IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. BLACKBAUD, INC., et al., Defendants.	Civ. Action No. 24-03993-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. WHITEPAGES, INC., et al., Defendants.	Civ. Action No. 24-03998-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. HIYA, INC., et al., Defendants.	Civ. Action No. 24-04000-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. WE INFORM, LLC et al., Defendants.	Civ. Action No. 24-04037-HB

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. INFOMATICS, LLC et al., Defendants.	Civ. Action No. 24-04041-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. THE PEOPLE SEARCHERS, LLC et al., Defendants.	Civ. Action No. 24-04045-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. COMMERCIAL REAL ESTATE EXCHANGE, INC., et al., Defendants.	Civ. Action No. 24-04073-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. DM GROUP, INC. et al., Defendants.	Civ. Action No. 24-04075-HB

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. CARCO GROUP INC., et al., Defendants.	Civ. Action No. 24-04077-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. DELUXE CORPORATION et al., Defendants.	Civ. Action No. 24-04080-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. TWILIO, INC., et al., Defendants.	Civ. Action No. 24-04095-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. DELVEPOINT, LLC et al., Defendants.	Civ. Action No. 24-04096-HB

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. QUANTARIUM ALLIANCE, LLC et al. Defendants.	Civ. Action No. 24-04098-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. YARDI SYSTEMS, INC. et al., Defendants.	Civ. Action No. 24-04103-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. 6SENSE INSIGHTS, INC., et al., Defendants.	Civ. Action No. 24-04104-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. LIGHTBOX PARENT, L.P., et al., Defendants.	Civ. Action No. 24-04105-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. SEARCH QUARRY, LLC, et al., Defendants.	Civ. Action No. 24-04106-HB

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. ACXIOM, LLC, et al., Defendants.	Civ. Action No. 24-04107-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. ENFORMION, et al., Defendants.	Civ. Action No. 24-04110-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. COSTAR GROUP, INC., et al., Defendants.	Civ. Action No. 24-04111-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. ORACLE INTERNATIONAL CORPORATION, et al., Defendants.	Civ. Action No. 24-04112-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. RED VIOLET, INC., et al., Defendants.	Civ. Action No. 24-04113-HB

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. RE/MAX, LLC, et al., Defendants.	Civ. Action No. 24-04114-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. DIGITAL SAFETY PRODUCTS, LLC, Defendants.	Civ. Action No. 24-04141-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. CIVIL DATA RESEARCH, Defendants.	Civ. Action No. 24-04143-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. SCALABLE COMMERCE, LLC et al., Defendants.	Civ. Action No. 24-04160-HB

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. EPSILON DATA MANAGEMENT, LLC, et al., Defendants.	Civ. Action No. 24-04168-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. PEOPLE DATA LABS, INC., et al., Defendants.	Civ. Action No. 24-04171-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. LABELS & LISTS, INC., Defendants.	Civ. Action No. 24-04174-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. CLARITAS, et al., Defendants.	Civ. Action No. 24-04175-HB

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. INNOVIS DATA SOLUTIONS INC. et al., Defendants.	Civ. Action No. 24-04176-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. ACCURATE APPEND, INC. et al., Defendants.	Civ. Action No. 24-04178-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. DATA AXLE, INC., et al., Defendants.	Civ. Action No. 24-04181-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. REMINE, INC., et al., Defendants.	Civ. Action No. 24-04182-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. LUSHA SYSTEMS, INC., et al., Defendants.	Civ. Action No. 24-04184-HB

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. TELTECH SYSTEMS, INC., et al., Defendants.	Civ. Action No. 24-04217-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. PEOPLECONNECT, INC., et al., Defendants.	Civ. Action No. 24-04227-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. CORELOGIC, INC., et al., Defendants.	Civ. Action No. 24-04230-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. BLACK KNIGHT TECHNOLOGIES, LLC, et al., Defendants.	Civ. Action No. 24-04233-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. ZILLOW, INC. et al., Defendants.	Civ. Action No. 24-04256-HB

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. EQUIMINE, INC., Defendants.	Civ. Action No. 24-04261-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. THOMSON REUTERS CORPORATION, et al., Defendants.	Civ. Action No. 24-04269-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. CHOREOGRAPH LLC, et al., Defendants.	Civ. Action No. 24-04271-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. TRANSUNION, LLC, et al., Defendants.	Civ. Action No. 24-04288-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. MELISSA DATA CORP. et al., Defendants.	Civ. Action No. 24-04292-HB

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. EQUIFAX, INC., et al., Defendants.	Civ. Action No. 24-04298-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. SPOKEO, INC., et al., Defendants.	Civ. Action No. 24-04299-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. RESTORATION OF AMERICA, Defendants.	Civ. Action No. 24-04324-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. i360, LLC et al., Defendants.	Civ. Action No. 24-04345-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. TELNYX LLC, et al., Defendants.	Civ. Action No. 24-04354-HB

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. GOHUNT, LLC et al., Defendants.	Civ. Action No. 24-04380-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. ACCUZIP, INC. et al., Defendants.	Civ. Action No. 24-04383-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. SYNAPTIX TECHNOLOGY, LLC et al., Defendants.	Civ. Action No. 24-04385-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. JOY ROCKWELL ENTERPRISES, INC. et al., Defendants.	Civ. Action No. 24-04389-HB

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. FORTNOFF FINANCIAL, LLC et al., Defendants.	Civ. Action No. 24-04390-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. MYHERITAGE, LTD, et al., Defendants.	Civ. Action No. 24-04392-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. E-MERGES.COM INC., Defendants.	Civ. Action No. 24-04434-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. WILAND, INC., et al., Defendants.	Civ. Action No. 24-04442-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. VALASSIS DIGITAL CORP., ET AL., et al., Defendants.	Civ. Action No. 24-04770-HB

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. ATDATA, LLC, et al., Defendants.	Civ. Action No. 24-04447-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. PRECISELY HOLDINGS, LLC, ET AL., et al., Defendants.	Civ. Action No. 24-04571-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. NUWBER, INC. et al., Defendants.	Civ. Action No. 24-04609-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. ROCKETREACH LLC et al., Defendants.	Civ. Action No. 24-04664-HB

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. OUTSIDE INTERACTIVE, INC., et al., Defendants.	Civ. Action No. 24-04696-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. THE LIFETIME VALUE CO. LLC, ET AL., et al., Defendants.	Civ. Action No. 24-04850-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. BELLES CAMP COMMUNICATIONS, INC. et al., Defendants.	Civ. Action No. 24-04949-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. FIRST AMERICAN FINANCIAL CORPORATION ET AL, et al., Defendants.	Civ. Action No. 24-05334-HB

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. PROPERTYRADAR, INC. et al., Defendants	Civ. Action No. 24-05596-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. THE ALESCO GROUP, L.L.C., Defendants	Civ. Action No. 24-05656-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. SEARCHBUG, INC., et al., Defendants	Civ. Action No. 24-05658-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. AMERILIST, INC.., Defendants	Civ. Action No. 24-05775-HB

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. LEXISNEXIS RISK DATA MANAGEMENT, LLC et al., Defendants	Civ. Action No. 24-06160-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. US DATA CORPORATION, et al., Defendants	Civ. Action No. 24-07324-HB
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. SMARTY LLC, et al., Defendants	Civ. Action No. 24-08075-HB

PLAINTIFFS' MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANTS' CONSOLIDATED MOTION TO DISMISS PLAINTIFFS' COMPLAINT

TABLE OF CONTENTS

TABLE OF AUTHORITIES iii

INTRODUCTION 1

BACKGROUND 3

Passage of Daniel's Law in New Jersey 3

Operation of Daniel's Law 3

Congress Passes Federal Daniel Anderl Judicial Security and Privacy Act in 2022 4

Defendants Concede That Daniel's Law Protects Against Actual Threats to Safety 5

LEGAL STANDARD 6

ARGUMENT 6

I. Defendants Cannot Establish Daniel's Law Is Unconstitutional in All Applications 6

II. The Data Regulated by Daniel's Law Is Not Speech 8

III. Daniel's Law Should Not Be Subject to Strict Scrutiny 10

A. Daniel's Law Is Not Content Based 11

B. Statutes Recognizing Privacy Torts Are Not Subject to Strict Scrutiny, Regardless of Whether They Are Content Based 13

1. The Supreme Court Has Rejected Strict Scrutiny for Privacy Torts 15

2. History and Tradition Show Daniel's Law Isn't Subject to Strict Scrutiny 17

C. Daniel's Law Has No Nexus with Viewpoint Discrimination 22

D. At Most, Daniel's Law Regulates Commercial Speech 25

IV. Daniel's Law Satisfies Any Standard of Review 26

A. Privacy Laws Have Repeatedly Survived First Amendment Challenges 26

B. Daniel's Law Is Neither "Overinclusive" Nor "Overbroad" 28

1. The definition of "disclose" further the interest of ensuring public official safety 28

2. The absence of a verification requirement does not render the statute overinclusive 32

3. The "liquidated damages" provision advances the interest Daniel's Law serves 33

C. Daniel's Law Is Not Underinclusive 33

D. Defendants Don't Actually Identify Less Restrictive Means 36

E. Defendants' Facial Vagueness Challenge Is Meritless 38

F. Daniel's Law Is Protected Under the Tenth Amendment 40

G. Regardless, Daniel's Law Meets the Strict Scrutiny Test Because Even Defendants Agree That It Protects Against The Occupational Hazards Faced by Covered Persons 40

CONCLUSION 42

TABLE OF AUTHORITIES

Page(s)

Cases

ACLU v. Clearview AI, Inc.,
2021 WL 4164452 (Ill. App. Ct. Aug. 27, 2021) 27

Americans for Prosperity Foundation v. Bonta,
594 U.S. 595 (2021) 7, 8, 28

B.V. v. Actavis, Inc.,
2016 WL 3027446 (D.N.J. May 26, 2016) 6

Barclift v. Keystone Credit Servs., LLC,
93 F.4th 136 (3d Cir. 2024) 13

Barr v. Am. Ass'n of Political Consultants,
591 U.S. 610 (2020) ..... passim

Bartnicki v. Vopper,
200 F.3d 109 (3d Cir. 1999) 15

Bartnicki v. Vopper,
532 U.S. 514 (2001) 16, 31

Boelter v. Hearst Commc'ns, Inc.,
192 F. Supp. 3d 427 (S.D.N.Y. 2016) 27

Bolger v. Youngs Drug Prod. Corp.,
463 U.S. 60 (1983) 25

Bowley v. City of Uniontown Police Dep't,
404 F.3d 783 (3d Cir. 2005) 16

Brayshaw v. City of Tallahassee,
709 F.Supp.2d 1244 (N.D. Fla. 2010) 12, 29

Brown v. Chemical Co.,
139 U.S. 540 (1891) 18

Burson v. Freeman,
504 U.S. 191 (1992) 17

Canessa v. J.I. Kislak, Inc.,

97 N.J. Super. 327 (Law Div. 1967) 14

Capra v. Thoroughbred Racing Ass'n of N. Am., Inc.,
787 F.2d 463 (9th Cir. 1986) 21, 41

Chicago v. Morales,
527 U.S. 41 (1999) 8

Christopherson v. Cinema Entertainment Corporation,
2024 WL 1120925 (D. Minn. Mar. 6, 2024) 27

Citizens for Health v. Leavitt,
428 F.3d 167 (3d Cir. 2005) 26

City of Austin v. Reagan Nat'l Advertising of Austin, LLC,
596 U.S. 61 (2022) 11, 12, 13, 18

Clark v. Community for Creative Non-Violence,
468 U.S. 288 (1984) 8

Corliss v. E.W. Walker Co.,
57 F. 434 (D. Mass. 1893) 19

Counterman v. Colorado,
600 U.S. 66 (2023) 41

Cox Broadcasting Corp. v. Cohn,
420 U.S. 469 (1975) 16

Crash Proof Retirement, LLC v. Price,
533 F.Supp.3d 227 (E.D. Pa. 2021) 25, 26

Davenport v. Washington Ed. Ass'n,
551 U.S. 177 (2007) 10, 22, 23, 24

Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.,
472 U.S. 749 (1985) 23, 27

Edison v. Edison Polyform Mfg. Co.,
73 N.J.Eq. 136 (N.J.Ch.1907) 19

Ettore v. Philco Television Broad. Corp.,
229 F.2d 481 (3d Cir. 1956) 14

Facenda v. N.F.L. Films, Inc.,
542 F.3d 1007 (3d Cir. 2008) 25

Florida Star v. B.J.F.,
491 U.S. 524 (1989) 15, 16

G.D. v. Kenny,
205 N.J. 275 (2011) 31

Goldstein v. Costco Wholesale Corp.,
559 F. Supp. 3d 1318 (S.D. Fla. 2021) 10

Greater Phila. Chamber of Com. v. City of Philadelphia,
949 F.3d 116 (3d Cir. 2020) 25

Gundy v. United States,
588 U.S. 128, (2019) 28

Hart v. Electronic Arts, Inc.,
717 F.3d 141 (3d Cir. 2013) 14, 29

Hedges v. United States,
404 F.3d 744 (3d Cir. 2005) 6

Hennessey v. Coastal Eagle Point Oil Co.,
129 N.J. 81 (1992) 15

Hill v. Colorado,
530 U.S. 703 (2000) 29, 40, 41

Holder v. Humanitarian Law Project,
561 U.S. 1 (2010) 38, 39

Hyde v. City of Columbia,
637 S.W.2d 251 (Mo. Ct. App. 1982) 21, 41

IMDb.com Inc. v. Becerra,
962 F.3d 1111 (9th Cir. 2020) 12

In re Google Inc. Cookie Placement Consumer Privacy Litig.,
806 F.3d 125 (3d Cir. 2015) 9, 11

In re Nickelodeon Consumer Privacy Litig.,
827 F.3d 262 (3d Cir. 2016) 14, 15

In re Zynga Privacy Litig.,
750 F.3d 1098 (9th Cir. 2014) 10, 11

Kellman v. Spokeo, Inc.,
599 F. Supp. 3d 877 (N.D. Cal. 2022) 27

Kratovil v. City of New Brunswick,
2024 WL 1826867 (App. Div. Apr. 26, 2024) 2, 21, 23

Krause v. Rocketreach,

561 F. Supp. 3d 778 (N.D. Ill. 2021) 20, 28

Landham v. Lewis Galoob Toys, Inc.,
227 F.3d 619 (6th Cir. 2000) 14

Los Angeles Police Dep't v. United Reporting Publishing,
Co., 528 U.S. 32 (1999) 24

M & R Marking Sys., Inc. v. Top Stamp, Inc.,
1996 WL 805485 (D.N.J. Nov. 20, 1996) 6

Marshall v. Klebanov,
188 N.J. 23 (2006) 31

Melo–Sonics Corp. v. Cropp,
342 F.2d 856 (3d Cir.1965) 6

Melvin v. Reid,
297 P. 91 (Cal. App. 1931) 18

Nat'l Coal. of Prayer, Inc. v. Carter,
455 F.3d 783 (7th Cir. 2006) 27

New York Times Co. v. Sullivan,
376 U.S. 254 (1964) 24

New York v. United States,
505 U.S. 144 (1992) 40

NFIB v. Sebelius,
567 U.S. 519 (2012) 40

Nixon v. Administrator of Gen. Servs.,
433 U.S. 425 (1977) 17

Ostergren v. Cuccinelli,
615 F.3d 263 (4th Cir. 2010) 12, 32

Paul P. v. Farmer,
227 F.3d 98 (3d Cir. 2000) 17, 29

Pavesich v. New England Life Ins. Co.,
50 S.E. 68 (Ga. 1905) 20

People v. Austin,
155 N.E.3d 439 (Ill. 2019) 22

Phillips v. Cnty. of Allegheny,
515 F.3d 224 (3d Cir. 2008) 6

Publius v. Boyer-Vine,
237 F.Supp.3d 997 (E.D. Cal. 2017) 12, 32

R.A.V. v. St. Paul,
505 U.S. 377 (1992) 22

Reed v. Town of Gilbert, Ariz.,
576 U.S. 155 (2015) 11, 12, 23

Rumsfeld v. Forum for Academic & Institutional Rights,
547 U.S. 47 (2006) 9

Sabri v. United States,
541 U.S. 600 (2004) 8

Saunders v. Hearst Television, Inc.,
2024 WL 126186 (D. Mass. January 11, 2024) 27

Schrader v. District Attorney of York Cnty.,
74 F.4th 120 (3d Cir. 2023) 16

Sheehan v. Gregoire,
272 F.Supp.2d 1135 (W.D. Wash. 2003) 12, 29, 32

Simon & Schuster, Inc. v. Members of N.Y. State Crime Victims Bd.,
502 U.S. 105 (1991) 22

Snyder v. Phelps,
562 U.S. 443 (2011) 21

Sorrell v. IMS Health Inc.,
564 U.S. 552 (2011) 12

Sosa v. Onfido, Inc.,
2022 WL 1211506 (N.D. Ill. 2022) 27

Spence v. Washington,
418 U.S. 405 (1974) 9

State v. Hoffman,
149 N.J. 564 (1997) 31

State v. VanBuren,
214 A.3d 791 (Vt. 2019) 15, 18

Sterling v. Borough of Minersville,
232 F.3d 190 (3d Cir. 2000) 17

Tenafly Eruv Ass'n, Inc. v. Borough of Tenafly,

309 F.3d 144 (3d Cir. 2002) 9

Tennessee Wine & Spirits Retailers Assoc. v. Thomas,
588 U.S. 504 (2019) 40

Time, Inc. v. Hill,
385 U.S. 374 (1967) 16, 31

Trans Union v. FTC,
267 F.3d 1138 (D.C. Cir. 2001) ..... passim

Troster v. Pennsylvania State Dep't of,
Corrs., 65 F.3d 1086 (3d Cir. 1995) 9

U.S. Healthcare, Inc. v. Blue Cross of Greater Phila.,
898 F.2d 914 (3d Cir. 1990) 25

U.S. West, Inc. v. F.C.C.,
182 F.3d 1224 (10th Cir. 1999) 26

United States Dep't of Justice v. Reporters Committee for Freedom of the Press,
489 U.S. 749 (1989) 21

United States v. Hansen,
599 U.S. 762 (2023) 1, 7

United States v. Marcavage,
609 F.3d 264 (3d Cir. 2010) 6

United States v. O'Brien,
391 U.S. 367 (1968) 9

United States v. Rahimi,
144 S. Ct. 1889 (2024) 1, 7

United States v. Salerno,
481 U.S. 739 (1987) 7

United States v. Williams,
553 U.S. 285 (2008) 38

Vanderbilt v. Mitchell,
67 A. 97 (N.J. App. 1907) 20

Vasil v. Kiip,
2018 WL 1156328 (N.D. Ill. Mar. 5, 2018) 10

Vidal v. Elster,
602 U.S. 286 (2024) ..... passim

Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc.,
455 U.S. 489 (1982) 39

Warnig v. Atlantic Cnty. Special Servs.,
363 N.J. Super. 563 (App. Div. 2003) 31

Washington State Grange v. Washington State Republican Party,
552 U.S. 442 (2008) 8

Williams-Yulee v. Florida Bar,
575 U.S. 433 ..... 18, 34, 35

Yale v. Clicktale,
2021 WL 1428400 (N.D. Cal. Apr. 15, 2021) 10

Zacchini v. Scripps-Howard Broadcasting Co.,
433 U.S. 562 (1977) 17

Statutes

18 U.S.C. § 1702 19

42 U.S.C. § 1320d-6 20

California Government Code § 7928.215(c) 37

N.J.S. § 47:1B-1(a) 21

N.J.S.A. § 19:31-18.1(c) 30

N.J.S.A. § 2C:20-31.1 3

N.J.S.A. § 47:1A-1 3

N.J.S.A. § 47:1B-1 4

N.J.S.A. § 47:1B-2(d) 35, 36

N.J.S.A. § 56:8-116.1(a)(2) 33

N.J.S.A. § 56:8-166.1 3

N.J.S.A. § 56:8-166.1(d) 25

N.J.S.A. § 56:8-166.1(d)(3) 4

Pub. L. 117–263 5

Rules

Fed. R. Civ. P. 12(b)(6) 6

Other Authorities

Access and Aggregation: Public Records, Privacy, and the Constitution,
86 Minn. L. Rev. 1176- (2002) 25

Assembly Bill No. 6167 4

Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet 50 (2000) 19

E. Bloustein, Privacy as an Aspect of Human Dignity,
39 N.Y.U. L. Rev. 962 (1964) 18

Natural Rights and the First Amendment,
127 Yale L.J. 246 (2017) 19, 20

P.L. 2020 3

Privacy's Other Path: Recovering the Law of Confidentiality,
96 Geo. L.J. 123 (2007) 18, 19

Reconciling Data Privacy and the First Amendment,
52 UCLA L. Rev. 1149 (2005) 10

Restatement (Second) of Torts §652A 14

Restatement (Second) of Torts §652D 13

The Boundaries of the First Amendment: A Preliminary Exploration of Constitutional Salience,
117 Harv. L. Rev. 1765 (2004) 24

The Right to Privacy,
4 Harv. L. Rev. 193 (1890) 18, 20

W. Prosser, Privacy,
48 Cal. L. Rev. 383 (1960) 18

INTRODUCTION

To prevail on a facial challenge, Plaintiffs need only show that Daniel's Law "is constitutional in some of its applications." *United States v. Rahimi*, 144 S. Ct. 1889, 1898 (2024). Because "litigants typically lack standing to assert the constitutional rights of third parties," *United States v. Hansen*, 599 U.S. 762, 769 (2023), a facial challenge cannot succeed if "the provision is constitutional as applied to" the Defendants' "own case." *Rahimi*, 144 S. Ct. at 1898. In other words, Defendants bear the high burden of demonstrating that Daniel's Law is unconstitutional in every one of its applications. *United States v. Rahimi*, 144 S. Ct. at 1889, 1898.

Defendants do not meet this initial burden for three separate reasons. First, the data regulated by Daniel's Law is not "speech" within the protection of the First Amendment. Second, even if that data could qualify as "speech" in every hypothetical circumstance (it cannot), the strict-scrutiny test does not apply because Daniel's Law is content-neutral and viewpoint-neutral; pursuant to the Supreme Court's guidance in *Vidal v. Elster*, 602 U.S. 286 (2024), itself built on decades of jurisprudence holding that such a law need not pass strict scrutiny. Third, even if the statute is deemed content-based, per *Vidal*, Daniel's Law is constitutional because it follows a longstanding tradition of coexistence between privacy rights and First Amendment rights.

In any event, if this Court were to subject Daniel's Law to strict scrutiny (or intermediate scrutiny for commercial speech), the law would readily pass the test, because, as Defendants have always conceded, the law protects judges, prosecutors, law enforcement, and their families from the significant hazards created as a result of their public-service jobs. Indeed, the strength of Daniel's Law is in its simplicity, underpinned by the Tenth Amendment of the U.S. Constitution which allows the State of New Jersey to exercise its own police power—including ensuring the safety of those public servants covered by the law. Critically, Defendants offered no less restrictive

means to advance the same compelling interests they themselves admit are served by Daniel's Law. As a result, Defendants' collective facial challenge fails.

Indeed, in open Court and through correspondence, Defendants repeatedly concur that Daniel's Law was passed to protect the safety of public servants and their families who, as the proposed amici directly attest to, admittedly remain constant targets of criminal threats, harassment, doxing, swatting, physical assaults, and assassinations. These concessions, coupled with Defendants' inability to proffer a narrower solution addressing these grave risks, show there is no real dispute that Daniel's Law facially passes any scrutiny that may apply.

Facing all of these obstacles to their First Amendment challenge, Defendants resort to outlandish hypotheticals. But such hypotheticals are not salient in a facial challenge. In one example, Defendants suggest that street addresses may actually be "newsworthy." Rejecting a constitutional challenge to Daniel's Law based on that very premise, the Court in *Kratovil v. City of New Brunswick* found that the specific street address of a judge or police officer is seldom of any real interest unless someone was trying to carry out a physical attack. *See* 2024 WL 1826867, at *6 (App. Div. Apr. 26, 2024) ("the publication of the town where Caputo lived was a matter of public concern, but Caputo's specific street address was not"). A facial challenge requires meeting a much higher burden, which Defendants have not and cannot satisfy.

Notably, Defendants fail to inform the Court that similar privacy laws have repeatedly survived First Amendment challenges, including before the Supreme Court. In pronouncing the Telephone Consumer Privacy Act (TCPA) constitutional against a similar First Amendment challenge, Justice Kavanaugh stated that "Congress found that banning robocalls was 'the only effective means of protecting telephone consumers from this nuisance and privacy violation' (internal citations omitted)." *Barr v. Am. Ass'n of Political Consultants*, 591 U.S. 610, 615 (2020).

Here, Defendants agree with the New Jersey Legislature that Daniel's Law was passed to protect the safety of Covered Persons, an even more compelling public interest than such a "nuisance."

BACKGROUND

Passage of Daniel's Law in New Jersey

In July 2020, the 20-year-old son of a sitting New Jersey Federal Judge was murdered at the front door of the family's New Jersey home by a gunman posing as a FedEx delivery man. Complaint at ¶5.[1] Authorities later found that the murderer had certain political and personal grievances against the Judge and went to her home that day intending to kill her. *Id.* at ¶6. Instead, he murdered the Judge's son and critically wounded her husband. *Id.*

Investigators eventually connected this attack with the prior shooting of an attorney in California who was slain while answering his front door to pick up a supposed package from the same disguised gunman. Authorities concluded that the shooter was disgruntled over legal cases with similar political and legal issues to what was pending before the Judge in New Jersey. Critically, the murderer found the home addresses of his targets through various Internet people finder resources; the same kind of data broker services offered by the Defendants. *Id.* at ¶7.

In response to this horrific shooting, the State of New Jersey enacted "Daniel's Law" in November 2020 (P.L. 2020, c. 125 *codified in* N.J.S.A. 47:1A-1, et seq., N.J.S.A 56:8-166.1 and N.J.S.A. 2C:20-31.1), to protect current and former judges, prosecutors, law enforcement officers, and their family members (defined thereunder as "Covered Persons").

Operation of Daniel's Law

[1] Citations to the Defendants' Consolidated Motion to Dismiss will refer to the ECF No. 27 in *Atlas Data Privacy Corporation, et al v. Lightbox Parent, L.P., et al*,, Civil Action No. 24-4105 (HB), which is where Defendants filed their consolidated motion. Because Defendants' motion cites to the Complaint that Plaintiffs filed against Blackbaud, we will do the same with references to the Complaint in our opposition. This Complaint is available as ECF 1-1 in *Atlas Data Privacy Corporation, et al v. Blackbaud, Inc., et al*, Civil Action No. 24-3993 (HB).

Any Covered Person may request that a data broker not "solicit, sell, manufacture, give, provide, lend, trade, mail, deliver, transfer, post, publish, distribute, circulate, disseminate, present, exhibit, advertise or offer . . . [which] shall include making available or viewable within a searchable list or database, regardless of whether a search of such list or database is actually performed." N.J.S.A. 56:8-166.1(d)(3). The home address and phone number of the Covered Person must cease to be disclosed within 10 business days of a request being made. *Id.* at (a)(1).

Other than this narrow prohibition on disclosing a Covered Person's home address and phone number, the data broker industry is left undisturbed. Not one Defendant has articulated how Daniel's Law prohibits any Defendant from otherwise carrying on with its business.

Notably, Daniel's Law also allows Covered Persons to redact their home address and phone number from the records of New Jersey government agencies, by submitting a request for redaction to the Office of Information Privacy. *See e.g.* N.J.S.A 47:1B-1, *et seq.* In other words, insofar as New Jersey law previously required home address and phone number as part of any official records, Daniel's Law allowed Covered Persons to remove that information from public disclosure. *Id.*; *see also* Senate Judiciary Committee Statement, Statement to Assembly Bill No. 6167, at 2 (Jan. 6, 2022).

Congress Passes Federal Daniel Anderl Judicial Security and Privacy Act in 2022

Following the actions taken by the State of New Jersey, the Judicial Conference of the United States (among others) proposed and supported a federal version of Daniel's Law. This similar federal bill, which had broad bipartisan support, applied to federal judges and their family members. It protected an enumerated list of personal information, including but not limited to home addresses and phone numbers, from unwanted disclosure by data brokers. It also allowed federal judges to redact their personal information displayed on federal government websites.

Judge Roslynn Mauskopf, then Director of the Administrative Office of the Courts, noted in a formal statement of support that these protections "further a compelling government interest – the safety of federal judges and the derivative ability of the judiciary to function." The bill passed as the Daniel Anderl Judicial Security and Privacy Act. Pub. L. 117–263, div. E, title LIX, subtitle D, Dec. 23, 2022, 136 Stat. 3458. Chief Justice John G. Roberts Jr., writing in his 2022 Year-End Report, recognized Congress for passing the bill noting that "a judicial system cannot and should not live in fear." *See* Chief Justice John Roberts, 2022 Year-End Report on the Federal Judiciary at 4, (December 31, 2022), available at https://www.supremecourt.gov/publicinfo/year-end/2022year-endreport.pdf.

Defendants Concede That Daniel's Law Protects Against Actual Threats to Safety

Defendants conceded again and again before this Court that New Jersey's Daniel's Law was passed to protect the legitimate "security interests" of Covered Persons:

- At the April 18, 2024 initial status hearing, lead counsel speaking on behalf of all Defendants, stated: "Everyone in this courtroom understands the noble intent of Daniel's Law. ***It's to protect the privacy and safety of public servants***." Transcript p. 26:22-24 (emphasis added). None of the other dozens of defense counsel present disagreed.
- At that hearing, another lead defense counsel stated: "I don't think anyone here is wanting to, despite Daniel's Law, publish the addresses and phone numbers of New Jersey judges, police officers and prosecutors . . . ***we all want to suppress that information***." *Id. at* 88:20-88:6 (emphasis added). Again, not one defendant disagreed.
- At the June 3, 2024 status hearing, that same lead attorney went further, stating: "[t]he Legislature's articulated interest ***is actually safety***. I just wanted to make that clear on the

record . . . ***It's the safety interest***, Your Honor." Transcript 91:1-8 (emphasis added). As before, not one defendant disagreed.

These statements reflect that Defendants fail to contest that Daniel's Law advances a compelling interest, while failing also to offer this Court a narrower way to advance that same interest.

LEGAL STANDARD

"As the long-established federal policy of civil litigation is to decide cases on the proofs, the district courts generally disfavor Rule 12(b)(6) motions." *M & R Marking Sys., Inc. v. Top Stamp, Inc*., 1996 WL 805485, at *5 (D.N.J. Nov. 20, 1996) (citing, *inter alia*, *Melo–Sonics Corp. v. Cropp*, 342 F.2d 856 (3d Cir.1965)). In deciding a motion to dismiss under Fed. R. Civ. P. 12(b)(6), a court must "accept as true all factual allegations in the complaint and draw all inferences from the facts alleged in the light most favorable to the plaintiff, and determine whether, under any reasonable reading of the complaint, the plaintiff may be entitled to relief." *Phillips v. Cnty. of Allegheny*, 515 F.3d 224, 228, 231 (3d Cir. 2008). The moving party carries the burden of proving that no claim has been stated. *B.V. v. Actavis, Inc.,* 2016 WL 3027446, at *2 (D.N.J. May 26, 2016) (citing *Hedges v. United States*, 404 F.3d 744, 750 (3d Cir. 2005)).

ARGUMENT

I. Defendants Cannot Establish Daniel's Law Is Unconstitutional in All Applications

A defendant who seeks to challenge the constitutionality of a statute can do so as a facial attack or as-applied attack. A facial attack "tests a law's constitutionality based on its text alone and does not consider the facts or circumstances of a particular case." *United States v. Marcavage*, 609 F.3d 264, 273 (3d Cir. 2010). On the other hand, an as-applied challenge "does not contend that a law is unconstitutional as written but that its application to a particular person under particular circumstances deprived that person of a constitutional right." *Id*. Here, Defendants

challenge the facial validity of Daniel's Law. They argue that the "statute is facially unconstitutional" because it contains a broad definition of the term "disclose," imposes "liquidated damages" for failure to adhere to the compliance deadline, and levies less stringent nondisclosure requirements on public agencies. *See* Motion to Dismiss, ECF No. 27-33, at 1.

As the Supreme Court recently explained, a facial attack on the constitutional validity of a statute is "the 'most difficult challenge to mount successfully,' because it requires the challenging defendant to 'establish that no set of circumstances exists under which the Act would be valid.'" *United States v. Rahimi*, 144 S. Ct. 1889, 1898 (2024) (quoting *United States v. Salerno*, 481 U.S. 739, 745 (1987)). "[T]o prevail" against a facial attack, Plaintiffs need only show that Daniel's Law "is constitutional in some of its applications." *Id*. And because "litigants typically lack standing to assert the constitutional rights of third parties," *United States v. Hansen*, 599 U.S. 762, 769 (2023), a facial challenge cannot succeed if the provision "is constitutional as applied to" the Defendants' "own case." *Rahimi*, 144 S. Ct. at 1898.

The overbreadth doctrine recognizes "'a second type of facial challenge, whereby a law may be invalidated as overbroad if a substantial number of its applications are unconstitutional, judged in relation to the statue's plainly legitimate sweep." *Americans for Prosperity Foundation v. Bonta*, 594 U.S. 595, 615 (2021). Defendants never try to meet this burden, offering only hypotheticals and edge cases that effectively concede the statute is constitutional in most applications. The failure to even attempt to make this showing is compounded by Defendants' acknowledgement that the safety of public servants and their families is a serious concern that is best addressed by the prompt removal of their home addresses and phone numbers from Defendants' sites. April 18, 2024, Transcript p. 88:20-88:6 ("[W]e all want to suppress that information . . . [s]o the harm . . . is going to be addressed right away with this production that you

may order . . . ") (statement of Defendants' lead counsel to this Court).

Courts "disfavor[]" facial challenges for several important reasons. *Washington State Grange v. Washington State Republican Party*, 552 U.S. 442, 450 (2008). "Claims of facial invalidity often rest on speculation,'" which "raise[s] the risk of 'premature interpretation of statutes on the basis of factually barebones records.'" *Id*. (quoting *Sabri v. United States*, 541 U.S. 600, 609 (2004) (quotation marks omitted)). Such challenges also are "contrary to the fundamental principle of judicial restraint that courts should neither anticipate a question of constitutional law in advance of the necessity of deciding it nor formulate a rule of constitutional law broader than is required by the precise facts to which it is to be applied." *Id*. (quotation marks and citation omitted). Indeed, Justices have doubted whether courts even have "the power to pronounce that a statute is unconstitutional in all applications." *Americans for Prosperity Found. v. Bonta*, 594 U.S. 595, 621 (2021) (Thomas, J., concurring); *see also Chicago v. Morales*, 527 U.S. 41, 77 (1999) (Scalia, J., dissenting) ("[To] pronounce that the statute is unconstitutional in all applications [is] no more than an advisory opinion—which a federal court should never issue at all."). Finally, "facial challenges threaten to short circuit the democratic process by preventing laws embodying the will of the people from being implemented in a manner consistent with the Constitution." *Washington State Grange,* 552 U.S. at 450.

Defendants' facial challenge should be rejected.

II. The Data Regulated by Daniel's Law Is Not Speech

Absent hypothetical outliers, the moving papers set forth very few examples of how Daniel's Law actually regulates speech. Precedent defines "speech" as expressive activity "intended to be communicative" and, "in context, would reasonably be understood . . . to be communicative." *Clark v. Community for Creative Non-Violence*, 468 U.S. 288, 294 (1984); *see*

also Rumsfeld v. Forum for Academic & Institutional Rights, 547 U.S. 47, 65-66 (2006); *Spence v. Washington*, 418 U.S. 405, 410-11 (1974). The "putative speaker bears the burden of proving that his . . . content is expressive." *Tenafly Eruv Ass'n, Inc. v. Borough of Tenafly*, 309 F.3d 144, 161 (3d Cir. 2002). At minimum, a speaker must "have intended subjectively" to communicate a message to an "intended audience." *Id.* The speaker's activity only qualifies as "speech" if an objectively reasonable listener would understand the speaker to have communicated a "*message* (ideological or otherwise)." *Id.*; *see also Rumsfeld*, 547 U.S. at 65-66 (rejecting "the view that 'conduct can be labeled 'speech' whenever the person engaging in the conduct thereby intends to express an idea.'") (quoting *United States v. O'Brien*, 391 U.S. 367, 376 (1968)).

In many, if not most applications, Daniel's Law does not implicate, let alone restrict "speech." First, not everything that qualifies as a "disclosure" under Daniel's Law involves speech with a message or thought. To be sure, for example, a speaker can ***use*** an address or phone number in speech. But in and of itself, an address or phone number posted online or sold to a marketer is not a "message" or "thought" because it does not "*tell*[]" the audience "anything about the [poster's] beliefs." *Troster v. Pennsylvania State Dep't of Corrs.*, 65 F.3d 1086, 1092 (3d Cir. 1995) (citing P. Tiersma, *Nonverbal Communication and the Freedom of "Speech,"* Wis. L. Rev. 1525, 1554 & n.122 (1993)). Instead, such pure "fact[s]" are only "elements of speech." *Rumsfeld*, 547 US. at 61-62, which qualify for First Amendment protection only when a speaker gives them "an expressive or communicative 'use'" in a complete speech act intended to express the speaker's own message. *Troster*, 65 F.3d at 1092 (citing *Spence*, 418 U.S. at 410).

In analogous contexts and while defending against comparable lawsuits, the data broker industry has argued that home address and phone number data are not "communications." *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 136-37 (3d Cir. 2015)

("addressing information with respect to the delivery" not "communications" for the purposes of wiretap acts, which prohibit the interception of communications); *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1105-06 (9th Cir. 2014) (web addresses is equivalent to mail addresses, and therefore not contents of a communication for the purposes of the Electronic Communications Act); *Goldstein v. Costco Wholesale Corp.*, 559 F. Supp. 3d 1318, 1322 (S.D. Fla. 2021) (identifying and addressing information about a user not communications for the purposes of the ECPA); *Yale v. Clicktale*, 2021 WL 1428400 at *3 (N.D. Cal. Apr. 15, 2021) (user electronic address information not content of communications for California wiretap act); *Vasil v. Kiip*, 2018 WL 1156328 at *3 (N.D. Ill. Mar. 5, 2018) (holding same as to the Illinois wiretap act).[2] Data brokers should not be allowed to argue that information like addresses are not "communications" in one context, only to turn around and claim that addresses are protectable communications. Nor can their change of course alter the reality that the data at issue is not speech.

III. Daniel's Law Should Not Be Subject to Strict Scrutiny

Even if the Court finds that Daniel's Law affects some speech, Defendants' arguments still fail. **First**, Daniel's Law is not content based because it does not target "disclosures" based on the message or thought expressed, or the purpose of the disclosure. **Second**, Daniel's Law is a viewpoint-neutral statute that prohibits tortious conduct against privacy. Supreme Court precedent has consistently rejected the application of strict scrutiny to statutes creating such torts, and *Vidal v. Elster*, recently reaffirmed that viewpoint-neutral statutes that have a long history of coexistence with the First Amendment—such as those adopted to protect privacy interests—are never subject to strict scrutiny. **Third**, Daniel's Law carries no risk of viewpoint discrimination, and when "that risk is inconsequential . . . strict scrutiny is unwarranted." *Davenport v. Washington Ed. Ass'n*,

[2] N. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. Rev. 1149 (2005).

551 U.S. 177, 188 (2007); *see also Vidal*, 602 U.S. at 311-12 (Barrett, J., concurring). **Fourth**, many covered "disclosures" are (at most) commercial speech subject to intermediate scrutiny.

A. Daniel's Law Is Not Content Based

Content-based restrictions warrant strict scrutiny when they are facially content-based or are content-based in their practical operation. *City of Austin v. Reagan Nat'l Advertising of Austin, LLC*, 596 U.S. 61, 69, 76 (2022). Daniel's Law fits neither category. **First**, Facially, Daniel's Law does not target speech based on the topic discussed, idea conveyed, or message expressed. Instead, the statute applies to acts of "disclosure" that contain specific bits of data that when provided create a very real threat for the public servants and their families—leaving the rest of the output alone. But data is not the same thing as "communicative content." The "communicative content" of a speech act is the "topic discussed or an idea or message expressed." *City of Austin*, 596 U.S. at 69 (quotation marks and citation omitted). A disclosure simply listing the home address or phone number of a Covered Person does not "discuss" any "topic" or express a "substantive message." *Id.* at 71; *cf. In re Zynga Privacy Litigation*, 750 F.3d 1098, 1106-07 (9th Cir. 2014) (equating the "content" of a communication with its "substance" or "meaning"); *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125, 136-37 (3d Cir. 2015) (same).

Defendants ignore the Supreme Court's interpretation of *Reed v. Town of Gilbert, Ariz.*, 576 U.S. 155 (2015), in *City of Austin*, when they contend that "the hallmark of a content-based restriction" are statutes that "'ask[] what a person said' and depending on the answer, either allows or prohibits the speech.'" Motion to Dismiss, ECF No. 27-33, at 23 (citing *Reed*, 576 U.S. at 169). *City of Austin* explicitly rejected "the view that *any* examination of speech or expression inherently triggers heightened First Amendment concern." 596 U.S. 61, 73-74 (2022) (emphasis in original) (holding statute distinguishing between signs advertising on-site businesses from off-site business

was not content based). As *City of Austin* clarified, *Reed* was premised on "the First Amendment's hostility to content-based regulation" aimed at "particular viewpoints" or prohibition of "public discussion of an entire topic." 596 U.S. at 70 (internal alterations and quotations omitted). Tellingly, *Reed* deemed the subject regulation content-based because it singled out speech based on whether it "*conveys the message* of directing the public to church or some other 'qualifying event,'" and treated "the Church's signs inviting people to attend its worship services . . . differently from signs *conveying other types of ideas*." 576 U.S. at 164 (emphases added).

At most, Daniel's Law is content-based as applied to "disclosures" that communicate a speaker's own message, rather than simply regurgitating addresses and phone numbers. Some of Defendants' cases effectively concede as much, suggesting that regulation of data is content-based only when the data is "integral to [the speaker's] message." *Ostergren v. Cuccinelli*, 615 F.3d 263, 271 (4th Cir. 2010); *see also Sorrell v. IMS Health Inc.*, 564 U.S. 552, 564-65 (2011) (statute was content-based because it "disfavor[ed] marketing" in comparison to other "purposes and viewpoints"). Other cases cited by Defendants held that a statute is content-based if applying the statute "requires the examination" of the disclosure—precisely the test rejected by *City of Austin*. *See Sheehan v. Gregoire*, 272 F.Supp.2d 1135, 1146 (W.D. Wash. 2003); *Publius v. Boyer-Vine*, 237 F.Supp.3d 997, 1013 (E.D. Cal. 2017); *IMDb.com Inc. v. Becerra*, 962 F.3d 1111, 1120 (9th Cir. 2020). Others simply assumed that a statute prohibiting disclosure of names and addresses is facially content-based without explaining how such data in itself constitutes a topic or message. *See Brayshaw v. City of Tallahassee*, 709 F.Supp.2d 1244 (N.D. Fla. 2010). And here, Defendants proffer no instances when the home address or phone number of a Covered Person would actually be part of a message, other than those aimed toward carrying out some type of threat, act of violence or harassment targeted at the Covered Person and their family members.

Second, nothing in Daniel's Law suggests the Legislature intended to suppress substantive communications discussing any idea, directed at promoting or criticizing a particular "topic," or aimed at expressing any particular "message." *City of Austin*, 596 U.S. at 69. The statute simply seeks to strengthen protections against the undisputed dangers facing a Covered Person as a result of their public service, a noble but neutral goal of which even Defendants are supportive. Like the regulation at issue in *City of Austin*, Daniel's Law is "agnostic" about the substantive content or message expressed by the speaker. And "absent a content-based purpose or justification," a statute "is content neutral and does not warrant the application of strict scrutiny." *Id.* at 69.

B. Statutes Recognizing Privacy Torts Are Not Subject to Strict Scrutiny, Regardless of Whether They Are Content Based

Even if Daniel's Law were content based, strict scrutiny would not apply to virtually any of its applications. Supreme Court precedent recognizes that when a content-based restriction has a history of "longstanding coexistence . . . with the First Amendment," courts should not apply strict scrutiny. *Vidal v. Elster*, 602 U.S. at 288 (prohibiting trademarks of names of living individuals without consent was not subject to any scrutiny because of longstanding coexistence between right to control one's name and the First Amendment). Daniel's Law creates a tort closely related to three traditional privacy torts—public disclosure, misappropriation of name and likeness, and intrusion upon seclusion—which have long existed in harmony with the First Amendment.

First, the tort created by Daniel's Law closely resembles the "public disclosure of private information" tort recognized by virtually every state. This tort imposes liability on a defendant "when he 'gives publicity to a matter concerning the private life of another . . . if the matter publicized . . . (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.'" *Barclift v. Keystone Credit Servs., LLC*, 93 F.4th 136, 145 (3d Cir. 2024) (quoting Restatement (Second) of Torts §652D). Daniel's Law similarly targets "disclosures" that

give publicity to facts generally of no legitimate concern to the public, with the only differences being that Daniel's Law (i) is limited to two particular types of data; and (ii) provides a remedy to specific classes of Covered Persons who face special risks of being subjected to threats, violence, and harassment as a result of their public service.

Second, Daniel's Law protects the right to control one's name traditionally protected by the misappropriation-of-name-and-likeness tort. The economic value of prohibited disclosures are directly related to the use of the Covered Person's name, because it is impossible to sell someone's home address or phone number *as that person's home address or phone number*, without also using their name in the disclosure. The law in New Jersey and elsewhere has long recognized that "the right to exploit the value" of a person's name "belongs to the individual with whom it is associated, for an individual's name, likeness, and endorsement carry value and an unauthorized use harms the person both by diluting the value of the name and depriving that individual of compensation." *Hart v. Electronic Arts, Inc.*, 717 F.3d 141, 150 (3d Cir. 2013) ("right of publicity grew out of the right to privacy torts, specifically, from the tort of "invasion of privacy by appropriation."); *Landham v. Lewis Galoob Toys, Inc.*, 227 F.3d 619, 622, 626 (6th Cir. 2000); *Ettore v. Philco Television Broad. Corp.*, 229 F.2d 481, 491 (3d Cir. 1956); *Canessa v. J.I. Kislak, Inc.*, 97 N.J. Super. 327, 351 (Law Div. 1967) ("[P]laintiffs' names and likenesses belong to them. As such they are property."); Restatement (Second) of Torts §652A. Many acts of "disclosure" identified by the statute—such as "solicit," "sell," "manufacture," "lend," "trade,"—govern the potential appropriation of a Covered Person's home address and phone number.

Third, Daniel's Law protects the same interests as the "intrusion upon seclusion" tort, which involves "(i) an intentional intrusion (ii) upon the seclusion of another that is (iii) highly offensive to a reasonable person." *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 293

(3d Cir. 2016); *see also Hennessey v. Coastal Eagle Point Oil Co.*, 129 N.J. 81, 94-95 (1992). Liability for intrusion "arises when [the defendant] has intruded into a private place, or has otherwise invaded a private seclusion that the plaintiff has thrown about his person or affairs." *Nickelodeon*, 827 F.3d at 294. Preventing widespread publication of a Covered Person's home address and phone number makes it harder for third parties to intrude upon their private lives. And Daniel's Law allows Covered Persons to have their information redacted from public and commercial records to protect their seclusion by making that information harder to find. The demonstrated "longstanding coexistence" between the privacy torts created by statutes like Daniel's Law and the First Amendment forecloses the application of strict scrutiny.

1. The Supreme Court Has Rejected Strict Scrutiny for Privacy Torts

The Supreme Court has never suggested that privacy torts are facially unconstitutional or subject to strict scrutiny in all applications. To the contrary, the Court has repeatedly held that "the sensitivity and significance of the interests presented in clashes between [the] First Amendment and privacy rights counsel relying on limited principles that sweep no more broadly than the appropriate context of the instant case." *Florida Star v. B.J.F.*, 491 U.S. 524, 533 (1989); *State v. VanBuren*, 214 A.3d 791, 802 (Vt. 2019) ("[T]he Court has repeatedly reconciled the tension between the right to privacy and freedom of expression with an analysis of the specific privacy claims and the public interest in the communications at issue, rather than a broad ruling prioritizing one of these values over another."); *Trans Union v. FTC*, 267 F.3d 1138, 1140-41 (D.C. Cir. 2001) (similar). Citing "the Supreme Court's practice of narrowly circumscribing its holdings in this area," the Third Circuit insists that conflicts between the First Amendment and privacy must be decided "in light of the unique facts and circumstances", *Bartnicki v. Vopper*, 200 F.3d 109, 117 (3d Cir. 1999), and has never held a statute that imposes liability for publishing

lawfully obtained information facially invalid or even invalid *as applied* to speech on a matter of public concern when the statute "serves 'a need to further a state interest of the highest order.'" *Schrader v. District Attorney of York Cnty.*, 74 F.4th 120, 126 & 127-28 (3d Cir. 2023) (quoting *Smith*, 443 U.S. at 103); *see also Bowley v. City of Uniontown Police Dep't*, 404 F.3d 783, 788-89 (3d Cir. 2005) (same). Daniel's Law serves this exact purpose.

An unbroken line of Supreme Court precedent rejects the application of strict scrutiny as a facial matter in cases where privacy torts clash with the First Amendment. In *Time, Inc. v. Hill*, 385 U.S. 374 (1967), the Court's first case addressing privacy torts and the First Amendment, the Court held that the First Amendment requires a plaintiff asserting a "false light" claim against speech on a matter of public concern to prove that the defendant "published the report with knowledge of its falsity or with reckless disregard of the truth." *Id.* at 387-88. But the Court refused to hold the statute "unconstitutional on its face." *Id.* at 397. *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975), acknowledged that in the "collision between claims of privacy and those of the free press, the interests on both sides are plainly rooted in the traditions and significant concerns of our society," and thus "focus[ed] on the narrower interface between press and privacy that this case presents." *Id.* at 491. *Florida Star* again emphasized that courts should resolve conflicts "between the right which the First Amendment" protects and "the protections which various statutes and common-law doctrines accord to personal privacy against the publication of truthful information" only "in a discrete factual context." 491 U.S. at 530. *Bartnicki v. Vopper*, 532 U.S. 514 (2001), reiterated the Court's "repeated refusal to answer categorically" whether privacy restraints on "truthful publication" are "consistent with the First Amendment," and held only that the "privacy concerns" present on the facts of those cases were outweighed by "the interest in publishing matters of public importance." *Bartnicki*, 523 U.S. at 529 & 534.

For misappropriation of name and likeness, the Supreme Court has likewise held that "the First and Fourteenth Amendments do not immunize the media" from claims based on misappropriation "of a right of publicity existing under state law." *Zacchini v. Scripps-Howard Broadcasting Co.*, 433 U.S. 562, 574-75 (1977). Courts thus "must balance the interests underlying the right to free expression against the interests in protecting the right of publicity" in the context of a particular case. *Hart*, 717 F.3d at n. 47 (refraining from applying strict scrutiny to plaintiff's identity and likeness claim against defendant videogame manufacturer, finding that although "video games communicate ideas . . . and social messages, . . . the interest protected by the right of publicity . . . outweighs the Constitutional shield.").

This case-specific approach to conflicts between privacy and the First Amendment is necessary because privacy cases balance free speech against the constitutional interest "in avoiding disclosure of personal matters." *Nixon v. Administrator of Gen. Servs.*, 433 U.S. 425, 457 (1977); *Sterling v. Borough of Minersville*, 232 F.3d 190, 194 (3d Cir. 2000) ("[T]he constitutional right to privacy" protects "an individual's interest in avoiding divulgence of highly personal information."); *Paul P. v. Farmer*, 227 F.3d 98, 101 (3d Cir. 2000) (recognizing a constitutional "interest in one's home address by persons who do not wish it disclosed"). When "the exercise of free speech rights conflicts with another fundamental right," reasonable compromises "survive[] strict scrutiny." *Burson v. Freeman*, 504 U.S. 191, 211 (1992). That compromise is already embodied in existing precedent, which rejects any attempt to mechanically apply a test for content-based restrictions to Daniel's Law. By itself, this is enough to defeat Defendants' facial challenge.

2. History and Tradition Show Daniel's Law Isn't Subject to Strict Scrutiny

The Supreme Court's rejection of strict scrutiny for statutes recognizing privacy torts is supported by their long history of coexistence with the First Amendment. As the Supreme Court

has repeatedly held, "history and tradition" illuminate "the scope of the First Amendment." *Vidal*, 602 U.S. at 301; *see City of Austin*, 596 U.S. at 75 (citing an "unbroken tradition of on-/off-premises distinctions"); *Williams-Yulee v. Florida Bar*, 575 U.S. 433, 446 (2015 (recognizing "history and tradition" determines the scope of the First Amendment). Because such torts have "deep roots in our legal tradition," Daniel's Law is not subject to strict scrutiny, and its validity should only be evaluated through a case-specific assessment of the privacy and First Amendment interests at stake in a particular case. *Vidal*, 602 U.S. at 301; *see also VanBuren*, 214 A.3d at 802 (Vt. 2019) ("United States legal history supports the notion that states can regulate expression that invades individual privacy without running afoul of the First Amendment.").

With the rise of mass media in the late 19th century, contemporary common-law privacy torts began to crystallize into their current form, particularly after the publication of Samuel Warren and Justice Brandeis's famous article *The Right to Privacy*. S. Warren & L. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890). But "Warren and Brandeis did not invent the right to privacy from a negligible body of precedent . . . By 1890, a robust body of confidentiality law protecting private information from disclosure existed throughout the Anglo-American common law." N. Richards & D. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 Geo. L.J. 123, 125 (2007); *see* W. Prosser, *Privacy*, 48 Cal. L. Rev. 383 (1960) (collecting cases); E. Bloustein, *Privacy as an Aspect of Human Dignity*, 39 N.Y.U. L. Rev. 962 (1964) (same).

Since the time of the Founding, courts have held that "'[a] man's name is his own property, and he has the same right to its use and enjoyment as he has to that of any other species of property.'" *Vidal*, 602 U.S. at 301 (quoting *Brown v. Chemical Co.*, 139 U.S. 540, 544 (1891)). Common-law courts extended this principle to other misappropriations of another's identity and disclosures of private facts without consent. *See Melvin v. Reid*, 297 P. 91, 92 (Cal. App. 1931);

see also Yovatt v. Wingard, 1 J. & W. 394 (1820) (publication of recipes without consent) (cited by Brandeis & Warren, at 212); *Abernathy v. Hutchinson*, 3 L.J. Ch. 209 (1825) (publication of lectures) (cited by Brandeis & Warren, at 207-08); *Prince Albert v. Strange*, 2 De Gex. & Sm. 652 (1849) (publication of etchings) (cited by Brandeis & Warren, at 201-02, 204 & 208); *Tuck v. Priester*, 19 Q.B.D. 639 (1887) (cited by Brandeis & Warren, at 208); *Pollard v. Phot. Co.*, 40 Ch. Div. 345 (1888) (copying photographs of without consent) (cited by Brandeis & Warren, at 208-09); *Corliss v. E.W. Walker Co.*, 57 F. 434, 435-36 (D. Mass. 1893) (photograph); *Edison v. Edison Polyform Mfg. Co.*, 73 N.J.Eq. 136 (N.J.Ch.1907) (name or likeness of Thomas Edison).

Statutory protections for confidentiality likewise date back to the early Republic. *See* Richards & Solove, *Privacy's Other Path*, 96 Geo. L. J. at 139-142. In 1782, the Continental Congress passed a law to protect the confidentiality of letters. *See* Smith, *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet* 50 (2000). In 1825, well after the enactment of the First Amendment to the Constitution, Congress passed a law protecting the confidentiality of letters. Act of Mar. 3, 1825, ch.64, §22, 4 Stat. 102 (codified as amended at 18 U.S.C. §1702). In 1889, Congress enacted a law fining census officials $500 for disclosing confidential information. *See* Act of Mar. 1, 1889, ch. 319, §§ 8, 13, 25 Stat. 760, 763, 764.

The early cases developing the privacy torts were careful to reconcile privacy interests with free speech in accordance with the original meaning of the First Amendment. Under the original understanding, speech and press freedoms were "natural rights" that were "subject to restrictions under laws that promoted the public good" and that prevented interference "with the rights of others." J. Campbell, *Natural Rights and the First Amendment*, 127 Yale L.J. 246, 276-77 (2017). And because "the Founders recognized considerable underdeterminacy about what natural law required," courts relied on the methods of "the common law" to "determine the proper boundaries

of natural liberty." *Id.* at 291. Early cases developing privacy torts applied precisely this approach. For example, the leading case of *Pavesich v. New England Life Ins. Co.*, 50 S.E. 68 (Ga. 1905), employed "the common law" method of "judg[ing] according to the law of nature and the public good." *Id.* at 69; *see also Vanderbilt v. Mitchell*, 67 A. 97, 100 (N.J. App. 1907) (adopting *Pavesich*). The court determined that "[t]he right of privacy . . . is a right derived from natural law," but which is "unquestionably limited by the right to speak and print." *Pavesich*, 50 S.E. at 71 & 74. To reconcile these competing rights, the court followed the approach of Founding-era courts and held that First Amendment interests were adequately protected by building into common-law privacy torts a principle that "[t]he truth may be spoken . . . about all matters of a public nature, as well as matters of a private nature in which the public has a legitimate interest." *Pavesich*, 50 S.E. at 74; *see also The Right to Privacy*, 4 Harv. L. Rev. at 193, n.42.

The accommodation of interests reflected in these cases has proven workable for more than a century. Comparable developments of the common-law privacy rights into statutory rights to restrain disclosure are a fixed feature of many areas of law. *See e.g.*, 42 U.S.C. § 1320d-6 (preventing healthcare provider from disclosing certain information without patient's consent).

Daniel's Law is in keeping with this long tradition. Like other privacy torts, the statute grants Covered Persons the right to prevent others from (i) giving unreasonable publicity to personal facts of little to no public significance and (ii) misappropriating their identity. The statute does not imperil First Amendment interests any more than traditional common-law disclosure, misappropriation, and intrusion torts—indeed, it restricts speech far less than common-law protections that prohibit disclosure of private facts based on the risk of emotional, reputational, or dignitary harm. *See e.g.*, *Krause v. Rocketreach*, 561 F. Supp. 3d 778, 783-84 (N.D. Ill. 2021) (rejecting First Amendment argument against Illinois' identity misappropriation statute). Daniel's

Law is targeted at information that subjects officers and other "Covered Persons" to threats, violence, and harassment; courts routinely allow disclosure torts to be used to prevent disclosure of such information. *See, e.g.*, *Capra v. Thoroughbred Racing Ass'n of N. Am., Inc.*, 787 F.2d 463, 464 (9th Cir. 1986); *Hyde v. City of Columbia*, 637 S.W.2d 251, 254 (Mo. Ct. App. 1982).

Further, the data regulated by Daniel's Law has virtually no relationship with matters of public concern. "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." *Snyder v. Phelps*, 562 U.S. 443, 453 (2011). The specific home address and phone number of a judge, prosecutor, or law enforcement officer has no bearing on any question of political or social significance, as New Jersey's appellate court deciding an as-applied challenge to Daniel's Law has held. *See Kratovil*, 2024 WL 1826867, at *6 ("[T]he publication of the town where Caputo lived was a matter of public concern, but Caputo's specific street address was not"); *see also Trans Union*, 267 F.3d at 1140 ("[N]ames, addresses, and financial circumstances" were "speech of purely private concern"). Absent this home address and phone number data, the data brokers may carry on with their business.

Moreover, Daniel's Law specifically permits Covered Persons to obtain redaction of virtually all public records containing their home address, so long as the Covered Person affirms that he or she understands the rights and benefits relinquished by redacting that information from public record. N.J.S. 47:1B-1(a). But even where a Covered Person does not request redaction from public records, privacy violations can occur when information is republished in a way that greatly expands access to that information. "[T]he extent of the protection accorded a privacy right at common law rested in part on the degree of dissemination of the allegedly private fact," and not merely whether the information was available in *some form*. *United States Dep't of Justice*

v. Reporters Committee for Freedom of the Press, 489 U.S. 749, 763-64 (1989) (recognizing a "distinction, in terms of personal privacy, between scattered disclosure of bits of information" in public records and widespread "revelation"); *see also* D. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 U. Minn. L. Rev. 1137, 1173 (2002) ("Privacy involves an expectation of a certain degree of accessibility of information" and "can be violated by altering levels of accessibility, by taking obscure facts and making them widely accessible."). To apply strict scrutiny notwithstanding the privacy rights at issue would ignore this long line of precedent.

C. Daniel's Law Has No Nexus with Viewpoint Discrimination

Daniel's Law is also not subject to strict scrutiny because any "content-based rules" it imposes are designed "not to 'suppres[s] . . . ideas,' but simply to serve [the] law's purposes." *Vidal*, 602 U.S. at 316 (Barrett, J., concurring) (quoting *Davenport*, 551 U.S. at 189). "The rationale of the general prohibition" on content-based restrictions "is that content discrimination 'raises the specter that the Government may effectively drive certain ideas or viewpoints from the marketplace.'" *R.A.V. v. St. Paul*, 505 U.S. 377, 387 (1992) (quoting *Simon & Schuster, Inc. v. Members of N.Y. State Crime Victims Bd.*, 502 U.S. 105, 116 (1991)). Thus, when "'there is no realistic possibility that official suppression of ideas is afoot,'" strict scrutiny does not apply. *Vidal*, 602 U.S. at 316 (Barrett, J., concurring); *see also id.*, slip op. at 1 (Kavanaugh, J., concurring) (accepting that a "viewpoint-neutral" restriction "might well be constitutional even absent such a historical pedigree"); *Davenport*, 551 U.S. at 188 (identifying "numerous" cases in which the risk of viewpoint discrimination "is inconsequential, so that strict scrutiny is unwarranted."); *People v. Austin*, 155 N.E.3d 439, 459 (Ill. 2019) (holding privacy statute had no "potential for censorship or manipulation as to justify application of strict scrutiny.").

Daniel's Law creates no risk of viewpoint discrimination, so it should be upheld if its restrictions are "reasonable" considering the statute's purposes. *Davenport*, 551 U.S. at 189. "No matter the message" a party disclosing information about a Covered Person "wants to convey," the statute "prohibits" disclosing the Covered Person's home address and phone number "without consent." *Vidal*, 602 U.S. at 293-94. The statute does not target disclosures "based on the specific motivating ideology or the opinion or perspective of the speaker." *Reed*, 576 U.S. at 168 (quotation marks omitted). Nor does the statute exhibit any features suggesting it was designed to "discriminate based on viewpoint in its practical operation." *Vidal*, 602 U.S. at 294. "[T]here are many reasons why a person may be unable to secure another's consent" to republish his address and phone number which have nothing to do with viewpoint, such as "to prevent his name from being exploited for another's gain." *Id*. Moreover, the statute only prohibits "disclosures" that include two types of data—a Covered Person's home address and phone number. No other data is excluded from any "disclosure." And as New Jersey courts have recognized, speech about where a Covered Person lives (and presumably, similar statements about a Covered Person's phone number) is not barred in any way by the statute. *Kratovil*, 2024 WL 1826867, at *5.

Analogies with other areas of First Amendment doctrine further support this conclusion. **First**, speech "can be constitutionally proscribed because the social interest in order and morality outweighs the negligible contribution of those categories of speech to the marketplace of ideas." *Davenport*, 551 U.S. at 188. Preventing widespread dissemination of the home addresses and phone numbers of judges, prosecutors, and law enforcement officers ensures the preservation of order. Re-publication of home address and phone numbers, particularly at the massive, automated scale involved here, makes no real contribution to the marketplace of ideas on any subject other than where someone lives and how to contact them. *Cf. Dun & Bradstreet, Inc. v. Greenmoss*

Builders, Inc., 472 U.S. 749, 762 (1985) (holding "credit reporting" did not "require[] special protection to ensure that 'debate on public issues [will] be uninhibited, robust, and wide-open.'") (citing *New York Times Co. v. Sullivan*, 376 U.S. 254, 270 (1964)); *Trans Union*, 267 F.3d at 1141 (marketing lists were "private speech warranting only qualified constitutional protection").

Second, "the risk that content-based distinctions will impermissibly interfere with the marketplace of ideas" is limited "when the government is acting in a capacity other than as regulator." *Davenport*, 551 U.S. at 188. For example, "it is well established that the government can make content-based distinctions when it subsidizes speech" or permits speech in "a nonpublic forum." *Id.* at 188-89 (upholding statute that required public-sector unions to receive authorization from a nonmember before spending that nonmember's agency fees on election-related purposes). Here, the State does not act as a regulator—it grants *individual persons* the power to control the republication of their home address and phone number, much as the statute upheld in *Davenport* empowered individuals to prevent unions from spending fees they contributed to the union on election-related speech without authorization. Laws that recognize one private person's rights against another private person often attract no scrutiny at all when there is no risk of viewpoint discrimination.[3] Moreover, much of the data disclosed is information generated by the State and contained in government records. The statute limits re-publication of that information to prevent widespread dissemination, which increases the risk of harm. "The restriction on the state-bestowed entitlement was thus limited to the state-created harm" that the New Jersey Legislature "sought to remedy." *Davenport*, 551 U.S. at 189; *Los Angeles Police Dep't v. United Reporting Publishing Co.*, 528 U.S. 32 (1999); D. Solove, *Artificial Intelligence and Privacy*, at 28 ("[T]he government

[3] *See* F. Schauer, *The Boundaries of the First Amendment: A Preliminary Exploration of Constitutional Salience*, 117 Harv. L. Rev. 1765, 1768 (2004) (collecting examples of similar content-based regulation that receive no scrutiny at all).

can place conditions on much of the data it releases to the public, similar to how a company can provide conditions in its terms of service."); D. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 Minn. L. Rev. 1176-78 (2002).

Considering the purpose of Daniel's Law, its practical application, and precedent declining to apply strict scrutiny to other forms of content-based restrictions makes clear that Daniel's Law has no nexus with viewpoint discrimination and therefore should not be subject to strict scrutiny.

D. At Most, Daniel's Law Regulates Commercial Speech

Many data "disclosures" regulated by Daniel's Law at most qualify as commercial speech, "merit[ing] only intermediate scrutiny." *Trans Union*, 267 F.3d at 1141 (marketing lists of names and addresses were commercial speech). To determine if speech is commercial, courts consider three factors: whether the speech (1) is "an advertisement"; (2) "refer[s] to a specific product or service"; and (3) is driven by "an economic motivation." *Greater Phila. Chamber of Com. v. City of Philadelphia*, 949 F.3d 116, 137 (3d Cir. 2020) (quoting *U.S. Healthcare, Inc. v. Blue Cross of Greater Phila.*, 898 F.2d 914, 933 (3d Cir. 1990)). These factors "provide[] 'strong support for the conclusion that the speech is commercial,'" but they "are not dispositive, and the inquiry involves 'making a commonsense distinction between speech proposing a commercial transaction . . . and other varieties of speech.'" *Crash Proof Retirement, LLC v. Price*, 533 F.Supp.3d 227, 230 (E.D. Pa. 2021) (quoting *Facenda v. N.F.L. Films, Inc.*, 542 F.3d 1007, 1017 (3d Cir. 2008)).

Daniel's Law is directed at many commercial acts, making it unlawful "to solicit, sell, manufacture , . . . lend, trade , . . . advertise, or offer" home addresses or phone numbers of Covered Persons. N.J.S.A. 56:8-166.1(d). These "disclosures" are obviously driven by an economic motivation and are necessarily incident to speech that "does no more than propose a commercial transaction." *Bolger v. Youngs Drug Prod. Corp.*, 463 U.S. 60, 66 (1983) (quotation marks and

citation omitted). While home address and phone number data offered in such transactions may not, by itself, "refer" to a product or service, such data *is* a product or service. And many businesses use the home address and phone number data within the ambit of Daniel's Law for the purpose of identifying people to target with marketing. *See, e.g.*, *U.S. West, Inc. v. F.C.C.*, 182 F.3d 1224, 1233 n.4 (10th Cir. 1999) (speech whose purpose was "to facilitate the marketing of telecommunications services to individual customers" was "integral to and inseparable from the ultimate commercial solicitation" and thus was "properly categorized as commercial speech").

Moreover, the data "disclosed" on many websites operates as an advertisement to view further advertisements for other goods and services. Companies will post the home addresses and phone numbers of persons to draw customers to their sites, who in turn will then see advertisements for other goods and services. And "[g]enerally, courts consider speech that draws the public's attention to a product or service for purposes of promoting its sale an advertisement." *Crash Proof Ret., LLC v. Price*, 533 F.Supp.3d at 231. Thus, in many applications, the "disclosures" regulated by Daniel's Law (if they are speech at all) will at most be subject to intermediate scrutiny.

IV. Daniel's Law Satisfies Any Standard of Review

A. Privacy Laws Have Repeatedly Survived First Amendment Challenges

Despite being frequently targeted by data brokers, multiple privacy laws have survived First Amendment challenges, including before the United States Supreme Court.

- Health Information Privacy Protection Act (HIPAA): *Citizens for Health v. Leavitt*, 428 F.3d 167, 184 (3d Cir. 2005) (rejecting First Amendment claim that HIPAA's Privacy Rule infringes on individuals' right to confidential communications with healthcare providers).
- (Federal and state) Telephone Consumer Privacy Act (TCPA) and state companion statutes: *Barr v. Am. Ass'n of Political Consultants*, 591 U.S. 610, 635 (2020) (other than

exception for government debt collection texts, finding TCPA constitutional against defendants' First Amendment challenge); *Nat'l Coal. of Prayer, Inc. v. Carter*, 455 F.3d 783, 789 (7th Cir. 2006) (rejecting similar challenge to Indiana do-not-call list law on basis that it curtailed telemarketing noting it "effectively protects residential privacy").

- (Federal and state) Video Rental Protection Statutes: *Boelter v. Hearst Commc'ns, Inc.*, 192 F. Supp. 3d 427, 452 (S.D.N.Y. 2016) (upholding Michigan's Video Rental Privacy Act limiting businesses' dissemination of customer information); Saunders v. Hearst Television, Inc., 2024 WL 126186 at *5-6 (D. Mass. January 11, 2024) (upholding federal Video Privacy Protection Act's prevention of owners of news applications from disclosing users' personally identifiable information); *Christopherson v. Cinema Entertainment Corporation*, 2024 WL 1120925, at *5 (D. Minn. Mar. 6, 2024) (rejecting argument that the Video Privacy Protection Act violated the First Amendment at the PI stage).
- (Federal) Fair Credit Reporting Act (FCRA): *King v. Gen. Info. Servs, Inc.*, 903 F. Supp. 2d 303, 313 (E.D. Pa. 2012); *see also Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 762 (1985) (a consumer "credit report concerns no public issue" and "was speech solely in the individual interest of the speaker and its specific business audience.").
- Illinois Biometric Information Protection Act (BIPA): *Sosa v. Onfido, Inc.*, 2022 WL 1211506 (N.D. Ill. 2022) (denying First Amendment challenge, finding law content neutral); *ACLU v. Clearview AI, Inc.*, 2021 WL 4164452, at *9 (Ill. App. Ct. Aug. 27, 2021) (concluding "BIPA's restrictions . . . are no greater than what's essential to further Illinois' interest in protecting its citizens' privacy and security").
- Right of Publicity Statutes: *Kellman v. Spokeo, Inc*., 599 F. Supp. 3d 877, 899-900 (N.D. Cal. 2022) (upholding right of publicity and misappropriation statutes in California,

Indiana, and Ohio against First Amendment challenges because "[t]he protection of privacy interests is . . . a longstanding commitment of the law—and an important one"). *Krause v. RocketReach*, 561 F. Supp. 3d 778, 783-784 (N.D. Ill. 2021).

For the same reasons courts have denied First Amendment challenges to other privacy laws, the Court should deny Defendants' as well. At minimum, Daniel's Law's restrictions on information —assuming *arguendo* speech is implicated—is far narrower than that of the TCPA. Yet, even in that case, the Supreme Court found that the statute survived the First Amendment challenges put forth by the data brokers because "the people's representatives have made crystal clear that robocalls must be restricted." *Barr*, 591 U.S. at 635. Daniel's Law is likewise constitutional, especially given Defendants' inability to articulate a more narrowly tailored way to protect the safety of the Covered Persons, which everyone agrees is a compelling state interest.

B. Daniel's Law Is Neither "Overinclusive" Nor "Overbroad"

Defendants never expressly raise an overbreadth challenge, but Plaintiffs address the "over-inclusiveness" point raised by Defendants both on its own terms and as an overbreadth challenge for the sake of completeness. As the Supreme Court recently articulated, the overbreadth doctrine requires that Defendants show "a substantial number of its applications are unconstitutional, judged in relation to the statue's plainly legitimate sweep." *Americans for Prosperity Foundation*, 594 U.S. at 615. Defendants never try to meet this burden, nor could they.

1. The definition of "disclose" further the interest of ensuring public official safety

"The words of a statute must be read in their context and with a view to their place in the overall statutory scheme." *Gundy v. United States*, 588 U.S. 128, 141, (2019). Yet, Defendants exaggerate the scope of the statute's definition of "disclose" when they claim that it prohibits purely private disclosures. *See* Motion to Dismiss, ECF No. 27-33, at 27-28. Read in context, the

statute reaches two categories of disclosures. First, most of the acts of "disclosure" enumerated in the statute—to "post," "publish," "distribute," "circulate," "disseminate," "present," "exhibit," or "advertise"—are only naturally read to refer to acts of generalized, widespread publication. Second, other acts of disclosure—to "solicit," "sell," "manufacture," "give," "provide," "lend," "trade," "mail," "deliver," and "transfer"—are naturally read to include transfers between businesses, which may or may not be public.

Contrary to Defendants' submission, both categories of "disclosures" are justified by the State's compelling interest, an interest to which even they accede. Defendants' cases consistently define the State's interest far too narrowly, focusing almost exclusively on whether the statutes at issue were directed at "true threats." *See Brayshaw*, 709 F.Supp.2d at 1248; *Sheehan*, 272 F.Supp.2d at 1141-42. But empowering Covered Persons to (i) protect their interest in personal solitude and freedom from violence and harassment; and (ii) prevent misappropriation of their names and likenesses, advances compelling interests regardless of whether a disclosure specifically enables a so-called "true threat." *Barr*, 591 U.S. at 622 (privacy is a compelling interest); *Hill v. Colorado*, 530 U.S. 703, 715 (2000) (preventing threats to "safety"); *Hart*, 717 F.3d at 150 ("interest in safeguarding the right of publicity"); *Paul P.*, 227 F.3d at 101 (3d Cir. 2000) (recognizing "interest in one's home address"). The first category of "disclosures" clearly implicates the State's interest in preventing threats, violence, and harassment against Covered Persons. The second category of "disclosures" is focused on business transactions, rather than publication, but disclosures in that category likewise increase risks for Covered Persons by enabling the development of a market for their home addresses and phone numbers. Both categories of "disclosures" prevent misappropriation of the identities of Covered Persons.

The following examples of supposedly covered private disclosures cited by Defendants

reflect Defendants' exaggerated reading of the statute:

- "Disseminating" voter addresses to campaigns would not violate the statute, because "disseminate" refers to acts of generalized publication or commercial distribution and should be construed to have the same reach. *Cf.* N.J.S.A. 19:31-18.1(c) (barring certain commercial use of voter registration lists).
- The acquisition of a customer address list by an acquiring company in a merger would not qualify as "giving" the acquirer anything, because the acquirer would simply assume the acquired company's existing assets—including the address information.
- Moving an address to a cloud-storage service does not qualify as "transferring" the address, because it remains within the legal control of the business and involves neither publication nor a commercial transaction in which the address is transferred as consideration.
- Maintaining an internal database obviously does not suffice to make the address "available or viewable" on "the Internet" in a "searchable list or database," because those terms must be understood by reference to the other verbs in the definition.
- "Selling" a Covered Person's home address or phone number would be covered by the statute, but that is only because the statute aims to prevent misappropriation of the home addresses and phone numbers of Covered Persons for commercial purposes.

Similarly without merit are Defendants' claims that the statute prohibits disclosures that do not include information linking the address or phone number to the Covered Person. *See* Motion to Dismiss, ECF No. 27-33, at 30-31. By prohibiting disclosure of the home address or phone number "of any Covered Person," the statute is most naturally read to only cover disclosures that link the address or phone number to that person—which requires the use of their name.

Defendants also take issue with "otherwise make available." *See* Motion to Dismiss, ECF

No. 27-3, at 29, 47. But read in the context in which it appears in the statute, this phrase is only intended to create a residual category of acts of publication or commercial sale that might not satisfy the definition of "disclose." Under "the ejusdem generis principle," "general words [that] follow specific words in a statutory enumeration . . . are construed to embrace only the objects similar in nature to those objects enumerated by the preceding specific words." *State v. Hoffman*, 149 N.J. 564, 584 (1997) (interpreting catch-all clause narrowly in addressing vagueness challenge). Because the specific words "disclose" and "re-disclose" are expressly defined to cover specified acts of online publication and transmission by commercial transaction, the phrase "otherwise make available" can only apply to closely analogous acts.

Finally, Defendants' argument that Daniel's Law is overinclusive because it does not contain an express exception for speech on a matter of public concern ignores common law tradition. New Jersey courts follow the principle that statutes "in derogation of the common law should be strictly construed." *Marshall v. Klebanov*, 188 N.J. 23, 37 (2006) (quotation marks and citation omitted); *see also Warnig v. Atlantic Cnty. Special Servs*., 363 N.J. Super. 563, 571 (App. Div. 2003) ("If a change in the common law is to be effectuated, the legislative intent to do so must be clearly and plainly expressed."). Nothing in Daniel's Law suggests the Legislature intended to override the common-law rule that "'[t]he right of privacy does not prohibit any publication of matter which is of public or general interest,'" *Bartnicki,* 532 U.S. at 534 (quoting Warren & Brandeis, *The Right to Privacy*, at 214)—let alone offer a clear statement. The statute should be construed to preserve this restriction. *Time*, 385 U.S. at 397 (rejecting facial challenge to privacy statute on the assumption that state courts would interpret the statute to include a public-concern exception); *G.D. v. Kenny*, 205 N.J. 275, 299 (2011) (rejecting "literal and overly broad reading" that "would criminalize truthful speech on matters of public interest and concern").

Moreover, as discussed, the circumstances in which the specific home address or phone number of a Covered Person could ever qualify as a matter of public concern are few in number—if they exist. Defendants' chief cases do not hold otherwise. That alone is fatal to a facial challenge. Almost to a one, they addressed as-applied challenges involving unusual circumstances in which addresses, phone numbers, or similar were "integral to [the speaker's] message." *See Ostergren v. Cuccinelli*, 615 F.3d 263, 271 (4th Cir. 2010) (law prohibiting posting Social Security Numbers was unconstitutional as applied to speaker who posted SSNs to "publicize her message that governments are mishandling SSNs"); *Publius v. Boyer-Vine*, 237 F.Supp.3d 997, 1016 (E.D. Cal. 2017) (statute prohibiting posting of legislators' names and addresses was unconstitutional as applied to blog post protesting public database of gun owners); *Sheehan v. Gregoire*, 272 F.Supp.2d 1135, 1139 n.2 (W.D. Wash. 2003) (blog on "criminal history of individual officers" and "serving process or subpoenas on officers" concerned "a subject of legitimate public interest").

At most, Defendants' arguments establish that Daniel's Law might be invalid as applied to purely private acts of "disclosure," to certain acts of "otherwise making available" the home addresses and phone numbers of Covered Persons, or communicative acts that necessarily use the home address or phone number of a Covered Person to address a matter of public concern. That is not enough to show the statute is facially unconstitutional, to say nothing of the fact that Defendants do not have standing as non-news gathering organizations to make this argument.

2. The absence of a verification requirement does not render the statute overinclusive

Defendants also claim Daniel's Law is overinclusive because it does not include a verification requirement, but whether the statute contains a verification requirement does not alter the scope of its coverage or the amount of speech it restricts. Moreover, regardless of whether the statute requires a verified notice, to prevail on a Daniel's Law claim, a plaintiff must prove his

case—which includes showing that he is in fact a Covered Person. Likewise, Defendants' complaints about the assignment process permitted by the statute to facilitate the efficient prosecution of claims have nothing to do with the First Amendment and everything to do with Defendants' desire to escape liability for their acts.

3. The "liquidated damages" provision advances the interest Daniel's Law serves

Defendants' complaints about the standard of liability and the liquidated-damages provision in Daniel's Law are equally irrelevant to the First Amendment inquiry. To begin with, the statute does not, as Defendants say, employ a strict-liability standard. By its terms, the statute requires notification pursuant to N.J.S.A 56:8-116.1(a)(2) before there is a duty to cease disclosure of a home address or phone number. Thus, any defendant held liable under the statute must have received "written notice" that they must cease disclosure of the Covered Person's home address or phone number to comply with the statute, which means such a defendant necessarily had actual or constructive knowledge of their duties to the Covered Person in question.

Defendants' alternative remedy of protective order or injunction would not advance the State's interests to nearly the same degree. The suggestion that the Legislature should have limited Covered Persons to seeking a protective order or injunction is simply an argument that the Legislature should have made it more difficult for Covered Persons to enforce their rights under the statute. If an injunction or protective order were issued, Defendants would still be liable for contempt if they disregarded that order—virtually the same consequence as being subjected to $1,000 in liquidated damages for failure to timely respond to a nondisclosure request. But the costs of litigating injunctive relief claims on an individualized basis would be prohibitive, and many Covered Persons would have no real prospect of ever enforcing their rights under the statute.

C. Daniel's Law Is Not Underinclusive

Defendants' underinclusivness concern is similarly unfounded. The Supreme Court has long held that "'the First Amendment imposes no freestanding 'underinclusiveness limitation.'" *Williams-Yulee v. Florida Bar*, 575 U.S. 433, 449 (2015). "A State need not address all aspects of a problem in one fell swoop; policymakers may focus on their most pressing concerns." *Id.* And the Court has "upheld laws—even under strict scrutiny—that conceivably could have restricted even greater amounts of speech in service of their stated interests." *Id.* Underinclusiveness can justify invalidating a statute in two circumstances: first, when underinclusiveness shows "the government is [not] in fact pursuing the interest it invokes, rather than disfavoring a particular speaker or viewpoint," and second, when underinclusiveness "reveal[s] that a law does not actually advance a compelling interest." *See Williams-Yulee*, 575 U.S. at 448-49. Neither circumstance is present. Defendants concede the law is not viewpoint discriminatory, nor is it "riddled with exceptions" preventing it from advancing the State's interests. *Id.*

First, Defendants argue that Daniel's Law is underinclusive because Covered Persons are not ***required*** to seek redaction of public records containing their home addresses and phone numbers or target ***every website*** that posts their data at once. *See* Motion to Dismiss, ECF No. 27-33, at 38. But these are not ***exceptions*** to Daniel's Law, because the statute does not purport to enact a flat ban on disclosure of home addresses and phone numbers. The statute empowers Covered Persons to decide for themselves whether a given website is sufficiently accessible to create a risk of violence or harassment, and whether to enforce their rights to their name and likeness against a particular party. And "[a] regulation is not fatally underinclusive simply because" the State could have adopted "an alternative regulation[] which would restrict more speech or the speech of more people." *Trans Union*, 267 F.3d at 1143.

Moreover, public records are far less accessible than information posted on websites that

render such information easily searchable by any user or member of the general public. Defendants offer no reason to think that the traditional availability of home addresses in public records presents anything close to the risks associated with easy, aggregated, curated, and widespread access—particularly given that Covered Persons can obtain redaction of virtually all public records upon request. "Even under strict scrutiny, '[t]he First Amendment does not require States to regulate for problems that do not exist.'" *Williams-Yulee*, 575 U.S. at 451 (marks and citation omitted).

Second, Defendants insist that the statute is underinclusive because it does not regulate property records. *See* Motion to Dismiss, ECF No. 27-33, at 39. But this lone exception does not show that the statute "is littered with exceptions that substantially negate the restriction," as required to invalidate a statute as underinclusive. *Barr*, 591 U.S. at 622 (upholding TCPA against underinclusiveness challenge); *see also Trans Union*, 267 F.3d at 1143 ("[A] rule is struck for *under*inclusiveness only if it cannot fairly be said to advance any genuinely substantial government interest."). Moreover, property records are not nearly as accessible as data easily available on any search engine and do not misappropriate a Covered Person's personal information in commerce.

Finally, Defendants' underinclusiveness argument overlooks New Jersey's legitimate basis for treating redaction of public records differently from the redaction of private records. New Jersey's public agencies, unlike Defendants, provide substantial and important services to their constituents, including Covered Persons, in exchange for their constituents' tax dollars. Daniel's Law expressly advises Covered Persons that, if they should choose to redact their information from the records of public agencies, they risk losing access to public benefits that depend on these records, and they risk missing notifications regarding their duties and obligations. The affected benefits, duties, and obligations are set out expressly in the statute. *See* N.J.S.A. § 47:1B-2(d).

Because any Covered Person who seeks the nondisclosure of their home address from a

public agency could lose the benefit of these government-provided services, Daniel's Law provides that the Covered Person "shall affirm in writing that the person understands that certain rights, duties, and obligations are affected as a result of the request." *Id.* And because Covered Persons' rights, duties, and obligations would be affected by nondisclosure, Daniel's Law logically requires the Office of Information Privacy to verify the authenticity of the Covered Person's request and accordingly gives the office additional time to process it. Because Covered Persons may receive no benefit whatsoever from allowing their information to remain on Defendants' websites, the Legislature's choice to treat public records differently from Defendant's disclosures makes eminent sense and demonstrates that the law is not underinclusive.

D. Defendants Don't Actually Identify Less Restrictive Means

Defendants barely attempt to identify a less restrictive means. They suggest that Daniel's Law should be limited to disclosures that involve "publication." *See* Motion to Dismiss, ECF No. 27-33, at 41. But this is not a solution that protects the compelling interests at stake, which Defendants seem to quietly acknowledge. For example, such a limitation would not prevent business-to-business disclosures. Potential assailants looking to perpetrate harm are often sophisticated and, as set forth in the Complaint, have obtained home address and phone data meant only for "business" recipients in numerous ways: through misrepresentation, through their own employer, by hiring a business (such as a private investigator), or by simply acting or operating as a proprietorship themselves. *Cf.* ECF No. Compl. at ¶¶ 15 and 17. Nor does such a limitation serve as a prophylactic against the development of a market for the home addresses and phone numbers of Covered Persons, which increases the probability that this data will be accessible by those looking to harass, threaten, or harm them.

Defendants next assert that the law would be less restrictive on their exercise of speech if

it contained a fault or verification requirement. *See* Motion to Dismiss, ECF No. 27-33, at 27-33 & 41. Yet, as the Court is aware, Daniel's Law requires ten business days prior written notice before the obligation to cease disclosure of home address or phone data becomes effective; therefore liability under the statute only follows actual or constructive knowledge. Here, Defendants make no attempt to explain how Daniel's Law "restricts substantially more speech than necessary to achieve its goal of enhancing the safety of public officials." *Id.*at 26. Because the law only applies to Covered Persons who have sent nondisclosure notices, it is difficult to conceive of any substantial additional speech of that person's home address or phone information that would be enabled, after receipt of such a notice, if an additional fault requirement existed.

Similarly, a verification requirement would do nothing to narrow the scope of the statute's alleged restriction on speech. Indeed, even if a defendant received nondisclosure requests from individuals who are not Covered Persons, they do not need to cease the disclosure of their information and will not be liable to those individuals under Daniel's Law. Notably, the record contains no such evidence and Defendants do not suggest that such a circumstance exists here, let alone in every circumstance as required for a facial constitutional challenge. Defendants' reliance upon California Government Code § 7928.215(c), which requires a nondisclosure demand in that state to "include a statement describing a threat or fear for the safety" of the requesting official, is a red herring. Such a requirement eliminates the protection that New Jersey affords under Daniel's Law, namely that public servants should receive protection before they or their family members are in the proverbial cross-hairs. Indeed, such a requirement is impractical when read *in pari materia* with Defendants' other process arguments; a Covered Person in the midst of dealing with an imminent danger, has to then send nondisclosure requests to hundreds of data brokers with the hope that they comply within the ten-day compliance period. While Defendants do not further

elaborate, New Jersey chose not to risk the safety of public servants by creating additional pre-requisites for protection; recall that the murder that gave rise to the law came without any warning.

Defendants finally claim that Daniel's Law has been made "consistently broader and harsher." *Id.*at 42. But this claim is demonstrably false. While New Jersey has unanimously amended the law, it also increased the compliance period from 72 hours to 10 business days, taking the needs of private data brokers into consideration in the process. None of these legislative changes occurred in a vacuum or without notice. The Defendants have had years to create compliance processes and systems, but apparently—unlike some of their peers who did comply—chose not to do so until the commencement of these actions.[4]

Ultimately, Defendants' unabashed outward support of Daniel's Law as an important and legitimate means of protecting public servants and their families coupled with their failure to articulate a less-restrictive means of advancing the same compelling interest is all-but dispositive of their facial challenge. Thus, as set forth below, Defendants' facial Constitutional challenge fails and their motions to dismiss must be denied.

E. Defendants' Facial Vagueness Challenge Is Meritless

Defendants' vagueness challenge does not belong in this motion to dismiss, which the court limited to facial First Amendment challenges. "Vagueness doctrine is an outgrowth not of the First Amendment, but of the Due Process Clause." *United States v. Williams*, 553 U.S. 285, 304 (2008); *see also Holder v. Humanitarian Law Project*, 561 U.S. 1, 19 (2010) ("[T]he lower court" erred because it "merged plaintiffs' vagueness challenge with their First Amendment claims.").

[4] Apparently in response to the instant actions, on a February 22, 2024, call "a collection of data brokers and industry groups [including several Defendants here] – outlined plans to weaken [Daniel's Law], pushing amendments that would protect them from lawsuits and let them resume sharing police officers' and judges' personal information." *Companies Line up to Undercut Key Data Privacy Law,* Politico.com (Apr. 5, 2024).

Regardless, Defendants' facial vagueness challenge fails. A statute "fails to comport with due process" under the vagueness doctrine if it "fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement." *Holder*, 561 U.S. at 18. To prevail on a facial vagueness challenge, Defendants must prove "the enactment is impermissibly vague in all of its applications." *Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc*., 455 U.S. 489, 495 (1982). They do not come anywhere close to satisfying this standard. At most, Defendants argue that it is unclear whether only publishing addresses and phone numbers on the internet is covered by the statute. *See* Motion to Dismiss, ECF no. 27-33, at 47. But that argument concedes that the statute applies to ***internet publication***. Because Defendants all engaged in such publication, it follows that this challenge fails. *See Holder*, 561 U.S. at 20 (a party "who engages in some conduct that is clearly proscribed cannot complain of the vagueness of the law as applied to the conduct of others.").

Defendants' argument also misreads the statute. As explained above, the traditional tools of statutory construction clearly limit the statute's reach to two categories of conduct: (i) online publication; and (ii) certain commercial transactions involving the home addresses and unpublished home telephone numbers of Covered Persons. Defendants' argument that the statute might reach acts such as putting someone's "name and address on [an] envelope" asks this Court to accept a reading of the statute that cannot be taken seriously.[5] That makes it hard to argue that persons of ordinary intelligence cannot determine what conduct Daniel's Law proscribes.

Finally, the alleged risk of "arbitrary" enforcement is not an issue when addressing a statute

---

[5] Defendants assert that talk of "unpublished" phone numbers is an anachronism. *See* Motion to Dismiss, ECF No. 27-33, at 49. But phone listing services still exist. And even if true, that would just mean that all phone numbers are de facto unpublished for purposes of the statute.

that grants individual persons a right to control how others use their information, as opposed to a civil or criminal statute enforced by the government. Daniel's Law allows Covered Persons to decide when and how to exercise their rights under the statute to protect their own interests. The statute is not "enforced" by anyone acting in an official capacity.

F. Daniel's Law Is Protected Under the Tenth Amendment

"The Tenth Amendment confirms that the power of the Federal Government is subject to limits that . . . reserve power to the States" and protects the essential "incidents of state sovereignty." *New York v. United States*, 505 U.S. 144, 156-57 (1992). This includes the "police power," which "is controlled by 50 States instead of one national sovereign," *NFIB v. Sebelius*, 567 U.S. 519, 535-36 (2012), and constitutes a reserved "right of the States," *Tennessee Wine & Spirits Retailers Assoc. v. Thomas*, 588 U.S. 504, 521 (2019).

"It is a traditional exercise of the States' 'police powers to protect the health and safety of their citizens (internal citations omitted).'" *Hill*, 530 U.S. at 715 (2000). New Jersey's attempt to protect its own judges, prosecutors, law enforcement officers, and their families, is a proper exercise of the police power, which encompasses the power to legislate "to protect the health, morals, and safety of the[] people" of a State. *Tennessee Wine & Spirits Retailers Assoc.*, 588 U.S. at 521 (quotation marks and citation omitted). Because Defendants have not identified a less restrictive means to advance the same safety interests, and because the Law was passed in the exercise of New Jersey's traditional police powers, it meets the strict scrutiny test.

G. Regardless, Daniel's Law Meets the Strict Scrutiny Test Because Even Defendants Agree That It Protects Against The Occupational Hazards Faced by Covered Persons

In upholding a Colorado ordinance, the Supreme Court recognized that "the States' 'police powers to protect the health and safety of their citizens'" may be sufficient to override First Amendment challenges. *Hill v. Colorado*, 530 U.S. at 715. In cases where the First Amendment

has met the compelling interest of people's safety, lower Courts have likewise followed the same reasoning. *See Capra v. Thoroughbred Racing Ass'n of N. Am., Inc*., 787 F.2d 463, 464 (9th Cir. 1986) (speech revealing "former identity and location" of person in witness-protection program was not protected by First Amendment); *Hyde v. City of Columbia*, 637 S.W.2d 251, 254 (Mo. Ct. App. 1982) (First Amendment did not apply to claims that newspaper negligently disclosed name and address of abduction victim while assailant was still at large). This is in line with the reason why a long-time exception to First Amendment challenges has been instances of "true threats" to the safety of individuals. *See Counterman v. Colorado*, 600 U.S. 66, 72 (2023) ("True threats of violence . . . lie outside the bounds of the First Amendment's protection."). In *Hill v. Colorado*, for example, the Supreme Court upheld the state ordinance designed to protect the safety of persons visiting abortion clinics. 530 U.S. at 716 (reasoning "it may not be the content of the speech, as much as the deliberate 'verbal or visual assault,' that justifies proscription") (citation omitted).

Here, in multiple proceedings before the District Court, in addition to numerous correspondence to Plaintiffs, Defendants concede that Daniel's Law protects the safety of the Covered Persons, and that it was enacted with that purpose in mind. *See* Motion to Dismiss, ECF No. 27-33, at 3; April 18, 2024 Transcript p. 26:22-24 ("Everyone in this courtroom understands the noble intent of Daniel's Law. It's to protect the privacy and safety of public servants"); June 3, 2024 Transcript 91:1-8 ("[t]he Legislature's articulated interest is actually safety. I just wanted to make that clear on the record . . . It's judicial, in other [C]overed [P]ersons [sic], safety… It's the safety interest, Your Honor"). Defendants have also stated on the record that they too are allegedly interested in the very compelling goal of protecting the lives of the Covered Persons. April 18, 2024 Transcript p. 88:2-6 ("we all want to suppress that information. So the harm, the alleged harm that's occurring, is going to be addressed right away with this production that you

may order, Your Honor."). Not one Defendant disputed their Co-Defendants' and lead counsels' statements. Failing to raise any real dispute as to whether Daniel's Law advances a compelling interest and likewise failing to provide any real alternative to do the same, Defendants' facial challenge cannot even be saved by the application of strict scrutiny.

CONCLUSION

The Court should deny Defendants' Motion to Dismiss.

Dated: August 5, 2024

Respectfully submitted,

PEM LAW LLP

By: s/ Rajiv D. Parikh

Rajiv D. Parikh
Kathleen Barnett Einhorn
One Boland Drive, Suite 101
West Orange, New Jersey 07052
Tel: (973) 577-5500
rparikh@pemlawfirm.com
keinhorn@pemlawfirm.com

BOIES SCHILLER FLEXNER LLP
Mark Mao (admitted *pro hac vice*)
44 Montgomery St., 41st Floor
San Francisco, CA 94104
Tel.: (415) 293-6800
mmao@bsfllp.com

Adam R. Shaw (admitted *pro hac vice*)
30 South Pearl Street, 12th Floor
Albany, NY 12207
Tel: (518) 434-0600
ashaw@bsfllp.com

Samantha Parrish (*pro hac vice* to be filed)
2029 Century Park East, Suite 1520N
Los Angeles, CA 90067
Tel.: (213) 629-9040
sparrish@bsfllp.com

Eric Palmer (*pro hac vice* to be filed)
401 East Las Olas Blvd., Suite 1200
Fort Lauderdale, FL 33301
Tel.: (954) 356-0011
epalmer@bsfllp.com

MORGAN & MORGAN COMPLEX LITIGATION GROUP
John A. Yanchunis (*pro hac vice* to be filed)
Ryan J. McGee (*pro hac vice* to be filed)
201 North Franklin Street, 7th Floor
Tampa, FL 33602
Tel.: (813) 223-5505
jyanchunis@ForThePeople.com
rmcgee@ForThePeople.com

Attorneys for Plaintiffs