ct. R. 2:12A-1	15, 55
N.J. Ct. R. 4:4-3	40

INTRODUCTION

Our legal tradition has long recognized the need to balance speech and privacy rights with care, particularly when the sanctuary of the home is at stake. In 2020, after the murder of a judge’s son on the doorstep of their home by an attorney seeking to murder the judge herself, the New Jersey Legislature continued that longstanding tradition by enacting Daniel’s Law. As relevant, Daniel’s Law grants certain individuals a civilly enforceable right to ask an entity to stop sharing their home address or unpublished home phone number. N.J. Stat. Ann. §56:8-166.1(a)-(b). If that entity receives valid written notice but fails to comply within ten business days, it faces civil liability. *Id.* The law also helps covered persons to vindicate their rights by assigning their claims to third parties, and provides for liquidated damages of \$1,000 per violation. *Id.* §56:8-166.1(c)-(d). The question this interlocutory appeal presents is whether Appellants—primarily data brokers and other companies that make large volumes of data available online—can dismiss the complaints against them on their theory that the law is facially unconstitutional. This Court should affirm the district court’s holdings that strict scrutiny is inappropriate to test a privacy law like this one and that Appellants’ facial motion to dismiss should fail.

Initially, in seeking facial invalidation of Daniel’s Law on this posture, Appellants face a steep climb. Even under the somewhat less stringent facial standard that applies in First Amendment cases, Appellants must still establish what

exactly the law covers and then show a disproportionate ratio of unconstitutional to constitutional applications. *Moody v. NetChoice, LLC*, 603 U.S. 707, 723-26 (2024). That showing is particularly difficult on this motion-to-dismiss posture.

In any event, on this facial posture it appears clear that the vast majority of Daniel’s Law’s applications warrant less than strict scrutiny for three reasons. First, the law fits within a longstanding tradition of safeguarding safety and privacy in the home and reflects no meddling in the marketplace of ideas, making a lower level of scrutiny appropriate regardless of the statute’s content-neutrality. *See Vidal v. Elster*, 602 U.S. 286, 300 (2024). The framework applied by the district court properly respects this tradition. *See Fla. Star v. B.J.F.*, 491 U.S. 524, 536-40 (1989); JA107. Second, because the law regulates primarily commercial speech—the sale of data with no expressive or non-commercial interests attached—it can likewise be analyzed under *Central Hudson Gas & Electric Corp. v. Public Service Commission*, 447 U.S. 557 (1980), regardless of the statute’s content-neutrality. And third, the law is not content-based, because while it applies to some types of speech and not others, the law’s coverage is driven by the choices of third parties and secondary effects.

Daniel’s Law likewise satisfies any form of facial review. As the district court recognized, the statute easily satisfies the *Florida Star* framework because few if any applications touch on matters of public concern, the law’s exceptions for public entities reveal no underinclusivity, and the New Jersey Supreme Court would likely

construe it to impose a negligence standard. Similarly, the law would satisfy *Central Hudson* or intermediate scrutiny—or, indeed, strict scrutiny, if that standard were to apply. There is no basis to overturn these careful conclusions.

In short, amid a rising tide of threats and violence, Daniel’s Law gives public servants, who face especially heightened threats to their safety and the safety of their families, a right to ask others to stop sharing non-expressive data that would allow malign actors to harm them and their families where they are most vulnerable—in their home. Such commonsense and targeted protections have long coexisted with the First Amendment, and they pose no threat to its cherished values. Daniel’s Law is facially valid, which resolves the instant appeal in its entirety.

STATEMENT OF THE ISSUE

Whether the district court correctly denied the motion to dismiss challenging Daniel’s Law as facially invalid under the First Amendment.

STATEMENT OF RELATED CASES

In addition to Appellants’ reported cases, an as-applied challenge to Daniel’s Law is pending before the New Jersey Supreme Court. *Kratovil v. City of New Brunswick*, No. A-6-24 (N.J.) (argued Mar. 3, 2025). The New Jersey Attorney General (NJAG) has also been notified of four facial challenges to Daniel’s Law pending in the New Jersey Superior Court, Law Division. The NJAG has intervened in two of those matters to date: *Atlas v. OWMN*, MID-L-992-24, and *Atlas v. Verisk*,

MID-L-903-24. The other two are *Atlas v. Choreograph LLC*, BER-L-920-24, and *Atlas v. InsideRE, LLC*, MID-L-991-24.

STATEMENT OF THE CASE

A. The Right To Privacy And Safety In The Home.

Our law has recognized the home as a sanctuary since before the Founding. New England colonists considered the home “a haven for solitude and intimacy” and “a barrier against intrusion by uninvited outsiders.” David Flaherty, *Privacy in Colonial New England 1630-1776*, at 85 (1972). Eavesdropping has been a crime since common law. *See* 4 Blackstone, Commentaries 169 (1772). And for centuries, jurists have recognized that the right to domestic privacy is coequal with the right to speak: “each must be recognized and enforced with due respect for the other.” *Pavesich v. New England Life Ins. Co.*, 50 S.E. 68, 73 (Ga. 1905); *see Frisby v. Schultz*, 487 U.S. 474, 484-85 (1988).

Starting in the 1800s, courts found this right to domestic privacy could be enforced through tort. *E.g.*, *De May v. Roberts*, 9 N.W. 146, 148-49 (Mich. 1881); *Pavesich*, 50 S.E. at 73; *Melvin v. Reid*, 297 P. 91, 92 (Cal. Ct. App. 1931) (collecting cases); Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890). By the mid-twentieth century, most States recognized such torts, *Friedman v. Martinez*, 231 A.3d 719, 729 (N.J. 2020), which fell into four categories: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) “false light”;

and (4) appropriation of name or likeness, Restatement (Second) of Torts §§ 652A-652E (1977). Each reflects one of “the most comprehensive of rights and the right most valued by civilized man”: “the right to be let alone.” *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

Statutory protections for personal information also date back centuries. In 1782, the Continental Congress passed a law protecting the confidentiality of letters. Act of Oct. 18, 1782, 23 J. Continental Cong. 670, 671-72. In 1825, Congress made it a crime to open letters en route. Act of Mar. 3, 1825, ch.64, §21, 4 Stat. 102, 107-08. And in 1889, Congress imposed monetary penalties on census officials who shared confidential information. Act of Mar. 1, 1889, ch.319, §§ 8, 13, 25 Stat. 760, 763-64.

Such privacy rights have evolved as society has entered the Information Age. In 1988, Congress passed the Video Privacy Protection Act (VPPA), after a newspaper reported the films Judge Robert Bork had rented from a local video store. *Stark v. Patreon, Inc.*, 656 F. Supp. 3d 1018, 1026-27 (N.D. Cal. 2023). Three years later, Congress enacted the Telephone Consumer Protection Act (TCPA), allowing individuals to opt out of telemarketing calls. 47 U.S.C. §227. In 1994, Congress enacted the Driver’s Privacy Protection Act (DPPA) in response to documented threats and attacks suffered by various individuals, including physicians and law

enforcement. *See Dahlstrom v. Sun-Times Media, LLC*, 777 F.3d 937, 944 & n.5 (7th Cir. 2015); 138 Cong. Rec. 7105 (Mar. 26, 1992), <https://tinyurl.com/bd7pzj87>.

States have also recognized that some individuals are especially likely to be targeted in their homes. New Jersey, for example, has various provisions protecting victims of sexual assault and domestic violence. *E.g.*, N.J. Stat. Ann. §2A:82-46(a); N.J. Stat. Ann. §47:4-1 to -6; N.J. Ct. R. 1:38-3(c)(12); *State v. Ramirez*, 284 A.3d 839, 853-54 (N.J. 2022) (collecting examples). So do other States. *E.g.*, 23 Pa. Cons. Stat. Ann. §§ 6701 to 6713; Del. Code Ann. tit. 11, §§ 9611 to 9619.

States have long enacted comparable provisions to protect public servants like judges and police officers, who often face threats to themselves and their families simply for doing their jobs. *See* Texas Gov’t Code §552.117(a)(1), (a)(15) (1993); Colo. Rev. Stat. Ann. §18-9-313 (2002); Kan. Stat. Ann. §21-5905(a)(7) (2010); 705 Ill. Comp. Stat. Ann. 90/2-5 (2012). New Jersey first enacted such a law in 2015, imposing criminal liability for purposeful or reckless disclosures of the “home address or unpublished home telephone number” of a law-enforcement officer, spouse, or child, P.L. 2015, ch.226, §1 (codified at N.J. Stat. Ann. §2C:20-31.1 (2016)), and allowing covered persons to obtain civil remedies for negligent conduct, *id.* §3 (codified at N.J. Stat. Ann. §56:8-166.1 (2016)).

B. Growing Threats To Public Servants.

The problem itself is not new. In 2005, a litigant murdered the family of U.S. District Judge Joan Lefkow. *See* Daniel Anderl Judicial Security and Privacy Act of 2022 (Federal Daniel’s Law), P.L. 117-263, §5932(a)(4), 136 Stat. 3459. In June 2013, another federal judge was “targeted by a gunman who purchased the address of his Florida home on the internet for a mere \$1.95.” 116 Cong. Rec. 213 (2020). “The gunshot missed his ear by less than 2 inches.” *Id.*

The problem, however, is getting worse. Between 2015 and 2019, “threats and other inappropriate communications against Federal judges and other judiciary personnel” saw a fivefold increase, Federal Daniel’s Law §5932(a)(3); in 2021, the U.S. Marshal’s Service reported 4,511 threats to the federal judiciary, USMS, 2022 Judicial Security Fact Sheet (Feb. 17, 2022), <https://tinyurl.com/4r3rb6ym>; *see also* Chief Justice Roberts, *2024 Year End Report on the Federal Judiciary*, U.S. Supreme Court, <https://tinyurl.com/5ckvnvps> (noting “significant uptick in identified threats at all levels of the judiciary”). A key factor is “online access to information,” which makes it easier “for malicious actors to discover where individuals live.” Federal Daniel’s Law §5932(a)(2).

Earlier this year, for instance, police responded to a threat of a bomb in Justice Amy Coney Barrett’s sister’s mailbox. Mattathias Schwartz & Abbie VanSickle, *Judges Fear for Their Safety Amid a Wave of Threats*, N.Y. Times (Mar. 19, 2025),

<https://tinyurl.com/2ft3pm4>. Judge John Coughenour was the victim of a “swatting” attack. *Id.* And federal judges have recently been receiving anonymous pizza deliveries in the name of Judge Esther Salas’ son, Daniel Anderl—the boy murdered by a deranged attorney with a case before Judge Salas. Jeff Goldman, *Pizzas With N.J. Judge’s Murdered Son’s Name on Them Being Sent To Intimidate Other Judges*, NJ.com (Apr. 15, 2025), <https://tinyurl.com/bdefpu8j>.

These threats are not limited to federal judges. In the past three years, at least three state court judges have been the victims of targeted shootings. S.B. 575, 2024 Leg., 446th Sess. (Md. 2024). In October 2023, hours after a Maryland judge issued a ruling in a divorce-and-custody case, one of the litigants shot the judge outside his home. *Id.*; JA761; *see also, e.g., State v. Taupier*, 193 A.3d 1, 9 (Conn. 2018) (threatening message from family-court litigant discussing using long-range rifle to shoot judge in her home from nearby cemetery). Other public servants, including law-enforcement officers in New Jersey, have faced similar harms. Just last year, a county detective named Monica Mosley was shot to death inside her home. *Fifth Person Charged in Connection to Murder of Cumberland County Detective*, NBC10 Phila., (Nov. 6, 2024), <https://tinyurl.com/96yt4rtb>. And myriad harms occur outside the media spotlight. As the complaints underlying this appeal allege, for example: one officer was “surveilled along with her young child at home by a major criminal organization she was investigating”; another had to move after receiving death

threats at home from MS-13, which then “targeted his mother and attempted to burn down her building”; and two others “received death threats and demands for ransom,” after which two armed individuals were arrested circling their house, “wearing ski masks.” JA98 n.7; *see also, e.g., id.* (threats suffered by other plaintiffs); *State v. Mrozinski*, 971 N.W.2d 233, 237 (Minn. 2022) (threatening letter and morgue “toe tags” left for child-protective-services officers).

C. Daniel’s Law.

In July 2020, a deranged attorney with a case before Judge Salas murdered her son, Daniel Anderl, and critically wounded her husband, at the front of door of their home. JA759. The murderer, who intended to kill Judge Salas, is believed to have found her address using a “people finder” resource online. *Id.*

In the wake of this crime, the New Jersey Legislature enacted Daniel’s Law. *See* P.L. 2020, ch.125 (codified as amended at N.J. Stat. Ann. §§ 2C:20-31.1; 47:1-17; 47:1A-1.1, -5; 47:1B-1 to -3; 56:8-166.1 to -166.3). Daniel’s Law exists “to enhance the safety and security of certain public individuals in the justice system” so they can “carry out their official duties without fear of personal reprisal.” N.J. Stat. Ann. §56:8-166.3. Building on precursor statutes noted above, it achieves those goals in relevant part by providing judges, law-enforcement officers, prosecutors, child-protective-services investigators, and immediate family members in the same household (collectively, “covered persons”) with a civilly enforceable right to

request that a private person or entity not “disclose” their home address or unpublished home telephone number going forward. *Id.* §56:8-166.1(a)(1), (d).

This civil provision (referred to here as “Daniel’s Law” for simplicity) is an opt-in. To invoke its protection, an “authorized person” must give the recipient “written notice” that the requestor “is an authorized person” and request that the recipient “cease the disclosure of the information.” *Id.* §56:8-166.1(a)(2). The recipient then has ten business days to cease such disclosure, *id.* §56:8-166.1(a)(1), subject to certain exceptions, *id.* §56:8-166.1(e)-(f). If the recipient fails to comply, they are civilly liable, most relevantly for “actual damages, but not less than liquidated damages” of \$1,000 per violation, and “punitive damages upon proof of willful or reckless disregard.” *Id.* §56:8-166.1(c). A covered person may assign their civil claim. *Id.* §56:8-166.1(d).

The Legislature also created the Office of Information Privacy (OIP) to process requests for public agencies not to disclose covered persons’ addresses. *Id.* §§ 47:1B-1(b), (c)(1). Because an approved request will generally limit notices and information the individual receives from the government, OIP must, in approving a request, obtain an affirmation of these impacts from the requestor. *Id.* §§ 47:1B-2(a), (d). If a request is approved, public agencies must cease sharing the covered person’s information within 30 days. *Id.* §47:1B-2(b). Under Daniel’s Law today, a covered

person need not go through the OIP process before asking a private entity to stop sharing their information.

Other States, and the Federal Government, have enacted similar laws. Like New Jersey's law, these laws apply to specific public servants and household members and require a written request, and some similarly allow for assignment of claims. While several such laws use a similar opt-in mechanism, they have shorter compliance windows and restrict more information.¹

D. This Litigation.

Atlas, as claim-assignee for numerous covered persons, sued Appellants for failing to cease disclosure of those persons' home addresses and/or unpublished home phone numbers within ten business days. JA767, 777. Nearly all Appellants are for-profit entities, including data brokers and marketing companies. Br.15-16. After removing to federal court, Appellants filed a consolidated motion to dismiss, asserting that Daniel's Law is facially invalid under the First Amendment. No. 1:24-

¹ *Compare, e.g.*, Federal Daniel's Law §§ 5933(2)(A) (covering more extensive information, including home address, phone number, email, SSN, bank account, license-plate number, birthdate, and minor children), 5934(b)(1) (claim-assignment), 5934(d)(2)(A)(i) (three days); Del. Code Ann. tit. 10, §§ 1921(6) (covering more extensive information), 1923(b)(1) (three days), 1924(d) (claim-assignment); Haw. Rev. Stat. §§ 92H-1 (covering more extensive information), 92H-2 (three business days); 705 Ill. Comp. Stat. Ann. 90/1-10 (covering more extensive information), 90/2-5(b)(1) (three days); Md. Code Ann., Cts. & Jud. Proc. §§ 3-2301(d) (covering more extensive information), 3-2303(d)(1) (three days); W.Va. Code §5A-8-24(h)(3) (one day).

cv-4105, ECF 27-28. The district court permitted the NJAG to intervene to defend the statute. No. 1:24-cv-4141, ECF 17.

The district court denied Appellants' motion and found Daniel's Law facially constitutional. JA121. First, Judge Bartle held that the statute regulates protected speech. JA100-01. He concluded that Daniel's Law is not a commercial-speech regulation as the expression it limits "does not propose a commercial transaction," JA102-03, and that it is content-based because it "regulates particular subject matter," JA103-04. But he concluded that strict scrutiny is nevertheless inappropriate because Daniel's Law continues a long historical tradition of laws protecting domestic privacy and "is analogous to the long-standing common law tort for invasion of privacy." JA105-08. To adjudicate this speech-versus-privacy dispute, Judge Bartle therefore applied the framework elucidated in *Florida Star*, 491 U.S. 524. JA107-09.

Judge Bartle held that Daniel's Law satisfied that framework. JA114. First, he held that the information covered does not generally implicate matters of public concern, acknowledging that unusual exceptions could be handled through as-applied challenges. JA109-10.² Second, he held that Daniel's Law serves a state interest of the highest order without the need for further tailoring: "enhanc[ing] the

² One such as-applied challenge was argued in the New Jersey Supreme Court on March 3, 2025. See *Kratovil v. City of New Brunswick*, No. A-6-24, <https://www.njcourts.gov/cases/a-6-24>.

safety and security of judges, prosecutors, and other law-enforcement officers so that they are able to carry out their official duties without fear of personal reprisal.” JA110-11. He also found the statute’s limited exemptions for public agencies did not render it underinclusive, JA111-12, and disagreed that other features rendered the law overbroad, JA112-15. Finally, he concluded the New Jersey Supreme Court would likely construe Daniel’s Law to impose a negligence standard. JA119.

Judge Bartle certified his order for interlocutory appeal, JA131, and this Court granted Appellants’ petition, JA141-42.

SUMMARY OF ARGUMENT

The district court correctly denied Appellants’ motion to dismiss and held that Daniel’s Law is facially valid under the First Amendment.

I. Appellants face a high bar to obtain facial relief. *NetChoice*, 603 U.S. at 723-24. They do not dispute that Daniel’s Law is “constitutional in some of its applications.” *United States v. Rahimi*, 602 U.S. 680, 693 (2024). Nor can they show the “lopsided ratio” of impermissible applications necessary for First Amendment overbreadth. *United States v. Hansen*, 599 U.S. 762, 769-70 (2023). That analysis requires totaling the law’s “impermissible and permissible” applications and “compar[ing] the two sets,” *NetChoice*, 603 U.S. at 726, which typically requires an evidentiary record that naturally cannot exist on this motion-to-dismiss posture. Courts have rightly denied similar facial motions to dismiss.

II. Appellants’ facial challenge entails no more than intermediate scrutiny.

A. As *Vidal*, 602 U.S. at 300, made clear, even content-based provisions do not trigger strict scrutiny if longstanding tradition shows they coexist with First Amendment values. Daniel’s Law continues a tradition of domestic-privacy protections that has long coexisted with the First Amendment. Because of that tradition and the lack of any “realistic probability that official suppression of ideas is afoot,” *Davenport v. Wash. Educ. Ass’n*, 551 U.S. 177, 188-89 (2007), strict scrutiny is unwarranted. Instead, the *Florida Star* framework properly balances privacy and speech.

B. Because Daniel’s Law primarily regulates commercial speech, Appellants’ facial challenge is also properly analyzed under *Central Hudson*, 447 U.S. 557, regardless of content-neutrality. Courts recognize that disclosing non-expressive data for profit, with no non-economic purpose, is commercial speech. *E.g.*, *Stark*, 656 F. Supp. 3d at 1034. Most applications of Daniel’s Law fit this description.

C. Daniel’s Law also warrants intermediate scrutiny because content does not drive its coverage. Although Daniel’s Law “requires an examination of speech,” it is “agnostic as to content.” *City of Austin v. Reagan Nat’l Advert. of Austin, LLC*, 596 U.S. 61, 69 (2022). Instead, the law protects certain data only where a covered person has requested nondisclosure, and only because that subclass of data “happens

to be associated with particular ‘secondary effects.’” *R.A.V. v. City of St. Paul*, 505 U.S. 377, 389 (1992) (citation omitted).

III. Daniel’s Law satisfies any level of facial scrutiny.

A. Daniel’s Law facially satisfies *Florida Star*. To start, Appellants do not dispute that the State’s interests are compelling, and nearly all applications involve only private concern. No public matter typically turns on whether a particular judge lives at one specific address or another.

The law is not overinclusive. Daniel’s Law’s opt-in regime is a hallmark of its narrow tailoring, as it leaves as much speech unregulated as possible, devolving control to those best situated to weigh the risks and requiring valid notice and time to comply. Nor is it overbroad on scienter grounds, as the New Jersey Supreme Court would likely conclude it operates as a negligent-disclosure law. Finally, Daniel’s Law is not facially underinclusive, because its exceptions are exceedingly narrow and easily explained.

B-C. Similarly, Daniel’s Law satisfies facial scrutiny under *Central Hudson*, intermediate scrutiny, or even strict scrutiny. Appellants concede that the State’s interests are compelling, Br.25; the law’s opt-in regime is amply tailored; and no less-restrictive means would adequately serve its compelling interests.

IV. Alternatively, this Court should certify any state-law questions to the New Jersey Supreme Court. *See* N.J. Ct. R. 2:12A-1.

STANDARD OF REVIEW

This Court exercises de novo review over denial of a Rule 12(b)(6) motion to dismiss, *Johnson v. NCAA*, 108 F.4th 163, 175 n.57 (3d Cir. 2024), and “may affirm on any basis supported by the record,” *Children’s Health Def., Inc. v. Rutgers*, 93 F.4th 66, 83 (3d Cir.), *cert. denied*, 144 S.Ct. 2688 (2024).

ARGUMENT

I. In Seeking Facial Relief, Appellants Face A High Bar.

“For a host of good reasons, courts usually handle constitutional claims case by case, not en masse.” *NetChoice*, 603 U.S. at 723. For one, such claims “often rest on speculation about the law’s coverage and its future enforcement.” *Id.* For another, they “threaten to short circuit the democratic process by preventing duly enacted laws from being implemented in constitutional ways,” *id.*—a problem that increases “when federal courts are asked to block states from enforcing their laws” amid uncertainty about their construction, *cf. Del. State Sportsmen’s Ass’n, Inc. v. Del. Dep’t of Safety & Homeland Sec.*, 108 F.4th 194, 205 (3d Cir. 2024) (making similar observation in preliminary-injunction context), *cert. denied*, 145 S.Ct. 1049 (2025). Such challenges are “hard to win,” and typically require showing the law has *no* valid applications, or *no* “plainly legitimate sweep.” *NetChoice*, 603 U.S. at 723.

That high bar is not met here. Appellants themselves indicate they would accept applications in which a covered person sought to have their information

removed from public and private sources alike; provided “sufficient” identity-verifying information; submitted their request in a non-“bundle[d]” form; and indicated that further disclosure posed significant risks. *See* Br.37-39. That is hardly a “hypothetical situation,” *Bruni v. City of Pittsburgh*, 824 F.3d 353, 363 (3d Cir. 2016), and Appellants do not claim it is. That even Appellants do not dispute that Daniel’s Law is “constitutional in some of its applications,” *Rahimi*, 602 U.S. at 693, easily forecloses facial relief under the usual test.

That leaves the “less demanding” but “still rigorous” standard that applies in free-speech cases. *NetChoice*, 603 U.S. at 723. In such cases, to “provide[] breathing room for free expression,” courts will strike down statutes as “overbroad” if a “substantial” number of the law’s applications are unconstitutional, relative to its “plainly legitimate sweep”—that is, if there is a “lopsided ratio” of unconstitutional to constitutional applications. *Hansen*, 599 U.S. at 769-70. Assessing whether such a ratio exists requires determining both the numerator and the denominator: first identifying the law’s total coverage; next deciding “which of the law’s applications violate the First Amendment”; and finally comparing those applications “against the rest.” *NetChoice*, 603 U.S. at 724-25. But because this necessarily “destroys some good along with the bad,” it too is “strong medicine,” not lightly dispensed. *Hansen*, 599 U.S. at 770.

This appeal’s odd posture—arising from the denial of a motion to dismiss—makes facial relief particularly remote. Because overbreadth requires a court to total up the law’s “impermissible and permissible” applications and “compare the two sets,” *NetChoice*, 603 U.S. at 726, it is an inquiry in which “[e]vidence is key,” *Mazo v. N.J. Sec’y of State*, 54 F.4th 124, 152 (3d Cir. 2022), *cert. denied*, 144 S.Ct. 76 (2023). So courts typically cannot “undertake the needed inquiries” if “the record is underdeveloped,” *NetChoice*, 603 U.S. at 726—as it inherently is on this motion-to-dismiss posture, where no one has tested how many applications of Daniel’s Law would actually raise the issues Appellants complain of. For similar reasons, courts have rejected overbreadth challenges brought via motions to dismiss in analogous data-privacy contexts. *E.g.*, *Boelter v. Advance Mag. Publishers Inc.*, 210 F. Supp. 3d 579, 603 (S.D.N.Y. 2016); *Stark*, 656 F. Supp. 3d at 1039; *see also NetChoice*, 603 U.S. at 744 (remanding for lower courts to do this analysis).

Appellants largely seek to avoid the overbreadth standard, claiming that an abstract conception of the law “fails strict scrutiny,” and concluding that the law “is, by definition, facially unconstitutional.” Br.21-22 (citing *Bruni*, 824 F.3d at 363). But that is tautological: the question is what “the relevant constitutional test” *is*, *Bruni*, 824 F.3d at 363, and then whether sufficient applications would fail it. (They do not.) And as *NetChoice* made clear, courts cannot do this analysis in the abstract, with an “underdeveloped” record. 603 U.S. at 726. Instead, this Court must first

determine what Daniel's Law covers, and then assess how each of those applications would fare under the relevant form of scrutiny.

II. This Facial Challenge Implicates Less-Than-Strict Scrutiny.

Even leaving those concerns to the side, for three independent reasons this facial challenge should implicate no more than intermediate scrutiny. As Judge Bartle recognized, Daniel's Law continues a tradition of protections for privacy in the home that have long coexisted with the First Amendment, which makes *Florida Star* or a similar framework appropriate. Were this Court to apply traditional tiers of scrutiny, heartland applications of Daniel's Law's regulate only commercial speech, warranting *Central Hudson* scrutiny. Finally, Daniel's Law is content-neutral, offering a third reason to apply intermediate scrutiny.

A. The Longstanding Coexistence Of Domestic-Privacy Laws And The First Amendment Supports Reduced Scrutiny.

As *Vidal*, 602 U.S. 286, recently made clear, even content-based provisions do not trigger strict scrutiny if longstanding tradition shows they coexist with First Amendment values. *Id.* at 300-01. As a law safeguarding privacy in the home, Daniel's Law fits within such a longstanding tradition. Judge Bartle therefore correctly declined to apply strict scrutiny, and the framework he drew from *Florida Star* properly balances these coequal constitutional interests.

1. Daniel's Law Continues An Established Tradition.

Vidal reaffirms a sensible doctrinal point: established legal traditions do not ineluctably trigger strict scrutiny just because they happen to regulate some types of speech and not others. There, the Court held that even though the Lanham Act's prohibition on registering trademarks identifying living persons by name without consent is formally content-based, 602 U.S. at 294-95, heightened scrutiny was inappropriate given the history and tradition of trademark regulation, which largely could not function with some content-based features, *id.* at 299-300. In other words, content-based laws do not trigger heightened scrutiny if longstanding tradition shows that any content-discrimination arises organically from the nature of the regulation and does not threaten free speech. *See id.* at 300; *see also id.* at 299 (noting that such a "longstanding, harmonious relationship" belies a need for "heightened scrutiny"); *id.* at 312 (Barrett, J., concurring) (observing that such traditions will often reflect that a law "has always been content based without functioning as a ready tool of Government censorship"). And where there is "no realistic possibility that official suppression of ideas is afoot," strict scrutiny is unwarranted. *Davenport*, 551 U.S. at 188-89; *see Vidal*, 602 U.S. at 311 (Kavanaugh, J., concurring) ("[I]n my view, a viewpoint-neutral, content-based trademark restriction might well be constitutional even absent such a historical pedigree.").

Citing *Vidal*, the Tenth Circuit in *VoteAmerica v. Schwab*, 121 F.4th 822 (10th Cir. 2024), recently applied intermediate scrutiny and upheld a content-based law prohibiting private parties from partially filling out a mail-ballot application sent to a registered voter absent that voter’s consent. *Id.* at 850 The court reasoned that restrictions on when “someone can fill out for another person a government form seeking noncontroversial information do not on their face suggest hostility to any idea or point of view.” *Id.* at 851. And “like the ‘uniquely content-based nature of trademark regulation,’ the history of regulations (instructions) governing the filling out of noncontroversial information on government forms provides substantial comfort that such regulation is fully compatible with a lively market in controversial ideas.” *Id.* (quoting *Vidal*, 602 U.S. at 300).

Because protections for privacy and safety in the home have similarly “deep roots in our legal tradition,” heightened scrutiny is inappropriate here too. *See Vidal*, 602 U.S. at 301. As noted, *see supra* at 4-6, the home has occupied a special role “as a haven for solitude and intimacy and as a barrier against intrusion by uninvited outsiders” since before the Founding. Flaherty, *supra*, at 85. This right has been enforced through various means, including prohibitions against eavesdropping, data restrictions, do-not-call provisions, and tort. *See supra* at 4-6. Courts have repeatedly recognized the need to preserve the home’s “sanctity” and acknowledged “that unwilling listeners may be protected when within their own homes.” *Frisby*, 487

U.S. at 484-85; *see also De May*, 9 N.W. at 149 (acknowledging plaintiff “had a legal right to the privacy of her apartment”); *Mainstream Mktg. Servs. v. FTC*, 358 F.3d 1228, 1236-37, 1242 (10th Cir. 2004) (upholding national “do-not-call” registry). Through it all, “[t]he right to speak and the right of privacy have been coexistent.” *Pavesich*, 50 S.E. at 73.

Privacy protections have also expanded to encompass personal information. While basic protections date to the nineteenth century, *see supra* at 5, these protections have evolved with technology, *see Dirkes v. Borough of Runnemede*, 936 F. Supp. 235, 238 (D.N.J. 1996) (collecting federal privacy statutes); *supra* at 5-6 (collecting federal statutes). The VPPA, for instance, arose in the wake of disclosure of Judge Bork’s video-rental history, amid “the then-nascent threat of computerized mass-data collection.” *Stark*, 656 F. Supp. 3d at 1026-27.

These twin privacy traditions dovetail in the context of protections for information that exposes individuals to harassment or violence in their homes. The Privacy Act restricts disclosure of home addresses of federal employees. *U.S. Dep’t of Def. v. FLRA*, 510 U.S. 487, 502 (1994). Other laws prohibit a company from disclosing a caller’s telephone number without that caller’s consent. *Barasch v. Bell Tel. Co. of Pa.*, 605 A.2d 1198, 1202-03 (Pa. 1992) (Pennsylvania Wiretap Act). And since the rise of the Internet, New Jersey and other States have acted to protect the privacy and safety of individuals particularly likely to suffer targeting in the

home—from victims of domestic violence and sexual assault to, as relevant here, public servants facing growing threats simply because of the jobs they do. *See supra* at 6.

Daniel’s Law is part of this longstanding tradition. The law allows individuals to protect two pieces of sensitive personal data—their home address and unpublished home phone number—by making an affirmative, written request. N.J. Stat. Ann. §56:8-166.1(a). It thus allows them to safeguard the precise information that would enable malicious actors to attack or harass them at home. And like the TCPA and comparable do-not-call provisions, it is an opt-in.³ Because similar laws have long operated in harmony with free-speech values—and because, as Appellants concede, the statute was adopted through benign motives, with no “realistic possibility that official suppression of ideas is afoot,” *Davenport*, 551 U.S. at 188-89—the law does not merit strict scrutiny. *Accord* JA106-07.

Appellants’ counterarguments are unpersuasive. First, Appellants claim that Daniel’s Law is not a privacy statute because it is intended “to enhance the safety and security of certain public officials.” Br.44. But Judge Bartle rightly rejected this false dichotomy, as Daniel’s Law safeguards residential privacy *in order to* protect

³ Appellants’ suggestions that Daniel’s Law itself prohibits speech, *e.g.*, Br.25-28, are therefore misstated. The law prohibits no speech; it instead provides a covered person a civilly enforceable right to request that a specific speaker stop sharing their information.

“safety and security.” JA106. The history of other privacy laws reveals similarly intertwined interests. *E.g.*, *Dahlstrom*, 777 F.3d at 944 (noting DPPA is “a public safety measure”). That such privacy laws respond to risks graver than annoyance or embarrassment hardly counts *against* their facial validity.

Second, Appellants err in claiming that Daniel’s Law does not fit within historical privacy laws because “contact information is public” via some government lists. Br.44. Initially, a person’s interest in protecting personal information “does not dissolve simply because that information may be available to the public in some form.” *FLRA*, 510 U.S. at 500.⁴ Moreover, such records are less accessible than information posted on open websites, operated by private entities. *See U.S. Dep’t of Just. v. Reps. Comm. For Freedom of Press*, 489 U.S. 749, 764 (1989) (*RCFP*) (noting “vast difference between the public records that might be found after a diligent search ... and a computerized summary located in a single clearinghouse”). And here, Daniel’s Law already enables covered persons to restrict access to nearly all of these sources, with only one narrow exception for non-mortgage liens, obtainable only county-by-county. *See* N.J. Stat. Ann. §46:26A-6; *id.* §47:1B-3(a); *see also infra* at 50-51. That does not diminish the privacy interests associated with such information—much the same way a person has a substantial interest in

⁴ Appellants chide Judge Bartle for relying on FOIA decisions, Br.46-47, but he properly considered these precedents for what they reveal about privacy interests—not to suggest that FOIA and free speech are interchangeable. *See* JA105.

protecting her Social Security number (SSN) even if it remains obtainable with enough effort. *See RCFP*, 489 U.S. at 764; *Ostergren v. Cuccinelli*, 615 F.3d 263, 279-80 (4th Cir. 2010).

Third, Appellants’ related argument that there is “a long historical tradition of public access to” home addresses and telephone numbers, Br.45, misapprehends the core issue. Indeed, most people’s contact information is publicly available. But Daniel’s Law does not prohibit sharing contact information as a general matter; it applies only following a request to stop, so a history of general availability is not inconsistent. Instead, the probative history is “that a significant number of persons, ranging from public officials and performers to just ordinary folk, choose to list their telephones privately”—and have been understood to have a right to do so—“because they regard their home addresses to be private information.” *See Paul P. v. Farmer*, 227 F.3d 98, 101 (3d Cir. 2000); JA105. Moreover, because individuals generally cannot predict in advance whether they will become covered persons, the default availability of a person’s address before she is a covered person cannot logically preclude her from taking action once she is a covered person.

Fourth, Appellants’ claim that Daniel’s Law is not analogous to historic privacy laws because those laws did not typically extend to home addresses, Br.45-46, misconstrues the proper analysis. In *Vidal*, the historical analogues on which the Court relied were not twins of the Lanham Act’s names clause, but rather revealed

the general principle that because trademark law entails content differentiation and has long coexisted with the First Amendment, the names clause did not warrant strict scrutiny. 602 U.S. at 295-300; *cf. Rahimi*, 602 U.S. at 740 (Barrett, J., concurring) (“Historical regulations reveal a principle, not a mold.”). So too with privacy. For instance, while the tort of intrusion on seclusion predated modern technology, it has evolved to encompass protections for a person’s personal information, which in many cases *facilitate* a physical intrusion. *See, e.g., In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 294-95 (3d Cir. 2016); *Dirkes*, 936 F. Supp. at 238-39. The same logic applies to public disclosure of private facts—even if, in an earlier time, a home address was less likely to trigger the concerns it triggers today. In short, that our legal tradition has long safeguarded residential privacy and safety, in harmony with the First Amendment, explains why related efforts to do so amid today’s technological context likewise merit reduced scrutiny.

Finally, Appellants’ two cited cases—*Brayshaw v. City of Tallahassee*, 709 F. Supp. 2d 1244 (N.D. Fla. 2010), and *Sheehan v. Gregoire*, 272 F. Supp. 2d 1135 (W.D. Wash. 2003)—are not to the contrary. Br.43-44. *Brayshaw* involved a blanket prohibition on disclosure of a law-enforcement officer’s information absent the employing agency’s “authorization.” 709 F. Supp. 2d at 1247. And *Sheehan* similarly involved a law prohibiting disclosure of certain public employees’ information absent “express written permission.” 272 F. Supp. 2d at 1139. Both laws

thus imposed a default prohibition, unless a protected party opted *out*. So *Brayshaw* and *Sheehan* are both non-binding and inapposite, because a default ban—as opposed to a law empowering individuals to opt *into* nondisclosure—poses a greater risk to speech. That risk is absent here.⁵

2. The *Florida Star* Framework Properly Balances Privacy And Speech.

Given this longstanding legal tradition, Judge Bartle was correct to forgo strict scrutiny. His application of the *Florida Star* framework instead properly balanced privacy and speech.

In *Florida Star*, the Supreme Court considered a newspaper’s as-applied challenge to a Florida law prohibiting publication of a sexual-assault victim’s name, after the newspaper had obtained the name from a report placed in the local sheriff’s department’s pressroom. 491 U.S. at 526-27. Recognizing that privacy and speech rights are “both ‘plainly rooted in the traditions and significant concerns of our society’” and emphasizing “the sensitivity and significance of the interests presented in clashes between” those rights, the Court concluded that its analysis should “sweep no more broadly than the appropriate context of the instant case.” *Id.* at 533. To

⁵ Nor does *Barr v. American Association of Political Consultants, Inc.*, 591 U.S. 610 (2020), or *Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011), support heightened scrutiny. *Contra* FIRE.Br.12-13; CDIA.Br.9. While those cases involved privacy laws, neither concerned domestic safety. *See Barr*, 591 U.S. at 613 (robocalls to cellphones); *Sorrell*, 564 U.S. at 557 (physicians’ prescribing practices). Both also had tailoring flaws that Daniel’s Law lacks. *See infra* at 49-50.

perform this case-specific balancing, the Court drew from *Smith v. Daily Mail Publishing Co.*, 443 U.S. 97 (1979), to articulate a balancing test that required considering both (1) whether the newspaper “lawfully obtain[ed] truthful information about a matter of public significance,” and (2) whether the law served “a need to further a state interest of the highest order.” *Fla. Star*, 491 U.S. at 536-37. To analyze that second question, the Court looked to: (a) how the information was obtained; (b) the “sweep” of the statute (there, focusing on the lack of “a scienter requirement”); and (c) “the facial underinclusiveness” of the statute. *Id.* at 538-40.

The *Florida Star* test thus balances privacy and speech interests in an appropriately sensitive manner. It ensures that speech on matters “of public concern” receive greater protection than speech on purely private topics, consistent with core First Amendment principles, *e.g.*, *Snyder v. Phelps*, 562 U.S. 443, 451-52 (2011), while requiring meaningful but not least-restrictive-means-level tailoring. In other words, it approximates strict scrutiny if speech is on a matter of public concern, and intermediate scrutiny if not.⁶ It was therefore wholly appropriate for Judge Bartle to apply it to resolve this privacy-versus-speech dispute.

That approach also comports with this Court’s decision in *Schrader v. District Attorney of York County*, 74 F.4th 120 (3d Cir. 2023). *Contra* Br.42-43. *Schrader*

⁶ Accordingly, Appellants are incorrect to suggest that this test is more exacting than strict scrutiny. *See* Br.48. Relatedly, Appellants’ reliance on cases applying RLUIPA’s least-restrictive-means test, Br.37, is misplaced.

involved an as-applied First Amendment challenge to a Pennsylvania law criminalizing the purposeful release of child-abuse records, brought by the grandmother of a deceased two-year-old who wished to criticize how local officials had handled the child’s case. *Id.* at 123. In adjudicating that challenge, this Court acknowledged two lines of precedent: one applying strict scrutiny to content-based speech regulations, and the other applying *Florida Star*. *Id.* at 126. While noting that the *Florida Star* “test fits oddly with our modern focus on content-based restrictions,” this Court acknowledged that “its principle seems to date to the Founding,” and it “understandably stands apart from the content-focused analysis.” *Id.* at 128. While this Court did not need to “reconcile these two lines of precedent” in that as-applied context because the answer was clearly the same under either, *id.* at 126, the facts and posture here are distinct: Appellants press a facial challenge, and the precise home address of the mine-run covered person is not “significant to the public,” unlike the child-abuse records at issue in *Schrader*. *Id.* at 128. So the age-old principles reflected in *Florida Star* have something different to say here—and if they appear in tension with content-discrimination doctrine, *Vidal* shows how to reconcile the two.

B. Most Applications Impact Only Commercial Speech.

The denial of Appellants’ facial motion should also be affirmed because Daniel’s Law primarily regulates only commercial speech. Those applications are

thus subject to *Central Hudson* scrutiny. *See* 447 U.S. at 566; *City of Austin*, 596 U.S. at 68 n.3, 73-74 (even content-based commercial-speech restrictions are subject to *Central Hudson*). They easily satisfy it.

While no bright-line test distinguishes commercial from non-commercial speech in all circumstances, courts examine three non-exclusive factors. Those factors are: (1) whether “the speech refer[s] to a specific product or service,” (2) whether the speech is an advertisement; and (3) whether the speaker has “an economic motivation for the speech.” *Greater Phila. Chamber of Com. v. City of Philadelphia*, 949 F.3d 116, 137 (3d Cir. 2020).

Courts applying this “fact-driven” rubric, *Ariix, LLC v. NutriSearch Corp.*, 985 F.3d 1107, 1115 (9th Cir. 2021), regularly hold that disclosing personal information for profit is commercial speech. They do so, for instance, with respect to restrictions on sharing data in the media context, since the information “is arguably itself a product,” with disclosure “motivated by the commercial interests of both” the seller and the buyer—particularly where the data has “no expressive or creative content,” “contain[s] nothing of public interest, and serv[es] no non-economic purpose.” *Stark*, 656 F. Supp. 3d at 1033-34 (VPPA); *see also Saunders v. Hearst Television, Inc.*, 711 F. Supp. 3d 24, 32-33 (D. Mass. 2024) (same); *Boelter v. Hearst Commc’ns, Inc.*, 192 F. Supp. 3d 427, 445 (S.D.N.Y. 2016) (similar Michigan law); *Advance Mag.*, 210 F. Supp. 3d at 597 (Michigan Preservation of

Personal Privacy Act). So too with consumer-debt information shared by debt collectors. *See, e.g., Trans Union Corp. v. FTC*, 267 F.3d 1138, 1140-42 (D.C. Cir. 2001).

Here, mine-run applications of Daniel’s Law likewise regulate only commercial speech. These applications apply to data brokers and the like—for-profit companies that transmit gigabytes of personal information each day. *E.g.*, JA773; *accord* Br.15-16 For these applications, the information itself *is* the “specific product,” and is driven solely by “an economic motivation.” *Greater Phila. Chamber*, 949 F.3d at 137. Moreover, these applications impact “no expressive or creative content,” contain “nothing of public interest,” and serve “no non-economic purpose.” *Stark*, 656 F. Supp. 3d at 1034. So even accepting that these companies are speaking in the formal sense, “reduced constitutional protection” is warranted. *See Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 761-62 & n.8 (1985).

The counterpoint that this speech “does not propose a commercial transaction,” Br.24 (quoting JA103), is unpersuasive. While advertisements are the paradigmatic example of commercial speech, *e.g., Harris v. Quinn*, 573 U.S. 616, 648 (2014), they are not its exclusive remit, *Greater Phila. Chamber*, 949 F.3d at 137. And in any event, just as hanging a dress in the display window at Macy’s does

indeed propose a transaction, putting a judge's home address in the online corollary of that display window for \$1.95 does, too. *See supra* at 7.

Appellants' citations to *Dex Media West, Inc. v. City of Seattle*, 696 F.3d 952 (9th Cir. 2012); *Vrdolyak v. Avvo, Inc.*, 206 F. Supp. 3d 1384 (N.D. Ill. 2016); and *IMDb.com v. Becerra*, 962 F.3d 1111 (9th Cir. 2020), are inapposite. Br.24. *Vrdolyak* concerned a free online attorney directory, which that court reasoned did not engage in commercial speech simply because it ran advertisements. 206 F. Supp. 3d at 1388-89. Similarly, *Dex Media West* involved a challenge to a municipal ordinance regulating telephone directories "as a whole." 696 F.3d at 957. That court reasoned that the directories had "more than a commercial purpose," because they featured significant non-commercial information, including "community information," *id.*; their advertisements took "only a limited fraction of the space," *id.* at 963; and the State required phone companies to distribute the directories, *id.* at 957. None of those rationales suggest that for-profit disclosure of a judge's home address, without more, is non-commercial. *Cf. IMDb.com*, 962 F.3d at 1121-22 (finding wiki-style database including actors' ages was non-commercial speech, as content was "encyclopedic, not transactional").

Finally, even if Daniel's Law entails *some* non-commercial applications, the large number of commercial applications makes a difference in this facial posture. Courts confronting statutes with mixed commercial and non-commercial

applications begin with the commercial applications and only then, assuming those applications are valid, consider whether the law is nevertheless overbroad. *See Bd. of Trustees of State Univ. of N.Y. v. Fox*, 492 U.S. 469, 481, 485 (1989); *Am. Future Sys. v. Penn State Univ.*, 752 F.2d 854, 862 & n.26 (3d Cir. 1984). That approach is also the only one that comports with *NetChoice*. *See* 603 U.S. at 725 (noting, for one set of provisions, that the lower courts should consider “as to each thing covered,” whether it satisfies the test that applies to commercial disclosures). Put simply, if a hypothetical law has 100 applications, of which 80 cover commercial speech and satisfy *Central Hudson*, it is hard to see how *NetChoice* would permit striking down the entire law by applying strict scrutiny to the other twenty.

C. Daniel’s Law Is Content Neutral.

A third basis likewise justifies less-than-strict scrutiny: Daniel’s Law is content-neutral. While the law applies to some types of data and not others—*e.g.*, addresses but not birthdays—the feature that drives coverage is not content itself.

No law addresses all problems at once. To avoid the perverse results that would flow from applying strict scrutiny to all laws that even incidentally affect some kinds of speech but not others, courts distinguish laws that “target[] speech ... *because of the topic discussed or the idea or message expressed*” from those that are “agnostic as to content.” *City of Austin*, 596 U.S. at 69 (emphasis added). This makes sense, because “‘the rationale [for] the general prohibition’ on content-based

regulations ‘is that content discrimination raises the specter that the Government may effectively drive certain ideas or viewpoints from the marketplace.’” *Project Veritas v. Schmidt*, 125 F.4th 929, 949 (9th Cir. 2025) (en banc) (quoting *Davenport*, 551 U.S. at 188). But where a legislature treats one subclass of speech differently simply because “that subclass happens to be associated with particular ‘secondary effects,’” and “there is no realistic possibility that official suppression of ideas is afoot,” there is no need to apply strict scrutiny. *R.A.V.*, 505 U.S. at 389-90 (citation omitted).

A law can therefore be “agnostic as to content,” even if it “requires an examination of the speech,” so long as that examination is “only in service of drawing neutral ... lines.” *City of Austin*, 596 U.S. at 69. Under such circumstances, assessing whether a law is content-based requires assessing *why* that examination is required. Thus, in the sign-code context, courts first “identify the regulated category and a comparable category that is treated differently”; then “discern what feature distinguishes” the two categories; and finally “decide whether that feature is the sign’s [content].” *Camp Hill Borough Republican Ass’n v. Borough of Camp Hill*, 101 F.4th 266, 269 (3d Cir. 2024).

Here, that comparative exercise shows that Daniel’s Law is content-neutral. Daniel’s Law protects certain data only when a covered person has expressly requested nondisclosure, and only because this data uniquely allows wrongdoers to

target covered persons and their families at home. Thus, if Judge A has requested nondisclosure and Judge B has not, the feature that distinguishes their addresses is whether Judge A has deemed her family at sufficient risk to request nondisclosure—not the content of the addresses. Similarly, if Judge A is a covered person and Person C is not, the feature that distinguishes their addresses is that Judge A and her family are uniquely at risk because of the work Judge A does—not content. *See id.* at 269-70; *see also Dahlstrom*, 777 F.3d at 949 (finding DPPA content-neutral). And even if one compares home addresses and birthdays, the feature that drives the difference is not governmental favoring of address information *qua* address information (or targeting of birthdays *qua* birthdays), but rather that only the former happens to entail certain “secondary effects,” *R.A.V.*, 505 U.S. at 389—the risk of serious harm to Judge A or her family in their home.

III. Daniel’s Law Satisfies Facial Scrutiny.

Daniel’s Law satisfies any level of scrutiny. Judge Bartle correctly concluded that Daniel’s Law survives under *Florida Star*. For similar reasons, Daniel’s Law facially satisfies *Central Hudson* or intermediate scrutiny, and would satisfy even strict scrutiny if it were warranted.

A. Daniel’s Law Satisfies Facial Scrutiny Under *Florida Star*.

Judge Bartle properly concluded that Daniel’s Law is constitutional under *Florida Star*. *See* JA107-13. As noted, *Florida Star* considered (1) whether a speaker

“lawfully obtained truthful information about a matter of public significance,” and (2) whether the law served “a need to further a state interest of the highest order.” *Id.* at 536-37. To analyze that second question, the Court looked to: (a) how the information was obtained; (b) the statute’s “sweep” (particularly, its lack of a scienter requirement); and (c) the statute’s “facial underinclusiveness.” 491 U.S. at 538-40. Here, the NJAG does not dispute the information is true and lawfully obtained, and Appellants do not dispute the State’s interests are “compelling.” Br.18, 25; *see also* JA110-11. So the questions at issue are whether most applications of Daniel’s Law involve a matter of public concern, and whether the law is impermissibly over- or underinclusive. Each weighs against Appellants’ facial challenge.

1. Daniel’s Law Facially Implicates Only Private Concern.

That few if any applications implicate matters of public concern is straightforward. “Speech deals with matters of public concern when it can ‘be fairly considered as relating to any matter of political, social, or other concern to the community,’ or when it ‘is a subject of legitimate news interest,’” based on “the content, form, and context of [the] speech.” *Snyder*, 562 U.S. at 453; *see also Cox Broad. Corp. v. Cohn*, 420 U.S. 469, 492 (1975) (rooting test in public’s need “to vote intelligently,” “register opinions on the administration of government,” and oversee “the administration of justice”). For example, signs criticizing “the political

and moral conduct of the United States and its citizens,” fall on the public-concern side, *Snyder*, 562 U.S. at 454, while details from family court involving litigants “drawn into a public forum largely against their will” do not, *Time, Inc. v. Firestone*, 424 U.S. 448, 450-52, 457 (1976). Similarly, while the *names* of crime victims, *Fla. Star*, 491 U.S. at 536-37, and accused individuals, *Daily Mail*, 443 U.S. at 103; *Bowley v. City of Uniontown Police Dep’t*, 404 F.3d 783, 787-88 (3d Cir. 2005), are often of public concern, their addresses or phone numbers presumably are not, *see Trans Union Corp.*, 267 F.3d at 1140.

Here, a covered person’s home address and phone number are virtually never of public concern. Absent unusual circumstances, whether Officer Smith lives at 123 Main Street or 456 Broad Street has no bearing on anyone’s ability participate in self-government. *See Cox*, 420 U.S. at 492. And while the NJAG agrees that the *city and state* of a covered person’s residence will sometimes be “necessary for public oversight,” Br.51, New Jersey courts have already (correctly) agreed that Daniel’s Law does not regulate city-and-state information at all, *see Kratovil v. City of New Brunswick*, No. A-0216-23, 2024 WL 1826867, at *5 (N.J. Super. Ct. App. Div. Apr. 26, 2024)—just as no one would say that Jalen Hurts’s “home address” is “Philadelphia.” In short, a covered person’s precise address or phone number is seldom a matter of public concern. JA109.

Nor do *Sheehan*, 272 F. Supp. 2d 1135, or *Brayshaw*, 709 F. Supp. 2d 1244, compel a different conclusion. Br.51. Both involved posting police officers' information on websites discussing police accountability and the difficulty of serving process or subpoenas on officers. *See Sheehan*, 272 F. Supp. 2d at 1139 n.2; *Brayshaw*, 709 F. Supp. 2d at 1249. Even assuming *arguendo* that those decisions correctly applied the public-concern test, this is a facial challenge, and the mine-run applications are to businesses disclosing myriad addresses with no nexus to "legitimate news interest" or "value and concern to the public." *See Snyder*, 562 U.S. at 453; *see supra* at 36-37.

Appellants are also misguided in arguing that because home addresses and phone numbers are publicly available by default, the State has placed the information "in the public domain," so it "must be presumed to have concluded that the public interest was thereby being served." Br.49-50. To be sure, in *Cox*, the Court concluded that because the State made a victim's name available in an indictment, "the State must be presumed to have concluded that the public interest was thereby being served." 420 U.S. at 495; *see also Fla. Star*, 491 U.S. at 538 (including victim's name in "an incident report made available in a pressroom" served to "undercut" State's policy against disclosing rape victims' identities). But that kind of case-specific, public-interest-by-estoppel theory is ill-suited to a statutory regime that leaves private individuals free to share home addresses and phone numbers

before a covered person requests nondisclosure. *See supra* at 9-11; *see also Ostergren*, 615 F.3d at 282-83 (distinguishing *Florida Star* cases as implicating a “conception of privacy” “predicated upon secrecy,” whereas statutes like Daniel’s Law involve a conception of privacy that “hinges upon [a person’s] control” of her information).

2. Daniel’s Law Is Not Facially Overinclusive.

Daniel’s Law’s substantive provisions reveal no facial overinclusivity. Judge Bartle also correctly predicted that New Jersey courts would construe the law to impose a negligence standard.

i. Daniel’s Law’s Substantive Provisions Sweep No Further Than Is Warranted.

To start, as an opt-in regime, Daniel’s Law leaves as much speech unregulated as possible, prohibiting disclosure only after an authorized person has “provide[d] written notice” and the recipient has had “10 business days” to comply. N.J. Stat. Ann. §56:8-166.1. Such opt-in mechanisms are a hallmark of narrow tailoring, as decisions involving do-not-call registries reflect. *See Mainstream Mktg.*, 358 F.3d at 1236-46 (upholding constitutionality of national “do-not-call” registry). Such mechanisms do “not over-regulate protected speech,” but rather tailor coverage to speech “targeted at unwilling recipients.” *Id.* at 1242 (“speech restrictions based on private choice ... are less restrictive than laws that prohibit speech directly”); *see also Rowan v. U.S. Post Off. Dep’t*, 397 U.S. 728, 738 (1970) (upholding similar law

allowing removal from mass-mailing lists); *Nat'l Fed'n of the Blind v. FTC*, 420 F.3d 331, 342 (4th Cir. 2005) (do-not-call provision was a “permissibly narrow means of protecting the home environment”); *cf. Martin v. City of Struthers*, 319 U.S. 141, 147-49 (1943) (ordinance prohibiting door-to-door canvassing could have been less restrictive by giving residents the option to prohibit visitors). Much like these permissible opt-in regimes, Daniel’s Law does not prohibit *any* disclosures unless a valid request has been received. Moreover, by giving recipients ten business days to comply, N.J. Stat. Ann. §56:8-166.1(a)(1), Daniel’s Law affords more time than other, similar laws, *see supra* at 11 n.1.

The law also prohibits disclosure to others but does not prevent continued possession. *See* N.J. Stat. Ann. §56:8-166.1(a) (restricting only “disclosure”); *Disclose*, Merriam-Webster.com (“to make known or reveal to another or to the public”). And while Appellants claim the law’s definition of “disclosure” is too broad, Br.26-27, they overlook that its scope is necessary to adequately advance the law’s interests. For example, if Daniel’s Law did not prohibit disseminating “addresses to businesses for use in marketing campaigns” or “to law firms to facilitate service of process,” Br.26, it would not achieve its goals as effectively. Indeed, the man who murdered Daniel Anderl was *himself* a lawyer. JA93, JA759.⁷

⁷ Moreover, nothing in the Rules of Civil Procedure requires that process be served at one’s home. *See* N.J.Ct.R. 4:4-3(a) (allowing service at workplace); Fed. R. Civ. P. 4(e)(1) (allowing service per state law).

Nor does “‘delivering’ addresses to businesses in connection with credit checks” and “transferring” an address or phone number “to a vendor” for shipping products, Br.26-27, run afoul of Daniel’s Law. In those hypotheticals, the covered person would have had to first send a nondisclosure request to the business *and then* either authorize a credit check or order a product to be shipped from the business. Such a request would naturally operate as a limited waiver of the nondisclosure request. Similarly, Appellants leave unclear why businesses would need to share addresses with third parties to prevent bank fraud. Br.26. But presumably, if a covered person sought to open a bank account, that person would supply the bank with their address—and the bank could ask that would-be customer to execute a waiver if some third-party verification were needed.⁸

Nor does Daniel’s Law’s lack of a verification process for private entities raise overinclusiveness problems. Br.29-30. To start, Appellants cite no case invalidating a statute for lack of verification in an opt-in mechanism. Further, nothing in Daniel’s Law prevents a business from using its own data to verify a request or seeking additional information from the requestor, and a claimant must still show that she is

⁸ That also explains why Daniel’s Law is not overinclusive for declining to include the exemptions provided in New Jersey’s Data Privacy Law (NJDPL), N.J. Stat. Ann. §§ 56:8-166.4 to -166.19. *Contra* CDIA.Br.18-19. The NJDPL gives consumers certain privacy rights, but the interests it protects are not identical. The Legislature validly concluded that Daniel’s Law would not adequately protect the safety of covered persons if it included the NJDPL’s exemptions.

a covered person and that a valid written request was received to prevail in a lawsuit. Moreover, if Appellants sought verification in good faith (e.g., difficulty distinguishing two John Smiths) and the requestor refused or failed to timely provide it, there could be valid statutory or as-applied defenses. *Cf., e.g., Borough of Princeton v. Bd. of Chosen Freeholders*, 777 A.2d 19, 32 (N.J. 2001) (discussing equitable defenses). But that is no basis for facial invalidation, where few applications will raise these factbound concerns.

Meanwhile, the State's own approval mechanism for requests seeking redaction of its own agencies' records exists for good reason: an approved request to a public entity will generally impact a person's rights, by limiting the notices and information she receives from the government. *See* N.J. Stat. Ann. §47:1B-2(d) (requiring requestors to affirm their understanding of these impacts). Given those unique impacts, it is reasonable for the State to expend resources reviewing those requests. But no authority suggests a State's decision not to subsize *industry's* compliance with a corresponding opt-in mechanism creates a tailoring problem.

The claim-assignment and liquidated-damages provisions do not present tailoring problems either. Br.30-31. On the former, claim-assignment is a recognized means of ensuring litigants can better vindicate their rights. *See, e.g., Vt. Agency of Nat. Res. v. U.S. ex rel. Stevens*, 529 U.S. 765, 771-78 (2000) (discussing *qui tam* actions). And properly understood, that choice has no First Amendment implications

at all: a provision expanding *who* can communicate a covered person’s request to invoke Daniel’s Law protections “impose[s] no more restrictions on the plaintiffs’ speech” than a statute without one. *See Free Speech Coal., Inc. v. Att’y Gen.*, 974 F.3d 408, 425 (3d Cir. 2020). In any event, as Judge Bartle observed, claim-assignments “make the enforcement more effective”—otherwise, “many covered persons may find” the process “too difficult, too cumbersome, or too expensive.” JA115. Rather than evincing a lack of tailoring, this provision permissibly advances the State’s compelling interests.

Appellants’ liquidated-damages argument is similarly misplaced. The numerical civil penalty a legislature chooses “is not a basis to decide” a law “could be less restrictive,” because (at least outside of fantastical hypotheticals) it has no bearing on what the law covers. *Free Speech Coal.*, 974 F.3d at 425; *see Fort Wayne Books, Inc. v. Indiana*, 489 U.S. 46, 59-60 (1989) (size of penalties not “significant” under First Amendment). Were it otherwise, States would have greater leeway to restrict protected speech simply by reducing the fines, and courts would be responsible for parsing the quantum of various penalty provisions. *Free Speech Coal.*, 974 F.3d at 425-26. By contrast, *Schrader* involved a threat of *criminal* prosecution—a difference in kind—on as-applied facts. 74 F.4th at 127. *Contra* Br.39. It did not overrule precedent that the First Amendment does not police the marginal dollar value assigned to civil violations, least of all on facial review.

Daniel’s Law is also not overinclusive based on its reference to “unpublished” home phone numbers. Br.31. To start, telephone directories still exist, and the concept of an unpublished number is well understood: it denotes a number that is not listed in a local directory. *E.g.*, Cal. Pub. Util. Code §2891.1(h). Moreover, the use of “unpublished” simply gives a defendant a potential statutory *defense*—if the person’s number is publicly listed, it is not covered by the law. That makes the law narrower, not broader.

ii. Daniel’s Law Imposes A Negligence Standard.

Daniel’s Law is also not overbroad on scienter grounds, as the New Jersey Supreme Court would likely conclude (as Judge Bartle predicted) that it operates as a negligent-disclosure law. *See* JA119-20. Background state-law principles, as well as the law’s text, structure, context, and purpose, all confirm as much.

New Jersey courts embrace a strong presumption “that the legislature intended to act in a constitutional manner,” and thus, whenever possible, construe a statute “to conform to the Constitution.” *State v. Burkert*, 174 A.3d 987, 998 (N.J. 2017). Where a law has two potential meanings—“a narrow one” that would pass muster “and a broader one that raises serious constitutional issues”—New Jersey law requires that courts adopt the narrower one. *State v. Carter*, 255 A.3d 1139, 1156-57 (N.J. 2021); *see also N.J. Republican State Comm. v. Murphy*, 236 A.3d 898, 907-08 (N.J. 2020). Indeed, “[w]hen necessary,” New Jersey courts “have engaged

in ‘judicial surgery’ to save an enactment that otherwise would be constitutionally doomed.” *State v. Natale*, 878 A.2d 724, 740 (N.J. 2005); *see also, e.g., State v. Comer*, 266 A.3d 374, 399 (N.J. 2022) (“add[ing]” a statutory provision to cure a constitutional infirmity because “the Legislature would want the law to survive”). Employing these interpretive tools, the New Jersey Supreme Court would likely conclude that Daniel’s Law’s civil provision codifies a negligent-disclosure tort.

Start with the law’s text and structure. As noted, Daniel’s Law created an opt-in regime: it requires valid “written notice,” “recei[ved]” by the entity, which has ten business days to comply. N.J. Stat. Ann. §56:8-166.1(a). In other words, the Legislature did not want entities held responsible for disclosures they could not have reasonably avoided—such as where they lacked valid “notice,” or were not given sufficient time to comply. That regime accords with background principles of negligence law: it articulates a standard of care, in the form of a duty to avoid dissemination when put on notice of a risk and given time to mitigate it. *See* Restatement (Second) of Torts §282 (1965). And the law requires recklessness to impose punitive damages. N.J. Stat. Ann. §56:8-166.1(c)(2). Together, that structural evidence strongly supports that the Legislature intended to require negligence for basic liability.

Statutory history confirms as much. Since its precursor statute was enacted in 2015, Daniel’s Law has provided for criminal liability upon purposeful or reckless

conduct, *id.* §2C:20-31.1 (2016), but allowed civil remedies for negligent conduct, *id.* §56:8-166.1 (2016). The current version retains that architecture, and there is no indication in either statutory or legislative history that the Legislature intended to abandon it—least of all to invite obvious constitutional concerns by imposing strict liability. *Cf. Burkert*, 174 A.3d at 998 (strong presumption “the legislature intended to act in a constitutional manner”).

Background tort principles also bolster that conclusion that Daniel’s Law requires at least negligence. As Judge Bartle acknowledged, “the New Jersey Supreme Court has explained that recovery for this tort requires proof of ‘the *unreasonable* publication of private facts.’” JA119-20 (quoting *Romaine v. Kallinger*, 537 A.2d 284, 291 (N.J. 1988)) (emphasis added). Other States’ courts have confirmed this tort can be committed negligently, *see, e.g., Z.D. v. Cmty. Health Network, Inc.*, 217 N.E.3d 527, 533-34 (Ind. 2023), and legislatures, like New Jersey’s, have drawn on this tradition in enacting statutory protections, enforceable via negligence law, to protect sensitive information, *see O’Donnell v. United States*, 891 F.2d 1079, 1085-86 (3d Cir. 1989) (Pennsylvania negligent-disclosure claim protecting psychiatric records). By contrast, the limited areas of tort law in which strict liability applies are those in which special deterrence is needed—whether because reasonable care is insufficient (as with ultrahazardous activities or abnormally dangerous animals), *see* Restatement (Second) of Torts §§ 509, 519

(1977), or, for products liability, where a manufacturer is best situated to avoid the harm, *see Suter v. San Angelo Foundry & Mach. Co.*, 406 A.2d 140, 151 (N.J. 1979). Neither rationale fits with Daniel’s Law, reinforcing the unlikelihood that the Legislature sought to inject strict liability here.

That “matters of public record” are not typically subject to this established tort is not to the contrary. Br.45-46. At a basic level, that information can potentially be *found* in public documents is not dispositive, or else SSNs and protected health information, if ever inadvertently made accessible, would be fair game for all time. *But see Ostergren*, 615 F.3d at 282-83 (explaining why this is not the case). Further, while most individuals’ addresses are not especially sensitive, that is because most individuals are less likely to be victimized by targeted violence and harassment at home. But some are, which is why laws in New Jersey and elsewhere have protected such individuals’ data. *Supra* at 11. In these circumstances, the individual’s home address *is* “actually private.” *See Romaine*, 537 A.2d at 292.

Appellants’ two New Jersey Supreme Court cases are likewise inapposite. First, their reliance on *State v. Pomianek*, 110 A.3d 841 (N.J. 2015), is misplaced, because *Pomianek* involved a challenge to a bias-intimidation statute in which criminal liability turned on whether the *victim* of the allegedly biased remarks “reasonably believed” the defendant was motivated by racial bias. *Id.* at 843 (citation omitted). Even leaving aside the more stringent approach that New Jersey courts

apply when criminal liability is at stake, *State v. Maldonado*, 645 A.2d 1165, 1178 (N.J. 1994), that unusual statutory focus “on the victim’s, not the defendant’s, state of mind,” *Pomianek*, 110 A.3d at 843, is easily distinguished from this case, which simply asks what state of mind of the *defendant* triggers civil liability.⁹ And *Usachenok v. Department of the Treasury*, 313 A.3d 53 (N.J. 2024), is even further afield. There, the Court relied on the State Constitution to deem invalidate an outdated regulation that had once directed State investigators undertaking employment-discrimination investigations to “request” that interviewees “not discuss any aspect of the investigation with others,” and had stated that “[f]ailure to comply” could “result in administrative and/or disciplinary action.” *Id.* at 56-58 (citation omitted). While the Court declined to engage in judicial surgery to save this already-superseded *regulation*, *id.* at 63, that sheds little light on the statutory circumstances here.

Appellants’ other objections also lack merit. To the extent Appellants rely on the phrases “shall be liable,” Br.52, and “shall award,” Br.58, each simply redirects to the question of what mental state the law requires to impose liability and award damages. Nor is there any inconsistency requiring negligence and “the harm the speech restriction seeks to prevent,” Br.59—the same harm befalls a covered person

⁹ Nor does *Pomaniek* undermine the robust state-law tradition of remedial construction, including those more recent decisions cited above.

regardless of whether a disseminator is purposely or negligently sharing their information. Finally, Appellants' repeated references to preventing "self-censorship" ring hollow. *E.g.*, Br.53, 55. First Amendment doctrine enforces mental-state requirements in order to "provide[] breathing room for more valuable speech." *Counterman v. Colorado*, 600 U.S. 66, 75 (2023). But that need is hardly acute where, as here, few if any conceivable applications involve expressive speech. *See supra* at 30. In any event, Appellants' concern assumes an overly strict construction of the statute; a company denied sufficient information by a requestor may well have a valid statutory (or equitable) defense that valid "notice" was not "received" in the first place. *See supra* at 41.

Finally, even if this Court *were* to read Daniel's Law to impose strict liability, facial invalidation would be inappropriate. Rather than invalidate entire statutes, courts prefer "to enjoin only the unconstitutional applications." *Ayotte v. Planned Parenthood of N. New Eng.*, 546 U.S. 320, 328-29 (2006); *see also* N.J. Stat. Ann. §1:1-10 (mandating severance to greatest extent possible); *Barr*, 591 U.S. at 630, 636 (severing TCPA provision exempting government-debt robocalls). While that might require confirming that Appellants are entitled to argue to a factfinder that they were not negligent in any alleged violations, it would not justify invalidating

the law’s substantive requirements, nor its punitive-damages provision that undisputedly effectuates them through a recklessness requirement.¹⁰

3. Daniel’s Law Is Not Facially Underinclusive.

Appellants’ underinclusiveness arguments are also unavailing. To start, “the First Amendment imposes no freestanding underinclusiveness limitation.” *Williams-Yulee v. Fla. Bar*, 575 U.S. 433, 449 (2015). So a “[s]tate need not address all aspects of a problem in one fell swoop”; instead, the Legislature “may focus on their most pressing concerns,” and the Court has often “upheld laws—even under strict scrutiny—that conceivably could have restricted even greater amounts of speech in service of their stated interests.” *Id.*; *see also Mainstream Mktg.*, 358 F.3d at 1240 (calling underinclusiveness argument against do-not-call registry “difficult to fathom”). Instead, underinclusiveness primarily applies when a statute’s glaring omissions suggest that the State’s motive was really targeting disfavored speech. *See id.* at 1238-39; *cf. Sorrell*, 564 U.S. at 573-75 (invalidating regime that did little to protect confidentiality outside “a narrow class of disfavored speakers”). As Judge Bartle correctly held, Appellants’ critiques do not come close to this high bar.

First, Appellants are wrong that the availability of certain address information through non-mortgage encumbrance-related documents such as mechanic’s liens,

¹⁰ Appellants’ other quibbles with features like unpublished home phone numbers, claim-assignment, and liquidated damages are also at most arguments for severance, not facial invalidation.

N.J. Stat. Ann. §47:1B-3(a)(4)(d), somehow precludes covered persons from asking private entities to stop disseminating this information. Br.32-33. As noted, the *Florida Star* line of cases reflect the proposition that when the government itself suggests something is newsworthy, it can seldom tell a speaker otherwise. *See supra* at 27-29; *see also Ostergren*, 615 F.3d at 282-83 (distinguishing such cases from cases involving personal information like SSNs). But New Jersey has naturally never suggested that every non-mortgage lien is a matter of public importance. Further, this exception is extremely narrow, less commonly applicable, and reflects countervailing realities of these types of encumbrances—whereas the more common form of real-estate encumbrance (a home mortgage), *is* subject to redaction. N.J. Stat. Ann. §47:1B-3(a)(2); *see id.* §46:26A-2(e)-(f).¹¹ This limited exception in no way suggests the State is insufficiently committed to Daniel’s Law’s objectives.

Second, that Daniel’s Law does not require claimants first to seek redaction of public agencies’ records does not render it underinclusive. Br.34. There is a “vast difference” between easily accessible information on open websites and the possibility of finding information through a “diligent search” of government files. *RCFP*, 489 U.S. at 764; *see also Advance Mag.*, 210 F. Supp. 3d at 601 (rejecting underinclusiveness for PPPA). And Daniel’s Law would not serve its interests as

¹¹ Further, because non-mortgage liens are available only through county-by-county platforms, they are more difficult to locate (if they exist at all).

well if covered persons, who might face imminent threats, were precluded from obtaining relief from the entities whose dissemination they judged most concerning simply because they had not yet obtained OIP's approval.

Nor are Appellants' cited cases to the contrary. Br.34. The statute in *Publius v. Boyer-Vine*, 237 F. Supp. 3d 997, 1020-21 (E.D. Cal. 2017), was deemed underinclusive because it prohibited dissemination only on the Internet. And the statutes in *Brayshaw*, 709 F. Supp. 2d at 1250, and *Sheehan*, 272 F. Supp. 2d at 1147, were deemed underinclusive because they prohibited disclosing such information "with the intent to harm or intimidate" and not by, for example, for-profit commercial entities without such intent. Here, New Jersey properly *covered* such applications, in order to properly serve its compelling interests.

Finally, that covered persons may disclose their own information after invoking Daniel's Law's protections is no defect. Br.34-35. The point of Daniel's Law is to allow covered persons to take control of their *own* information, recognizing that they are best situated to weigh the risks. *See* N.J. Stat. Ann. §56:8-166.1(a); *see also Ostergren*, 615 F.3d at 282-83. That a covered person may wish to ask data brokers on the Internet to take down her address in no way forecloses her from disclosing this information to select individuals as needed—whether to open a credit card, register her child for school, or host a birthday party. In short, Daniel's Law is a sensible privacy statute, not a vow of solitude, and Appellants offer no reason a

covered person’s own selective disclosures present the risks associated with widespread dissemination by private entities.¹² The law is not underinclusive.

B. For Similar Reasons, Daniel’s Law Satisfies Facial Intermediate Scrutiny, Whether Under *Central Hudson* Or The Standard Test.

1. Start with *Central Hudson*. That four-part test begins with a threshold question: whether the speech at issue [1] “is misleading or concerns illegal activity.” *Bank of Hope v. Miye Chon*, 938 F.3d 389, 395 (3d Cir. 2019). If so, the inquiry ends; if it is not, “the restriction must satisfy three more prongs to survive”: there must be a substantial government interest; “the restriction must directly advance that interest”; and “the restriction must be no broader than necessary.” *Id.* The NJAG does not claim the threshold filter applies, and Appellants do not dispute that the first of the three remaining prongs is met. The final two prongs are also easily met.

First, Daniel’s Law directly advances its substantial (indeed compelling) interest. To succeed on this prong, the State must show “that the harms it recites are real and that its restriction will in fact alleviate them to a material degree.” *Rubin v. Coors Brewing Co.*, 514 U.S. 476, 487 (1995). Here, the undeniably real harms, Br.25, are directly linked to the private information that Daniel’s Law empowers

¹² Nor do Appellants’ claims that the Legislature failed to articulate sufficient reasons for its 2023 amendments, Br.12, 38, 40, have any bearing on the law’s constitutionality. *See Turner Broad. Sys., Inc. v. FCC*, 520 U.S. 180, 213 (1997) (“Congress is not obligated, when enacting its statutes, to make a record of the type that an administrative agency or court does to accommodate judicial review.”).

covered persons to protect. Individuals are usually most vulnerable at home, and would-be wrongdoers therefore often seek the precise information Daniel’s Law regulates.¹³ The would-be assassin who targeted a federal judge in 2013, for instance, purchased the judge’s home address “on the internet for a mere \$1.95.” 166 Cong. Rec. 213 (2020). The man who murdered Judge Salas’s son is likewise believed to have used the Internet to find her address. JA759. Allowing covered persons to have this information taken down alleviates these threats “to a material degree.” *Rubin*, 514 U.S. at 487.

Second, Daniel’s Law is no broader than necessary to serve its interests. This prong does not require the “least restrictive alternative,” *Greater Phila. Chamber*, 949 F.3d at 140; rather, there need only be a “reasonable fit” between the end and the means, *Fox*, 492 U.S. at 480. Here, for essentially the reasons above, a reasonable fit is apparent: Daniel’s Law is a limited “opt-in” provision. *See supra* at 39-40. That speech-permissive default easily renders the law reasonable and proportional.

2. Daniel’s Law satisfies intermediate scrutiny for substantially the same reasons. *See S.F. Arts & Athletics, Inc. v. U.S. Olympic Comm.*, 483 U.S. 522, 537 n.16 (1987) (*Central Hudson* and intermediate scrutiny are “substantially similar”); *see also Turner*, 512 U.S. at 662 (intermediate scrutiny requires “an important or

¹³ Allowing covered persons to remove their home phone numbers similarly ameliorates threatening or harassing phone calls. *See* Federal Daniel’s Law §5932(a)(3).

substantial governmental interest ... unrelated to the suppression of free expression” and means that “do not burden substantially more speech than is necessary”). Here, too, the governmental interests are undisputed, Br.18, 25, and unrelated to suppressing free expression, *see supra* sections II.A, II.C, and the means chosen do not burden substantially more speech than necessary, *see supra* section III.A.2.

C. For Similar Reasons, Daniel’s Law Would Satisfy Even Strict Scrutiny.

Strict scrutiny requires “that the restriction furthers a compelling interest and is narrowly tailored to achieve that interest,” *Reed v. Town of Gilbert*, 576 U.S. 155, 171 (2015), and Appellants again concede that the State’s interests are “compelling,” Br.25. For the reasons already given, no less-restrictive means would serve Daniel’s Law’s compelling interests, because those alternatives would inevitably leave covered persons more vulnerable to harm, all in order to safeguard data with only marginal First Amendment value. *See supra* section III.A.

IV. In The Alternative, Certification Is Appropriate.

To the extent this Court has questions about how Daniel’s Law would be interpreted under New Jersey law or applicable state-law remedies, it should certify such questions to the Supreme Court of New Jersey. *See* N.J.Ct.R. 2:12A-1; *cf. Virginia v. Am. Booksellers Ass’n, Inc.*, 484 U.S. 383, 397 (1988) (certifying state-law questions). But because Judge Bartle properly denied Appellants’ facial motion, certification is not warranted.

CONCLUSION

This Court should affirm.

Respectfully submitted,

MATTHEW J. PLATKIN
ATTORNEY GENERAL OF NEW JERSEY

By: /s/ Michael L. Zuckerman
Michael L. Zuckerman (NJ Bar 427282022)
Michael.Zuckerman@njoag.gov
Deputy Solicitor General

Dated: May 12, 2025

COMBINED CERTIFICATIONS

I hereby certify that the following statements are true:

1. I am an attorney in good standing of the bar of the Third Circuit.
2. This brief complies with the typeface, type style and type-volume limitation requirements of Fed. R. App. P. 32(a)(5)-(7) because this brief has been prepared using 14-point type in Times New Roman, a proportionally spaced typeface, using Microsoft Word, and contains 12,999 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f).
3. The text of the paper copies that will be submitted are identical to the PDF version of this brief being filed electronically with the Court today.
4. Prior to this brief being electronically filed with the Court, it was scanned by MacAfee, Inc.'s Endpoint Security, version 10.7.0.3012, a virus-detection software, and found to be free from computer viruses. *See* L.A.R. 31.1(c).
5. On May 12, 2025, this brief was filed electronically with the Clerk of the United States Court of Appeals for the Third Circuit using the appellate CM/ECF system. Counsel for all parties are registered CM/ECF users and will be served via CM/ECF.

By: /s/ Michael L. Zuckerman
Michael L. Zuckerman
Deputy Solicitor General

Dated: May 12, 2025