UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. LIGHTBOX PARENT, L.P., et al., Defendant.	Hon. Harvey Bartle, III Civil Action No. 24-4105
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. BLACKBAUD, INC., et al., Defendant.	Civil Action No. 24-3993
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. WHITEPAGES INC., et al., Defendant.	Civil Action No. 24-3998

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. HIYA, INC., et al., Defendant.	Civil Action No. 24-4000
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. WE INFORM, LLC, et al., Defendant.	Civil Action No. 24-4037
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. INFOMATICS, LLC, et al., Defendant.	Civil Action No. 24-4041

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. THE PEOPLE SEARCHERS, LLC, et al., Defendant.	Civil Action No. 24-4045
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. COMMERCIAL REAL ESTATE EXCHANGE, INC., et al., Defendant.	Civil Action No. 24-4073
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. DM GROUP, INC., et al., Defendant.	Civil Action No. 24-4075

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. CARCO GROUP, INC., et al., Defendant.	Civil Action No. 24-4077
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. DELUXE CORPORATION, et al., Defendant.	Civil Action No. 24-4080
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. TWILIO INC., et al., Defendant.	Civil Action No. 24-4095

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. QUANTARIUM ALLIANCE, LLC, et al., Defendant.	Civil Action No. 24-4098
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. YARDI SYSTEMS, INC., et al., Defendant.	Civil Action No. 24-4103
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. 6SENSE INSIGHTS, INC., et al., Defendant.	Civil Action No. 24-4104

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. DELVEPOINT, LLC, et al., Defendant.	Civil Action No. 24-4096
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. SEARCH QUARRY, LLC, et al., Defendant.	Civil Action No. 24-4106
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. ACXIOM, LLC, et al., Defendant.	Civil Action No. 24-4107

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. ENFORMION, LLC, et al., Defendant.	Civil Action No. 24-4110
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. COSTAR GROUP, INC., et al., Defendant.	Civil Action No. 24-4111
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. ORACLE INTERNATIONAL CORPORATION, et al., Defendant.	Civil Action No. 24-4112

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. RED VIOLET, INC., et al., Defendant.	Civil Action No. 24-4113
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. RE/MAX, LLC, et al., Defendant.	Civil Action No. 24-4114
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. EPSILON DATA MANAGEMENT, LLC, et al., Defendant.	Civil Action No. 24-4168

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. PEOPLE DATA LABS, INC., et al., Defendant.	Civil Action No. 24-4171
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. LABELS & LISTS, INC., et al., Defendant.	Civil Action No. 24-4174
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. CLARITAS, LLC, et al., Defendant.	Civil Action No. 24-4175

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. INNOVIS DATA SOLUTIONS INC., et al., Defendant.	Civil Action No. 24-4176
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. ACCURATE APPEND, INC., et al., Defendant.	Civil Action No. 24-4178
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. DATA AXLE, INC., et al., Defendant.	Civil Action No. 24-4181

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. REMINE, INC., et al., Defendant.	Civil Action No. 24-4182
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. LUSHA SYSTEMS, INC., et al., Defendant.	Civil Action No. 24-4184
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. TELTECH SYSTEMS, INC., et al., Defendant.	Civil Action No. 24-4217

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. PEOPLECONNECT, INC., et al., Defendant.	Civil Action No. 24-4227
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. CORELOGIC, INC., et al., Defendant.	Civil Action No. 24-4230
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. BLACK KNIGHT TECHNOLOGIES, LLC, et al., Defendant.	Civil Action No. 24-4233

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. ZILLOW, INC., et al., Defendant.	Civil Action No. 24-4256
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. EQUIMINE, INC., et al., Defendant.	Civil Action No. 24-4261
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. THOMSON REUTERS CORPORATION, et al., Defendant.	Civil Action No. 24-4269

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. CHOREOGRAPH LLC, et al., Defendant.	Civil Action No. 24-4271
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. TRANSUNION, LLC, et al., Defendant.	Civil Action No. 24-4288
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. MELISSA DATA CORP., et al., Defendant.	Civil Action No. 24-4292

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. EQUIFAX INC., et al., Defendant.	Civil Action No. 24-4298
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. SPOKEO, INC., et al., Defendant.	Civil Action No. 24-4299
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. i360, LLC, et al., Defendant.	Civil Action No. 24-4345

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. TELNYX LLC, et al., Defendant.	Civil Action No. 24-4354
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. GOHUNT, LLC, et al., Defendant.	Civil Action No. 24-4380
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. ACCUZIP, INC, et al., Defendant.	Civil Action No. 24-4383

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. SYNAPTIX TECHNOLOGY, LLC, et al., Defendant.	Civil Action No. 24-4385
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. JOY ROCKWELL ENTERPRISES, INC., et al., Defendant.	Civil Action No. 24-4389
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. FORTNOFF FINANCIAL, LLC, et al., Defendant.	Civil Action No. 24-4390

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. MYHERITAGE, LTD., et al., Defendant.	Civil Action No. 24-4392
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. E-MERGES.COM, INC., et al., Defendant.	Civil Action No. 24-4434
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. WILAND, INC., et al., Defendant.	Civil Action No. 24-4442

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. ATDATA, LLC, et al., Defendant.	Civil Action No. 24-4447
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. PRECISELY HOLDINGS, LLC, et al., Defendant.	Civil Action No. 24-4571
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. NUWBER, INC., et al., Defendant.	Civil Action No. 24-4609

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. ROCKETREACH LLC, et al., Defendant.	Civil Action No. 24-4664
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. OUTSIDE INTERACTIVE INC., et al., Defendant.	Civil Action No. 24-4696
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. VALASSIS DIGTIAL CORP., et al., Defendant.	Civil Action No. 24-4770

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. THE LIFETIME VALUE CO., LLC, et al., Defendant.	Civil Action No. 24-4850
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. BELLES CAMP COMMUNICATIONS, INC., et al., Defendant.	Civil Action No. 24-4949
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. FIRST AMERICAN FINANCIAL CORPORATION, et al., Defendant.	Civil Action No. 24-5334

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. PROPERTY RADAR, INC., et al., Defendant.	Civil Action No. 24-5600
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. THE ALESCO GROUP, L.L.C., et al., Defendant.	Civil Action No. 24-5656
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. SEARCHBUG, INC., et al., Defendant.	Civil Action No. 24-5658

ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. AMERILIST, INC., et al., Defendant.	Civil Action No. 24-5775
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. LEXISNEXIS RISK DATA MANAGEMENT, LLC, et al., Defendant.	Civil Action No. 24-6160
ATLAS DATA PRIVACY CORPORATION, et al., Plaintiff, v. RESTORATION OF AMERICA, et al., Defendant.	Civil Action No. 24-4324

INTERVENOR ATTORNEY GENERAL OF NEW JERSEY'S BRIEF IN OPPOSITION TO DEFENDANTS' MOTIONS TO DISMISS

MATTHEW J. PLATKIN
ATTORNEY GENERAL OF NEW JERSEY
R.J. Hughes Justice Complex
P.O. Box 116
Trenton, New Jersey 08625
(609) 376-3202
Daniel.Vannella@law.njoag.gov
Attorney for Intervenor

Jeremy M. Feigenbaum (NJ Bar No. 117762014)
Solicitor General

Michael L. Zuckerman (NJ Bar No. 427282022)
Deputy Solicitor General

Daniel M. Vannella (NJ Bar No. 015922007)
Assistant Attorney General

Liza B. Fleming (NJ Bar No. 441912023)
Kashif T. Chand (NJ Bar No. 016752008)
Joshua P. Bohn (NJ Bar No. 164922015)
James M. Greenberg (NJ Bar No. 026722009)
Bryce K. Hurst (NJ Bar No. 336532021)
Marcus D. Mitchell (NJ Bar No. 404482022)
Deputy Attorneys General

Of Counsel and On The Brief

TABLE OF CONTENTS

TABLE OF CONTENTS i

TABLE OF AUTHORITIES iii

PRELIMINARY STATEMENT 1

BACKGROUND 3

A. The Right To Privacy And Safety In One's Home. 3

B. The Growing Urgency Of Such Protections. 6

C. Daniel's Law 8

D. Recent Legislation In Other Jurisdictions. 10

E. This Proceeding. 11

STANDARD OF REVIEW 12

ARGUMENT 13

I. DEFENDANTS' FACIAL ATTACK SHOULD BE DENIED. 13

A. Defendants' Facial Challenge Must Meet An Extremely High Bar. 14

B. This Facial Attack Implicates Only Intermediate Scrutiny. 17

1. Defendants Cannot Avoid *Central Hudson* Scrutiny. 18

2. Daniel's Law Is Content-Neutral. 25

3. Strict Scrutiny Is Inappropriate Because Comparable Privacy Protections Have Always Coexisted With The First Amendment. ..30

C. Daniel's Law Easily Satisfies Scrutiny On This Posture. 35

1. Numerous Applications Satisfy The Applicable Form Of Scrutiny.....35

2. Defendants' Counterarguments Lack Merit. 40

i. Daniel's Law Is Not Overinclusive. 40

ii. Daniel's Law Is Not Underinclusive. 48

II. DANIEL'S LAW IS NOT UNCONSTITUTIONALLY VAGUE. 52

CONCLUSION.....55

TABLE OF AUTHORITIES

Cases **Page(s)**

ACLU v. Clearview AI, Inc.,
No. 20 CH 4353, 2021 WL 4164452 (Ill. Cir. Ct. Aug. 27, 2021).....29

Allen v. Vertafore, Inc.,
28 F.4th 613 (5th Cir. 2022) 41

Ariix, LLC v. NutriSearch Corp.,
985 F.3d 1107 (9th Cir. 2021) 20

Ashcroft v. Iqbal,
556 U.S. 662 (2009).....13

Ass'n of Cleveland Fire Fighters v. City of Cleveland,
502 F.3d 545 (6th Cir. 2007) 55

Bank of Hope v. Chon,
938 F.3d 389 (3d Cir. 2019)..... 20, 35, 36, 38

Barna v. Bd. of Sch. Dirs. of Panther Valley Sch. Dist.,
877 F.3d 136 (3d Cir. 2017).....16

Barr v. Am. Ass'n of Pol. Consultants, Inc.,
591 U.S. 610 (2020)..... 33, 55

Bartnicki v. Vopper,
200 F.3d 109 (3d Cir. 1999)..... 15, 34

Bd. of Trs. of State Univ. of N.Y. v. Fox,
492 U.S. 469 (1989)..... 20, 25, 38, 47, 54

Bell Atl. Corp. v. Twombly,
550 U.S. 544 (2007).....13

Bigelow v. Virginia,
421 U.S. 809 (1975).....22

Boelter v. Advance Mag. Publishers Inc.,
210 F. Supp. 3d 579 (S.D.N.Y. 2016) 17, 21, 50

Boelter v. Hearst Commc'ns, Inc.,
192 F. Supp. 3d 427 (S.D.N.Y. 2016) 21, 22

Bolger v. Youngs Drug Prods. Corp.,
463 U.S. 60 (1983) 19, 22

Brayshaw v. City of Tallahassee,
709 F. Supp. 2d 1244 (N.D. Fla. 2010) 11, 29

Carey v. Brown,
447 U.S. 455 (1980) 36

Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y.,
447 U.S. 557 (1980) 18, 19, 38, 39

City of Austin v. Reagan Nat'l Advert. of Austin, LLC, 596 U.S. 61 (2022) ..... passim

City of Pittsburgh v. W. Penn Power Co.,
147 F.3d 256 (3d Cir. 1998) 13

Courthouse News Serv. v. Hade,
631 F. Supp. 3d 349 (E.D. Va. 2022) 29

Cox Broad. Corp. v. Cohn,
420 U.S. 469 (1975) 34

Dahlstrom v. Sun-Times Media, LLC,
777 F.3d 937 (7th Cir. 2015) 26, 27, 28, 30

Davenport v. Wash. Educ. Ass'n,
551 U.S. 177 (2007) 31

De May v. Roberts,
9 N.W. 146 (Mich. 1881) 4, 32

Dex Media W., Inc. v. City of Seattle,
696 F.3d 952 (9th Cir. 2012) 23, 24

Dirkes v. Borough of Runnemede,
936 F. Supp. 235 (D.N.J. 1996) 3, 33

Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.,
472 U.S. 749 (1985) 22, 35

Elonis v. United States,
575 U.S. 723 (2015) 48

Fischer v. United States,
144 S. Ct. 2176 (2024) 43

Fla. Bar v. Went For It, Inc.,
515 U.S. 618 (1995) 38

Fla. Star v. B.J.F.,
491 U.S. 524 (1989) 14, 23, 34

Fort Wayne Books, Inc. v. Indiana,
489 U.S. 46 (1989) 47

Free Speech Coal. v. Att'y Gen. U.S.,
974 F.3d 408 (3d Cir. 2020) 46, 47

Friedman v. Martinez,
231 A.3d 719 (N.J. 2020) 4, 32

Frisby v. Schultz,
487 U.S. 474 (1988) 4, 31

FTC v. Accusearch Inc.,
570 F.3d 1187 (10th Cir. 2009) 34

FTC v. Wyndham Worldwide Corp.,
799 F.3d 236 (3d Cir. 2015) 34, 54

Grayned v. City of Rockford,
408 U.S. 104 (1972) 55

Greater Phila. Chamber of Com. v. City of Phila.,
949 F.3d 116 (3d Cir. 2020) 20, 21, 38, 41

Hill v. Colorado,
530 U.S. 703 (2000) 54

Holder v. Humanitarian L. Project,
561 U.S. 1 (2010) 54, 55

IMDb.com v. Becerra,
962 F.3d 1111 (9th Cir. 2020) 23, 24, 26

Jordan v. Jewel Food Stores, Inc.,
743 F.3d 509 (7th Cir. 2014) 20

Khimmat v. Weltman, Weinberg & Reis Co., LPA,
585 F. Supp. 3d 707 (E.D. Pa. 2022) 21

King v. Gen. Info. Servs., Inc.,
903 F. Supp. 2d 303 (E.D. Pa. 2012) 21

Kline v. Sec. Guards, Inc.,
159 F. Supp. 2d 848 (E.D. Pa. 2001) 48

Mainstream Marketing Services v. F.T.C.,
358 F.3d 1228 (10th Cir. 2004) 38, 49

Martin v. City of Struthers,
319 U.S. 141 (1943) 39

Matter of Subpoena 2018R00776,
947 F.3d 148 (3d Cir. 2020) 18

Mazo v. N.J. Sec'y of State,
54 F.4th 124 (3d Cir. 2022) ..... passim

Moody v. NetChoice, LLC,
144 S. Ct. 2383 (2024) ..... passim

N. Jersey Media Grp., Inc. v. Bergen Cnty. Prosecutor's Office,
964 A.2d 842 (N.J. Super. Ct. App. Div. 2009) 50

Nat'l Fed'n of the Blind v. FTC,
420 F.3d 331 (4th Cir. 2005) 39

Olmstead v. United States,
277 U.S. 438 (1928).....4, 31

Ostergren v. Cuccinelli,
615 F.3d 263 (4th Cir. 2010) 23, 51

Paroline v. United States,
572 U.S. 434 (2014).....44

Pavesich v. New England Life Ins. Co.,
50 S.E. 68 (Ga. 1905)..... 3, 4, 32

Pennsylvania v. Mimms,
434 U.S. 106 (1977).....36

Pension Benefit Guar. Corp. v. White Consol. Indus., Inc.,
998 F.2d 1192 (3d Cir. 1993)..... 17, 25

Philips v. Cnty. of Allegheny,
515 F.3d 224 (3d Cir. 2008).....13

Pitt News v. Pappert,
379 F.3d 96 (3d Cir. 2004)..... 52, 53

Publius v. Boyer-Vine,
237 F. Supp. 3d 997 (E.D. Cal. 2017) 23, 26, 47

R.A.V. v. City of St. Paul,
505 U.S. 377 (1992)..... passim

Reed v. Town of Gilbert,
576 U.S. 155 (2015) 26

Renton v. Playtime Theatres, Inc.,
475 U.S. 41 (1986) 28

Robert W. Mauthe, M.D., P.C. v. MCMC LLC,
387 F. Supp. 3d 551 (E.D. Pa. 2019) 33

Rosedale & Rosehill Cemetery Ass'n v. Twp. of Readington,
No. 21-1391, 2022 WL 996420 (3d Cir. Apr. 4, 2022) 55

Rowan v. U.S. Post Office Department,
397 U.S. 728 (1970) 39

Rubin v. Coors Brewing Co.,
514 U.S. 476 (1995) 36, 37, 49

S.F. Arts & Athletics, Inc. v. U.S. Olympic Comm.,
483 U.S. 522 (1987) 40

Santana Prod., Inc. v. Bobrick Washroom Equip., Inc.,
401 F.3d 123 (3d Cir. 2005) 14

Saunders v. Hearst Television, Inc.,
___ F. Supp. 3d ___, 2024 WL 126186 (D. Mass. Jan. 11, 2024) 21

Schrader v. District Attorney of York County,
74 F.4th 120 (3d Cir. 2023) 47, 48

Sheehan v. Gregoire,
272 F. Supp. 2d 1135 (W.D. Wash. 2003) 12, 29, 30

Sorrell v. IMS Health Inc.,
564 U.S. 552 (2011) 49

Sosa v. Onfido, Inc.,
600 F. Supp. 3d 859 (N.D. Ill. 2022) 29

Stark v. Patreon, Inc.,
656 F. Supp. 3d 1018 (N.D. Cal. 2023) 17, 20, 22, 33

State v. Fortin,
969 A.2d 1133 (N.J. 2009) 44

State v. Mrozinski,
971 N.W.2d 233 (Minn. 2022) 4

State v. Natale,
878 A.2d 724 (N.J. 2005) 13

State v. Taupier,
193 A.3d 1 (Conn. 2018) 8

Trans Union Corp. v. FTC,
267 F.3d 1138 (D.C. Cir. 2001) 21, 52

Turner Broad. Sys. v. FCC,
512 U.S. 622 (1994) 40

U.S. Dep't of Just. v. Reps. Comm. For Freedom of Press,
489 U.S. 749 (1989) 50

U.S. Healthcare, Inc. v. Blue Cross of Greater Phila.,
898 F.2d 914 (3d Cir. 1990) 19

United States v. Edge Broadcasting Co.,
509 U.S. 418 (1993) 51

United States v. Green Drugs,
905 F.2d 694 (3d Cir. 1990) 48

United States v. Hansen,
599 U.S. 762 (2023) 16, 25

United States v. O'Brien,
391 U.S. 367, 377 (1968) 35, 40

Vidal v. Elster,
602 U.S. 286 (2024) 18, 30, 31, 35

Village of Hoffman Estates v. Flipside, Hoffman Estates,
455 U.S. 489 (1982) 53, 54

Vrdolyak v. Avvo, Inc.,
206 F. Supp. 3d 1384 (N.D. Ill. 2016) 23

Vt. Agency of Nat. Res. v. U.S. ex rel. Stevens,
529 U.S. 765 (2000) 46

Ward v. Rock Against Racism,
491 U.S. 781 (1989) 27

Williams-Yulee v. Fla. Bar,
575 U.S. 433 (2015) 49

Yates v. Pinellas Hematology & Oncology, P.A.,
21 F.4th 1288 (4th Cir. 2021) 46

Statutes

705 Ill. Comp. Stat. Ann. 90/1-10 11

705 Ill. Comp. Stat. Ann. 90/2-5 (2012) 5, 10, 11, 40

Colo. Rev. Stat. Ann. § 18-9-313 (2002) 5

Daniel Anderl Judicial Security and Privacy Act of 2022, Pub. L. No. 117-263,
§§ 5932-5934, 136 Stat. 3458-66 ..... passim

Del. Code Ann. tit. 10, §§ 1921-1924 (2022) 10, 11, 40

Fla. Stat. § 843.17 (1997) 11

Kan. Stat. Ann. § 21-5905 (2010) 5

Md. Code Ann., Cts. & Jud. Proc. §§ 3-2301 to 3-2407 (2024) 10, 11, 40

N.J. Stat. Ann. § 1:1-10 13

N.J. Stat. Ann. § 19:44A-1 to -26 52

N.J. Stat. Ann. § 2C:20-31.1 (2016) 6, 8, 13

N.J. Stat. Ann. § 46:26A-6.....52

N.J. Stat. Ann. § 47:1-17.....13

N.J. Stat. Ann. § 47:1A-1.....49

N.J. Stat. Ann. § 47:1A-1.1.....8

N.J. Stat. Ann. § 47:1A-5.....8

N.J. Stat. Ann § 47:1B-1 ..... 10, 13, 44

N.J. Stat. Ann § 47:1B-2 ..... 10, 37, 45

N.J. Stat. Ann § 47:1B-3 ..... 42, 51

N.J. Stat. Ann. § 56:8-166.1..... passim

N.J. Stat. Ann. § 56:8-166.3..... 1, 8, 27, 36

Pub. L. No. 102-243, § 3, 105 Stat. 2395 33

Pub. L. No. 2015, ch. 226 6

Pub. L. No. 2020 ch. 125 8

Texas Gov't Code § 552.117(a)(1), (a)(15) (1993) 5

Wash. Rev. Code § 4.24.680 (2002).....12

47 U.S.C. § 227 (1991) 33

Regulations

Cal. Pub. Util. Code § 2891.1 55

N.J. Admin. Code § 19:25-10.2 52

Other Authorities

Joseph Story, Commentaries on the Constitution of the United States 704 (1833) 3

166 Cong. Rec. 213 (2020) 7, 23, 37

138 Cong. Rec. 1675 (Feb. 5, 1992) 34

Act of Mar. 1, 1889, ch. 319 33

Black's Law Dictionary (12th ed. 2024) 39

Charles Fried, *Privacy*, 77 Yale L.J. 475 (1968) 33

David H. Flaherty, *Privacy in Colonial New England 1630-1776* (1972) 3, 32

Disclose, Merriam-Webster.com 39, 42

Restatement (Second) of Torts §§ 652A-652E (Am. Law Inst. 1977) 4, 32

S.B. 575, 2024 Leg., 446th Sess. (Md. 2024) 7, 8

Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890) 4, 32

Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 Ind. L.J. 979 (2011) 32

U.S. Marshals Service, 2022 Judicial Security Fact Sheet (Feb. 17, 2022), https://tinyurl.com/4r3rb6ym 8

William L. Prosser, *Privacy*, 48 Calif. L. Rev. 383 (1960) 4, 32

PRELIMINARY STATEMENT

Some public servants face grave threats simply for doing their jobs. In recent years, judges and their family members have suffered horrific attacks, including murder. Judges and other officials have been facing an increased number of personal threats, too, facilitated by the ease through which their personal information can be found by those who would do them harm. New Jersey, unfortunately, is not immune from this appalling trend. The question in this case is how the State may combat it.

After the tragic death of Daniel Anderl, Judge Esther Salas's son, at the hands of a deranged attorney, New Jersey sought "to enhance the safety and security" of at-risk public officials. N.J. Stat. Ann. § 56:8-166.3. As relevant here, Daniel's Law does so by allowing current and former judges, law enforcement, prosecutors, child-protective-services investigators, and certain family members to request that private entities not "disclose … on the Internet or otherwise make available" their home addresses and/or unpublished home phone numbers. *Id.* § 56:8-166.1(a)(1), (d). A requestor must first, however, provide valid written notice, at which point the recipient has 10 business days to comply. *Id.* § 56:8-166.1(a)(1)-(2). If a recipient receives valid notice but fails to comply, they face civil penalties, which can be sought by the requestor or by an assignee. *Id.* § 56:8-166.1(b)-(c).

Nothing about that scheme is facially invalid under the First Amendment, let alone on a motion-to-dismiss posture. In seeking facial invalidation here, Defendants

must show that "no set of circumstances exists under which the law would be valid," or that it "lacks a plainly legitimate sweep." *Moody v. NetChoice, LLC*, 144 S. Ct. 2383, 2397 (2024). But the opposite is true. The Legislature was not motivated by any antipathy toward speech about home addresses and unpublished home phone numbers, nor was it otherwise seeking to distort the marketplace of ideas. On the contrary, the Legislature's aim was to give public officials most at risk of violence greater control over their own safety and privacy, which requires restricting data brokers and other entities that share their personal information, usually for commercial gain. It did so by empowering individuals to protect their own privacy *at home*, a tradition that has always coexisted with the First Amendment.

The law achieves that important public-safety goal, and reflects the venerable tradition of safety and privacy in one's home, in well-tailored ways. Because the Legislature was focusing on the substantial interest in ensuring that public officials have the tools to protect themselves, the law requires each individual to affirmatively request that an entity cease sharing their information. And because the Legislature was trained on public safety, its law limited the information that must be removed only to home addresses (where officials lack the security attendant to, *e.g.*, a courthouse) and their unpublished home phone numbers (a prime conduit for threats and similar intrusions). And because the government has other means to prevent its *own* dissemination of this information, Daniel's Law focuses on private entities, who

regularly sell such information for profit. Although Defendants protest the breadth of Daniel's Law, their claims either misread the law or rest on alternatives that would be far less effective at protecting these public servants' privacy and safety.

Defendants may ultimately seek to develop factual records in the consolidated cases to support claims that they either did not violate the law or warrant as-applied relief. But on this motion-to-dismiss posture, where their arguments would lead to the invalidation of this statute in all applications, their arguments fall far short.

BACKGROUND

A. The Right To Privacy And Safety In One's Home.

Since before the founding, the American legal tradition has recognized that one's home should be "a haven for solitude and intimacy" and "a barrier against intrusion by uninvited outsiders." David H. Flaherty, *Privacy in Colonial New England 1630-1776*, at 85 (1972). While "[t]he right to speak and the right of privacy have been coexistent," *Pavesich v. New England Life Ins. Co.*, 50 S.E. 68, 73 (Ga. 1905), one's right to speak has historically been limited such that "he does not injure any other person in his rights, person, property, or reputation," Joseph Story, Commentaries on the Constitution of the United States 704 (1833).

"Judicial recognition of the contours of an individual's right to privacy has been an evolutionary process." *Dirkes v. Borough of Runnemede*, 936 F. Supp. 235, 238-39 (D.N.J. 1996). Though property law was the earliest bulwark, *Pavesich*, 50

S.E. at 69, by the late nineteenth century, courts began to recognize a right to privacy in one's home that could be enforced through tort, *see De May v. Roberts*, 9 N.W. 146, 148-49 (Mich. 1881); *Pavesich*, 50 S.E. at 73; *Melvin v. Reid*, 297 P. 91, 92 (Cal. Ct. App. 1931) (collecting cases); *see also* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890). By the mid-twentieth century, most States had recognized such common law torts. *Friedman v. Martinez*, 231 A.3d 719, 729 (N.J. 2020); William L. Prosser, *Privacy*, 48 Calif. L. Rev. 383, 386-88 (1960). Those torts fell into four basic categories: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) "false light" publicity; and (4) appropriation of name or likeness. *Id.* at 389; *see* Restatement (Second) of Torts §§ 652A-652E (Am. Law Inst. 1977). Each reflected a different facet of one of "the most comprehensive of rights and the right most valued by civilized man": "the right to be let alone." *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

While this legal tradition recognizes that all people deserve safety and peace in their own homes, individuals occupying specific roles sometimes find themselves more likely to be targets of those who would pierce that solitude and security. *See, e.g.*, *Frisby v. Schultz*, 487 U.S. 474, 487 (1988) (targeted protests of doctor who performed abortions and his family "on their doorstep"); *State v. Mrozinski*, 971 N.W.2d 233, 237 (Minn. 2022) (threatening letter targeting child protective services

employees); *cf. also R.A.V. v. City of St. Paul*, 505 U.S. 377, 388 (1992) (noting constitutionality of specific law addressing threats against the President).

For decades, States have recognized that certain public servants and their families are especially likely to be targeted for violence, and have taken steps to protect them. In 1993, Texas expressly excluded contact information for government employees and judges from its public-records-access law. Texas Gov't Code § 552.117(a)(1), (a)(15) (1993). In 2002, Colorado made it a crime "to knowingly make available on the internet" a peace officer or their immediate family's personal information whenever the speaker knows or reasonable should know that doing so would "pose[] an imminent and serious threat to" their safety. Colo. Rev. Stat. Ann. § 18-9-313 (2002). In 2010, Kansas similarly criminalized knowingly disseminating "personal information" about a judge or their "immediate family member," if such dissemination "poses an imminent and serious threat to" their safety. Kan. Stat. Ann. § 21-5905(a)(7) (2010). Two years after that, Illinois prohibited public dissemination of "a judicial officer's personal information" once that officer requested in writing for it to be taken down. *See* 705 Ill. Comp. Stat. Ann. 90/2-5 (2012).

New Jersey, too, has long taken steps to protect its public servants. In 2015, the State enacted a law prohibiting the publication of law enforcement officers' and their immediate families' personal information, "with purpose to expose" them "to harassment or risk of harm to life or property, or in reckless disregard of the

probability of such exposure." Pub. L. No. 2015, ch. 226, § 1 (codified at N.J. Stat. Ann. § 2C:20-31.1 (2016)). That legislation—the precursor to the statute at issue here—allowed a law enforcement officer or household member to obtain civil remedies if someone disclosed their home address or unpublished home phone number on the internet "under circumstances in which a reasonable person would believe that" doing so "would expose another to harassment or risk of harm to life or property." *Id.* § 3 (codified at N.J. Stat. Ann. § 56:8-166.1 (2016)).

B. The Growing Urgency Of Such Protections.

Increasing threats against judges and other public officials have made such provisions more critical. "In recent years, … members of the Federal judiciary have been exposed to an increased number of personal threats in connection to their role." Daniel Anderl Judicial Security and Privacy Act of 2022, Pub. L. No. 117-263, § 5932(a), 136 Stat. 3458-59 (findings). A driving factor is "the rise in the use of social media and online access to information": the "ease of access" to information "has considerably lowered the effort required for malicious actors to discover where individuals live," which can leave judges, other public servants, and their families uniquely vulnerable to those who wish to do them harm. *Id.* Even relatively minor examples can give pause: disaffected individuals, for instance, have taken to social media to call for an "angry mob" to gather outside a federal judge's home after that judge's address circulated online, while another post, referencing a U.S. Court of

Appeals judge, emphasized "how easy it would be to 'get them.'" *Id.*

Worse still, in the past decade, "several members of the Federal judiciary have experienced acts of violence against themselves or a family member in connection to their Federal judiciary role." *Id.* § 5932(a)(4). In 2005, a disaffected litigant murdered the family of Judge Joan Lefkow, a U.S. District Judge for the Northern District of Illinois. *Id.* In June 2013, a federal judge in Florida was "targeted by a gunman who purchased the address of his Florida home on the internet for a mere $1.95." 166 Cong. Rec. 213 (2020). "The gunshot missed his ear by less than 2 inches." *Id.* And "in 2020, three shooters openly fired upon the Camden home of two New Jersey police officers and their 10-day old infant." Compl. ¶ 13.[1] In October 2023, hours after a Maryland judge issued a ruling in a divorce-and-custody case, one of the litigants found and shot the judge outside of his home. S.B. 575, 2024 Leg., 446th Sess., at 2 (Md. 2024); Compl. ¶ 14.

These horrifying examples are illustrative of a broader trend. Between 2015 and 2019, "threats and other inappropriate communications against Federal judges and other judiciary personnel increased from 926 in 2015 to approximately 4,449 in 2019"—a five-fold increase. § 5932(a)(3). In 2021 alone, the Marshal's Service reported 4,511 threats to the federal judiciary. *See* U.S. Marshals Service, 2022

[1] Unless otherwise noted, all citations to "Compl." are to the Complaint in *Atlas Data Privacy Corp. et al v. Blackbaud Inc., et al.*, No. 1:24-cv-3993 (D.N.J).

Judicial Security Fact Sheet (Feb. 17, 2022), https://tinyurl.com/4r3rb6ym. These threats are not limited to federal judges. In the past three years, three targeted shootings of state court judges have occurred. S.B. 575, 2024 Leg., 446th Sess., at 2 (Md. 2024); *see also, e.g.*, *State v. Taupier*, 193 A.3d 1, 9 (Conn. 2018) (family-court litigant discussing distance between judge's "master bedroom and a cemetery that provides cover and concealment," along with physics of specific-caliber rifle shot over that distance and "dying as I change out to the next [thirty rounds]").

C. Daniel's Law.

New Jersey is not immune from this horrific trend. In July 2020, a deranged attorney with a case before Judge Esther Salas murdered Judge Salas's son, Daniel Anderl, and critically wounded Judge Salas's husband, Mark Anderl, at the front of door of their home. Compl. ¶¶ 5-6; *see* § 5932(a)(5), 136 Stat 3459. The murderer, who had intended to kill Judge Salas, had obtained the judge's home address using one of the various "people finder" resources available online. Compl. ¶ 7.

In November 2020, in the wake of that tragedy, the New Jersey Legislature enacted Daniel's Law. *See* Pub. L. No. 2020, ch. 125 (codified as amended at N.J. Stat. Ann. §§ 47:1A-1.1, -5; *id.* § 47:1-17; *id.* § 2C:20-31.1; and *id.* §§ 56:8-166.1-166.3). Daniel's Law exists "to enhance the safety and security of certain public officials in the justice system" such that they can "carry out their official duties without fear of personal reprisal." N.J. Stat. Ann. § 56:8-166.3. It achieves those

goals, in relevant part, by providing judges, law enforcement officers, prosecutors, child-protective-services investigators, and immediate family members living in the same household (collectively "covered persons") with a legally enforceable mechanism to request that a private "person, business, or association" not "disclose … on the Internet or otherwise make available" their home address and/or unpublished home telephone number. *Id.* § 56:8-166.1(a)(1), (d).

That mechanism requires a formal request and provides time for compliance. The request must come from an "authorized person"—either a covered person or a designee—and must give the recipient of the request "written notice" that the requestor "is an authorized person." *Id.* § 56:8-166.1(a)(2). Within 10 business days of receipt, the recipient must then cease sharing the covered person's home address or unpublished home phone number with others. *Id.* § 56:8-166.1(a)(1). In other words, the law does not prohibit dissemination of a covered person's contact information as a blanket matter, but only requires it when a valid request is received, and only after affording the recipient 10 business days to comply.

If a recipient fails to comply within that time, the recipient is civilly liable. Specifically, the law provides for (1) "actual damages, but not less than liquidated damages" of $1,000 per violation; (2) "punitive damages upon proof of willful or reckless disregard"; (3) "reasonable attorney's fees and other litigation costs reasonably incurred"; and (4) "any other preliminary and equitable relief as the court

determines to be appropriate." *Id.* § 56:8-166.1(c). A covered person may, in writing, assign their right to bring a civil action in response to a violation. *Id.* § 56:8-166.1(d).

Daniel's Law also provides a mechanism for authorized persons to request nondisclosure of their home addresses from public agencies. To process such requests, Daniel's Law created the Office of Information Privacy (OIP), and directed OIP to establish a "secure portal" through which requestors can submit (or revoke) requests for redaction or nondisclosure. *Id.* § 47:1B-1(c)(1). Assuming the request is valid and thus approved by OIP's Director, the entity must cease sharing the information within 30 calendar days of the Director's approval. *Id.* § 47:1B-2 (b).

D. Recent Legislation In Other Jurisdictions.

Other States, along with the Federal Government, have also taken action in the face of these recent, troubling trends. *E.g.*, Pub. L. No. 117-263, 136 Stat. 3453-3458 (2022); Md. Code Ann., Cts. & Jud. Proc. §§ 3-2301 to 3-2407 (2024); Del. Code Ann. tit. 10, §§ 1921-1924 (2022). Like Daniel's Law, these statutes typically apply to specific public servants and certain family members/cohabitants, and require a valid written request.[2] Also like Daniel's Law, some of these statutes also allow for assignment of authority to act on behalf of covered persons. *See* § 5934(b)(1); Del. Code Ann. tit. 10, § 1924(d). And while several comparator laws

[2] *See* §§ 5933(1), 5934(d)(1); Md. Code Ann., Cts. & Jud. Proc. §§ 3-2301(e)(6), 3-2303(d); Del. Code Ann. tit. 10, §§ 1921, 1923; 705 Ill. Comp. Stat. Ann. 90/2-5.

use the same "opt-in" mechanism as Daniel's Law, they have shorter compliance windows, in several cases affording recipients only 72 hours to remove covered information.[3] Further, while Daniel's Law protects only home addresses and unpublished home phone numbers, other statutes restrict more information.[4]

Other jurisdictions have gone further. Some, for instance, have made it a crime to disseminate a law enforcement officer's address or phone number "without authorization" of their employer, *see* Fla. Stat. § 843.17 (1997), *invalidated by Brayshaw v. City of Tallahassee*, 709 F. Supp. 2d 1244 (N.D. Fla. 2010), or similarly prohibited dissemination of personal information (including a "birthdate") without the employee's "express written permission," *see* Wash. Rev. Code § 4.24.680 (2002), *invalidated by Sheehan v. Gregoire*, 272 F. Supp. 2d 1135 (W.D. Wash. 2003). By contrast, Daniel's Law and others like it require an affirmative request.

E. This Proceeding.

This proceeding stems from claims brought by Plaintiff Atlas Data Privacy Corporation, the assignee for thousands of covered persons, alleging that Defendants failed to cease disclosing information within 10 business days of receiving valid

[3] § 5934(d)(2)(A)(i); Md. Code Ann., Cts. & Jud. Proc. § 3-2303(d)(1); Del. Code Ann. tit. 10, § 1923(b)(1); 705 Ill. Comp. Stat. Ann. 90/2-5(b)(1).

[4] *E.g.*, § 5933(2)(A) (*e.g.*, license plate or similar vehicle-identifying numbers, tax and banking information, and personal email address); Md. Code Ann., Cts. & Jud. Proc. § 3-2301(d) (similar); Del. Code Ann. tit. 10, § 1921(6) (similar); 705 Ill. Comp. Stat. Ann. 90/1-10 (similar).

requests. Compl. ¶¶ 25-26, 57-60. Nearly all Defendants are for-profit entities, including "direct-mailing and marketing companies" and "data brokers." Consolidated Mot. to Dismiss Br., ECF 27-33 (Br.), at 18-19.

Plaintiff filed complaints against Defendants in New Jersey Superior Court. Seventy-three of the complaints were removed to this Court. Br.16-17. Defendants collectively sought to dismiss on the alleged ground that Daniel's Law is facially unconstitutional, and this Court set a briefing schedule. ECF 15, No. 1:24-cv-4037. This Court also ordered that the Attorney General be notified of the facial challenge, and permitted the Attorney General to intervene to defend the law's validity. ECF 17, No. 1:24-cv-4141. This opposition to Defendants' facial challenge now follows.

STANDARD OF REVIEW

In assessing a motion to dismiss for failure to state a claim, a court asks only whether the complaint contains "sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)**Error! Bookmark not defined.** (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A court therefore 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]," *Philips v. Cnty. of Allegheny*, 515 F.3d 224, 228 (3d Cir. 2008), while evaluating plaintiff's "legal conclusions" for itself, *Iqbal*, 556 U.S. at 678. Generally speaking, in undertaking this analysis, a court considers "only the

allegations contained in the complaint, exhibits attached to the complaint and matters of public record." *City of Pittsburgh v. W. Penn Power Co.*, 147 F.3d 256, 259 (3d Cir. 1998).

ARGUMENT

I. DEFENDANTS' FACIAL ATTACK SHOULD BE DENIED.

This Court should deny Defendants' motion to dismiss because Daniel's Law is not facially unconstitutional under the First Amendment.[5] As an initial matter, this facial challenge faces an extraordinarily high bar to succeed. And in undertaking this facial inquiry, this Court should apply only intermediate scrutiny, for three independent reasons: Daniel's Law (1) covers commercial speech; (2) is not content-discriminatory; and (3) accords with a longstanding tradition of privacy regulation that vitiates the need for strict scrutiny. And because Daniel's Law easily satisfies intermediate scrutiny (and, indeed, any level of constitutional scrutiny), Defendants' facial attack must be denied.

[5] Though Defendants refer to Daniel's Law as a totality, their precise challenge is to the operative provisions of N.J. Stat. Ann. § 56:8-166.1. This brief likewise refers to "Daniel's Law" for simplicity, but emphasizes that Section 166.1 is plainly severable and that therefore any finding of invalidity would not apply to the law's other provisions. *E.g.*, N.J. Stat. Ann. § 2C:20-31.1; *id.* § 47:1-17; *id.* §§ 47:1B-1 to -2; *see* N.J. Stat. Ann. § 1:1-10 (requiring severance to the greatest extent possible); *State v. Natale*, 878 A.2d 724, 740 (N.J. 2005) (detailing New Jersey's strong tradition of "judicial surgery" and severance "to save the major objectives" of a law).

A. Defendants' Facial Challenge Must Meet An Extremely High Bar.

"For a host of good reasons, courts usually handle constitutional claims case by case, not en masse." *NetChoice, LLC*, 144 S. Ct. at 2397. Facial attacks, after all, "often rest on speculation" about a statute's sweep and "future enforcement" and, further, "threaten to short circuit the democratic process by preventing duly enacted laws from being implemented in constitutional ways." *Id.* (cleaned up). Mindful of these problems with facial challenges, the Supreme Court has made such wholesale attacks "hard to win." *Id.*; *see also Santana Prods., Inc. v. Bobrick Washroom Equip., Inc.*, 401 F.3d 123, 130-31 (3d Cir. 2005) ("[I]t is well established that courts have a duty to avoid passing upon a constitutional question if the case may be disposed of on some other ground." (citation omitted)).

Courts have been especially loathe to issue sweeping rulings where privacy interests and speech interests clash. *See, e.g.*, *Fla. Star v. B.J.F.*, 491 U.S. 524, 533 (1989) ("We continue to believe that the sensitivity and significance of the interests presented in clashes between First Amendment and privacy rights counsel relying on limited principles that sweep no more broadly than the appropriate context of the instant case."); *Bartnicki v. Vopper*, 200 F.3d 109, 117 (3d Cir. 1999) ("In keeping with the Supreme Court's approach to deciding these illustrative cases, we will resolve the present controversy not by mechanically applying a test … , but by reviewing First Amendment principles in light of the unique facts and circumstances

of this case."), *aff'd*, 532 U.S. 514 (2001).[6] That is, of course, the case here.

In resolving this motion, this Court should apply the traditional standard for facial challenges, not the unique overbreadth standard. The usual facial test requires that the challenger "establish that no set of circumstances exists under which the law would be valid," or show "that the law lacks a plainly legitimate sweep." *NetChoice*, 144 S. Ct. at 2397 (cleaned up). Defendants' consolidated brief raises only this type of facial challenge, and thus implicates only this standard. *Cf.* Br.27 (alluding briefly to overbreadth doctrine only in single parenthetical). Most of the other, individual motion-to-dismiss briefs likewise avoid invoking the overbreadth standard.

It is unclear whether the Thomson Reuters Defendants intend to raise a facial overbreadth challenge, *cf.* ECF 28, No. 1:24-cv-4269 (Thomson Reuters Br.), at 1, 5 (calling statute "overbroad"), but, even if they do, that effort cannot succeed. For one, the "cursory treatment" they afford the overbreadth claim—failing to explain how the doctrinal standard works—is insufficient to bring the issue before this Court. *See Barna v. Bd. of Sch. Dirs. of Panther Valley Sch. Dist.*, 877 F.3d 136, 148 (3d Cir. 2017). For another, any such claim is fatally premature. Overbreadth permits

[6] For that reason, the Whitepages Defendants' reliance on these cases—in addition to overlooking that those cases involved matters of public concern, *see infra* at 34—is particularly ill-suited to this facial posture. *See* ECF 41, No. 1:24-cv-3998. If, for instance, a case arises in which residency became a matter "of public significance," *id.* at 5, such a dispute could then be addressed on its specific facts (though it is unclear why someone's precise street address would be a matter of public concern).

a party whose speech *is* proscribable without offending the First Amendment to still "vindicate the rights" of others whose speech is chilled. *United States v. Hansen*, 599 U.S. 762, 769-70 (2023). Such a claim triggers "a less demanding though still rigorous standard," which requires a court to determine whether "a substantial number of the law's applications are unconstitutional, judged in relation to the statute's plainly legitimate sweep." *NetChoice*, 144 S. Ct. at 2397 (cleaned up). In other words, an overbreadth challenge requires analyzing both parts of the ratio: to "assess" the law's full "scope"; to answer which of its "applications violate the First Amendment"; and then to "measure them against the rest." *Id.* at 2398.

That is difficult to do at this stage. Because overbreadth requires a court to total up both the law's "impermissible and permissible" applications and "compare the two sets," *id.*, it is an inquiry in which "[e]vidence is key," *Mazo v. N.J. Sec'y of State*, 54 F.4th 124, 152 (3d Cir. 2022), *cert. denied*, 144 S. Ct. 76 (2023). So courts typically cannot "undertake the needed inquiries" if "the record is underdeveloped." *NetChoice*, 144 S. Ct. at 2398-99—as it inherently is on a motion-to-dismiss posture. For that reason, courts have rejected facial overbreadth challenges brought via motions to dismiss in closely analogous contexts. *See, e.g.*, *Boelter v. Advance Mag. Publishers Inc.*, 210 F. Supp. 3d 579, 603 (S.D.N.Y. 2016) (deferring publisher's overbreadth challenge to data privacy law); *Stark v. Patreon, Inc.*, 656 F. Supp. 3d

1018, 1039 (N.D. Cal. 2023) (same); *see also NetChoice*, 144 S. Ct. at 2409 (remanding for lower courts to do this intensive analysis).

The same issue would arise here. If the Thomson Reuters Defendants wished to argue that Daniel's Law's "unconstitutional applications substantially outweigh its constitutional ones," *NetChoice*, 144 S. Ct. at 2397, they would need to point to "evidence of both the existence and prevalence of such unconstitutional applications," *Mazo*, 54 F.4th at 152. But in deciding a motion to dismiss, courts typically may consider "only the allegations contained in the complaint, exhibits attached to the complaint and matters of public record." *Pension Benefit Guar. Corp. v. White Consol. Indus., Inc.*, 998 F.2d 1192, 1196 (3d Cir. 1993). Thus, if these Defendants seek to raise an overbreadth challenge now, they can do so only on the allegations in *Plaintiffs'* complaints—an obviously insufficient record to prevail.

In sum, this Court should address the pending motions to dismiss under the default facial standard, and can reject these motions so long as *some* "set of circumstances exists under which the law would be valid" and the law has "a plainly legitimate sweep." *NetChoice*, 144 S. Ct. at 2397 (cleaned up).

B. This Facial Attack Implicates Only Intermediate Scrutiny.

For three independent reasons, assessing the facial challenge to Daniel's Law requires applying only intermediate scrutiny. First, Daniel's Law regulates primarily commercial speech, so the law cannot be facially invalid unless it fails the *Central*

Hudson test—a type of intermediate scrutiny. *See Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y.*, 447 U.S. 557, 566 (1980); *see also City of Austin v. Reagan Nat'l Advert. of Austin, LLC*, 596 U.S. 61, 68 n.3, 73-74 (2022) (noting that commercial-speech restrictions are subject to *Central Hudson* scrutiny even if content-based). Second, the law is content-neutral—another basis to apply intermediate scrutiny. *Matter of Subpoena 2018R00776*, 947 F.3d 148, 155 (3d Cir. 2020). Third, Daniel's Law reflects a tradition of protecting the privacy and safety of individuals in their own homes—one that coexists with the First Amendment and does not threaten the marketplace of ideas. *See Vidal v. Elster*, 602 U.S. 286, 299-300 (2024). For each reason, intermediate—not strict—scrutiny applies.

1. Defendants Cannot Avoid *Central Hudson* Scrutiny.

As noted, all this Court would need to acknowledge to dispose of Defendants' facial challenge is that at least some "set of circumstances exists under which the law would be valid," and that the law has at least some "plainly legitimate sweep." *NetChoice*, 144 S. Ct. at 2397 (citations omitted). The most obvious area of coverage is the one present in these very cases: commercial sales of contact information by for-profit entities whose business model involves making such contact information available. *See* Compl. ¶¶ 39-40, *Atlas Data Privacy Corp. v. Acxiom LLC*, No. 1:24-cv-4107 (D.N.J) (alleging that disclosure of covered data is core to "Defendants' business model"); *accord* Br.18 & nn.14-15 (acknowledging that Defendants

include "direct-mailing and marketing companies," "data brokers," and other "entities that provide fundraising solutions" and noting specific Defendants). Those applications doubtlessly burden only commercial speech.

No bright-line test distinguishes commercial from non-commercial speech in all circumstances, but when data itself is the commodity, courts have little trouble recognizing that restrictions on the for-profit provision of data are commercial-speech restrictions. Commercial speech is "expression related solely to the economic interests of the speaker and its audience," *Cent. Hudson*, 447 U.S. at 561—a label that obviously applies to a business that hopes to profit by selling home addresses. In determining whether speech ultimately qualifies as commercial, courts typically consult three non-exclusive factors drawn from *Bolger v. Youngs Drug Prods. Corp.*, 463 U.S. 60 (1983). *See U.S. Healthcare, Inc. v. Blue Cross of Greater Phila.*, 898 F.2d 914, 933 (3d Cir. 1990). Those factors are: (1) whether "the speech refer[s] to a specific product or service," (2) whether the speech is an advertisement; and (3) whether the speaker has "an economic motivation for the speech." *Greater Phila. Chamber of Com. v. City of Phila.*, 949 F.3d 116, 137 (3d Cir. 2020). "[A]ll three characteristics need not be present for a given expression to qualify." *Id.*[7]

[7] The Court has also described core commercial speech as that which only "propose[s] a commercial transaction," *Bd. of Trs. of State Univ. of N.Y. v. Fox*, 492 U.S. 469, 473-74 (1989); *see also Bank of Hope v. Miye Chon*, 938 F.3d 389, 395 n. † (3d Cir. 2019), but "courts view this definition as just as starting point," *Ariix, LLC*

Courts applying this "fact-driven" rubric, *Ariix*, 985 F.3d at 1115, regularly hold that disclosing personal information for profit is commercial speech. Take the Northern District of California's recent decision in *Stark*, 656 F. Supp. 3d 1018. There, the court considered a motion to dismiss by a web platform sued for alleged violations of the federal Video Privacy Protection Act (VPPA), in which the platform argued that the VPPA's restrictions on sharing of user data violated its First Amendment rights. *Id.* at 1021-22. In assessing whether the speech was "commercial," the court took a "common-sense" approach, noting that the information "is arguably itself a product," that disclosure was "motivated by the commercial interests of both" the seller and the buyer, and that the data at issue had "no expressive or creative content beyond the fact of Plaintiffs' personal information and interactions, contain[ed] nothing of public interest, and serv[ed] no non-economic purpose to either the speaker or the recipient." *Id.* at 1033-34.

A significant number of decisions find similar speech to be commercial. *See, e.g.*, *Saunders v. Hearst Television, Inc.*, ___ F. Supp. 3d ___, 2024 WL 126186, at *5 (D. Mass. Jan. 11, 2024) (sharing of data regarding video viewing history and personal information); *Khimmat v. Weltman, Weinberg & Reis Co., LPA*, 585 F. Supp. 3d 707, 714-15 (E.D. Pa. 2022) (debt collectors sharing information about

v. NutriSearch Corp., 985 F.3d 1107, 1115 (9th Cir. 2021) (quoting *Jordan v. Jewel Food Stores, Inc.*, 743 F.3d 509, 516 (7th Cir. 2014)).

debts with third parties); *Boelter v. Hearst Commc'ns, Inc.*, 192 F. Supp. 3d 427, 445 (S.D.N.Y. 2016) (disclosure of purchasers' identities "related to the economic interests of the speaker and the audience"); *Advance Mag.*, 210 F. Supp. 3d at 597 (disclosure and sale of subscriber information to "data miners" and to other "organizations that use it for solicitation purposes"); *King v. Gen. Info. Servs., Inc.*, 903 F. Supp. 2d 303, 306-09 (E.D. Pa. 2012) (restrictions on credit-report information imposed by Fair Credit Reporting Act analyzed under *Central Hudson*); *accord Trans Union Corp. v. FTC*, 267 F.3d 1138, 1140-42 (D.C. Cir. 2001) (same).

Applying Daniel's Law to data brokers and other for-profit sellers of contact information—which constitutes much if not most of the law's coverage—likewise qualifies as a commercial-speech restriction. Here too, the information itself *is* the "specific product," and is driven solely by "an economic motivation." *Greater Phila. Chamber*, 949 F.3d at 137. The applications of Daniel's Law that prevent further dissemination of this information impact "no expressive or creative content beyond the fact of [covered persons'] personal information," contain "nothing of public interest," and serve "no non-economic purpose to either the speaker or the recipient," *Stark*, 656 F. Supp. 3d at 1034, which explains why they merit only the "reduced constitutional protection" applicable to commercial speech, *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 761-62 & n.8 (1985). By the same token, such speech is more durable, being "an economic act" from which businesses enjoy

an "increasing ability to profit," and thus does not require more exacting scrutiny. *Hearst*, 192 F. Supp. 3d at 445; *see Dun & Bradstreet*, 472 U.S. at 758 n.5, 762 (noting commercial speech is "hardy" and "less likely to be deterred"). In short, the sale or marketing of covered persons' information by for-profit companies unrelated to any expressive purpose—the heart of this law's coverage—is commercial speech.

Defendants' assertion that their "economic motivation" alone is insufficient to make the speech commercial, Br.24 (quoting *Bolger*, 463 U.S. at 67), is not to the contrary. The point the Court was making in *Bolger* is uncontroversial: if a speaker's economic motivation alone were sufficient, then most books, films, and newspapers would qualify as no more than commercial speech. *See* 463 U.S. at 67; *see also Bigelow v. Virginia*, 421 U.S. 809, 818 (1975). But the difference between that speech and run-of-the-mill data-brokering is clear, because in the latter case, sharing a home address implicates no "expressive or creative" interests, *see Stark*, 656 F. Supp. 3d at 1034, whereas the author who publishes a book, even if motivated by a desire to profit, engages in speech that is itself expressive and creative, regardless of its commercial purpose. The same can hardly be said for a website that offers to sell a judge's home address for $1.95. *See* 166 Cong. Rec. 213.[8]

[8] Naturally, the analysis could be different in the context of an as-applied challenge brought by a speaker whose interests really *are* expressive. *Cf. Ostergren v. Cuccinelli*, 615 F.3d 263, 269-272, 287 (4th Cir. 2010) (as-applied injunction where advocate posted prominent individuals' personal information as part of campaign

The cases on which Defendants principally rely—*Vrdolyak v. Avvo, Inc.*, 206 F. Supp. 3d 1384 (N.D. Ill. 2016); *Dex Media W., Inc. v. City of Seattle*, 696 F.3d 952 (9th Cir. 2012); and *IMDb.com v. Becerra*, 962 F.3d 1111 (9th Cir. 2020), Br.24-25—are distinguishable. *Vrdolyak*, for instance, involved an attorney who sued a free online directory of attorneys under the Illinois Right of Publicity Act, claiming that the platform had misappropriated his identity "by placing ads for competing attorneys on his profile page." 206 F. Supp. 3d at 1385-86. The district court ruled that the platform was shielded from liability by the First Amendment, reasoning that the platform itself was not engaged in "commercial speech" simply because it ran advertisements, much the same way that a newspaper was not. *Id.* at 1388-89. Even assuming that is correct, the ruling in no way suggests that an entity whose business model is *selling* personal information is not engaged in commercial speech.

Dex Media West, similarly, involved a challenge to a municipal ordinance that regulated telephone directories "as a whole," rather than "individual advertisements contained therein." 696 F.3d at 957. In that context, the court declined to treat the

---

against government mismanagement of such information); *Publius v. Boyer-Vine*, 237 F. Supp. 3d 997, 1016 (E.D. Cal. 2017) (similar, where gun-rights advocates created "database" of legislators' information to protest legislators' perceived creation of database of gun owners). That question is not presented here and would have to be assessed on its own as-applied factual record—consistent with how courts normally address constitutional challenges, most of all when speech and privacy rights collide. *See NetChoice*, 144 S. Ct. at 2397; *Fla. Star*, 491 U.S. at 532-33; *cf.* ECF 16-1, No. 1:24-cv-4324, at 4-10 (brief of two nonprofits who publish voter records, raising essentially as-applied claims).

directories "differently from newspapers, magazines," and other media that display advertisements, *id.* at 965, emphasizing that the directories featured significant noncommercial information, like "community information, maps, and government lists," *id.* at 954; *see id.* at 959; that the commercial elements took up "only a limited fraction of the space in the phone book," *id.* at 963; and that the State required phone companies to distribute them, "demonstrating that the directories serve more than a commercial purpose," *id.* at 957. Again, even assuming the holding is correct, it lends no support to the untenable suggestion that a data broker's sale of a judge's home address is *itself* non-commercial speech. *Cf. also IMDB.com*, 962 F.3d at 1121-22 (finding "wiki-style" database including public information about actor ages not commercial speech, as content was "encyclopedic, not transactional").

Finally, to the extent this Court considers a facial overbreadth analysis on this motion-to-dismiss posture, *but see supra* Part I.A, that challenge would necessarily fail at this stage. "[O]verbreadth analysis does not normally apply to commercial speech" at all, *e.g.*, *Fox*, 492 U.S. at 481, and on this record, there can be no serious dispute that a substantial number of Daniel's Law's applications concern only commercial speech, *e.g.*, Compl. ¶¶ 39-40, *Acxiom LLC*, No. 1:24-cv-4107; *Pension Benefit Guar. Corp.*, 998 F.2d at 1195 (facts alleged must be taken as true on motion to dismiss). Given the posture, any Defendants who tried to raise an overbreadth claim would not be able to show "a lopsided ratio" of unconstitutional to

constitutional applications, *see Hansen*, 599 U.S. at 770—which helps explain why most if not all Defendants have properly eschewed an overbreadth claim thus far.

2. Daniel's Law Is Content-Neutral.

Intermediate scrutiny is the proper standard to apply in adjudicating this facial challenge for another reason: the law is content-neutral. The law's coverage hinges on whether someone has requested non-disclosure of information that is private, non-expressive, and regulated only because of the risks the information poses to privacy and security, not because of any impact on the marketplace of ideas.

The Supreme Court has made clear that assessing content-discrimination requires a more nuanced inquiry than simply asking whether one has to know the content of the speech to know if the law applies. Specifically, a regulation of speech is "facially content based" if it "targets speech based on its communicative content—that is, if it applies to particular speech because of the topic discussed or the idea or message expressed." *City of Austin*, 596 U.S. at 69 (cleaned up). "Content neutral laws, on the other hand, do not regulate speech based on its content, but rather do so based on some other neutral characteristic of the speech." *Mazo*, 54 F.4th at 148. That means that a law that restricts speech can be content-neutral even though applying it "may require some evaluation of the speech." *City of Austin*, 596 U.S. at 72. So long as the law "is 'agnostic as to content'" and thus "requires an examination of speech only in service of drawing neutral lines," it is content-neutral. *Mazo*, 54

F.4th at 149 (quoting *City of Austin*, 596 U.S. at 69).[9]

A key indicator that Daniel's Law is "agnostic as to content," *id*., is its opt-in mechanism. Courts have recognized that a law is content-neutral where it "proscribes only the publication of personal information that has been obtained from" a specific source, and thus is "agnostic to the dissemination of the very same information acquired from a lawful source." *See Dahlstrom v. Sun-Times Media, LLC*, 777 F.3d 937, 949 (7th Cir. 2015). In *Dahlstrom*, the Seventh Circuit rejected a First Amendment challenge to the U.S. Driver's Privacy Protection Act (DPPA), which prohibited the disclosure of personal information obtained "from a motor vehicle record." *Id.* at 939. The court found the provision content neutral, emphasizing the law allowed "publication of identical information so long as that information flows from a source other than driving records," and thus implicated First Amendment rights "to a far lesser extent than would restraints on dissemination of information in a different context." *Id.* at 950. After all, "Congress crafted the DPPA's limitation on disclosure of personal information not because it disagreed with the message communicated by drivers' personal details," but only as a result of

[9] In the wake of the Supreme Court's decision in *Reed v. Town of Gilbert*, 576 U.S. 155 (2015), courts did occasionally overread language in that opinion to suggest that a statute qualified as content-based so long as its application could be determined by looking at whether it covered certain content and not other content. *E.g.*, *IMDb.com*, 962 F.3d at 1120 (citing *Reed*); *Publius*, 237 F. Supp. at 1012-13 (same). The Court's 2022 decision in *City of Austin* put that "read-the-sign" rule to rest, 596 U.S. at 61, rendering such pre-*Austin* analyses particularly unpersuasive.

"public safety goals … 'unrelated to the content of [the regulated] expression.'" *Id.* (quoting *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989)).

The same is true of Daniel's Law. Daniel's Law proscribes the disclosure of a covered person's information only if the discloser has received a valid notice requesting that the information not be disclosed. *See* N.J. Stat. Ann. § 56:8-166.1(a). Thus, like the DPPA, Daniel's Law is "agnostic to the dissemination of" such information when *no request* for non-disclosure has been made. *See Dahlstrom*, 777 F.3d at 949. As a result, Daniel's Law "implicates the First Amendment rights of the restricted party to a far lesser extent than would" a blanket restraint on dissemination of such information. *Id.* at 950. Not only that, but this choice shows the Legislature was not motivated by any disagreement with the topic or message, but simply sought to allow particularly threatened individuals to safeguard their own "safety and security" as they saw fit. N.J. Stat. Ann. § 56:8-166.3. Like the DPPA, Daniel's Law is therefore content-neutral, "because its public safety goals are unrelated to the content of the regulated expression." *Dahlstrom*, 777 F.3d at 950 (cleaned up).

Further, even if Daniel's Law necessarily applies to some content and not other content (*e.g.*, home addresses but not birthdays), that does not mean that it "*target[s]* speech based on its communicative content," *City of Austin*, 596 U.S. at 69 (emphasis added). "[A]ccording differential treatment" to one subclass of speech does not trigger strict scrutiny when that subclass is "associated with particular

'secondary effects' of the speech, so that the regulation is '*justified* without reference to the content of the … speech." *R.A.V.*, 505 U.S. at 389 (quoting *Renton v. Playtime Theatres, Inc.*, 475 U.S. 41, 48 (1986)). Such a law does not apply to a type of speech "*because of* the topic discussed or the idea or message expressed," *City of Austin*, 596 U.S. at 69 (emphasis added), but rather based on "some other neutral characteristic of the speech," *Mazo*, 54 F.4th at 148—*e.g.*, that a judge is concerned that availability of her home address online would enable a deranged litigant to show up at her family's doorstep and do them harm and thus has requested its removal. Nothing about that "raises the specter that the Government may effectively drive certain ideas or viewpoints from the marketplace." *R.A.V.*, 505 U.S. at 387 (calling this the "rationale of the general prohibition" against content discrimination).

Defendants are therefore incorrect to argue that Daniel's Law "restricts speech based on its communicative content." Br.23. Rather, the law is concerned with—and its application turns on—whether the covered person has requested nondisclosure, and the fact the individual's contact information could put them in danger. Because the law does not "target speech based on its communicative content," it is neutral. *See City of Austin*, 596 U.S. at 69; *see also, e.g.*, *Sosa v. Onfido, Inc.*, 600 F. Supp. 3d 859, 880 (N.D. Ill. 2022) (BIPA was content-neutral because "biometric identifiers" did not "relate to the communicative content of that information"); *ACLU v. Clearview AI, Inc.*, No. 20 CH 4353, 2021 WL 4164452, at *7 (Ill. Cir. Ct.

Aug. 27, 2021) (same); *Courthouse News Serv. v. Hade*, 631 F. Supp. 3d 349, 361-62 (E.D. Va. 2022) (deeming regulation restricting attorneys' remote access to court records content-neutral as it "does not center around disagreement with the message it conveys, turn upon the communicative contents of the court records, nor change based on viewpoint or subject matter" but merely regulated electronic access).

Defendants' reliance on *Brayshaw*, 709 F. Supp. 2d 1244 (N.D. Fla.), and *Sheehan*, 272 F. Supp. 2d 1135 (W.D. Wash.), *see* Br.23, is also misplaced. *Brayshaw* concerned a blanket prohibition on disclosure of a law enforcement officer's personal information, unless the would-be speaker had received the employing agency's "authorization." 709 F. Supp. 2d at 1247. Similarly, the law in *Sheehan* prohibited disclosure of certain public employees' information (including "birthdate") unless the speaker received "express written permission." 272 F. Supp. 2d at 1139. Both required the covered individuals to opt *out* of the statute's protection, and thus implicated "the First Amendment rights of the restricted party to a far" *greater* extent than Daniel's Law, or the DPPA in *Dahlstrom*. *See* 777 F.3d at 950; *cf. also Vidal*, 602 U.S. at 294-95 (restriction on use of person's name *without* person's consent). In other words, in addition to being non-binding, *Brayshaw* and *Sheehan* are inapposite, because a default ban on a category of speech—as opposed to a law empowering specific individuals to *request* greater privacy—naturally raises a greater risk that the government is not really "agnostic" as to the type of speech at

issue, and instead is seeking to tamper with the marketplace of ideas. *Mazo*, 54 F.4th at 148; *accord R.A.V.*, 505 U.S. at 387-89; *Dahlstrom*, 777 F.3d at 949.

In short, Daniel's Law has no quarrel with contact information as a topic of speech, and applies only when a covered person affirmatively requests that their domestic privacy and safety be respected. Such a regime evinces no attempt to *target* a particular topic or message, is justified by reference to harms unrelated to expression, and raises no concern about the government meddling in the marketplace of ideas. Accordingly, the law is content-neutral and, for this reason too, needs satisfy only intermediate scrutiny to reject this facial attack. *See supra* Part I.A (law survives so long as it has valid applications and a plainly legitimate sweep).

3. Strict Scrutiny Is Inappropriate Because Comparable Privacy Protections Have Always Coexisted With The First Amendment.

Strict scrutiny also does not apply for a third reason: the history and tradition of safeguarding individual privacy in the home—which has long coexisted with the First Amendment—means that strict scrutiny is not warranted.

Vidal v. Elster, 602 U.S. 286, sets out the governing framework most clearly. There, the Court held that even though the Lanham Act's prohibition on registering a trademark that identifies a living person by name without consent is content-based, *id.* at 294-95, heightened scrutiny was nevertheless unwarranted in light of a history and tradition of restricting trademarks with names, *id.* at 299-300. In other words, even content-*based* provisions do not trigger strict scrutiny if longstanding tradition

shows such provisions coexist with First Amendment values and thus that the most skeptical form of judicial review is not needed. *See Vidal*, 602 U.S. at 300; *see also Davenport v. Wash. Educ. Ass'n*, 551 U.S. 177, 189 (2007) (noting that "content-based regulation is permissible so long as 'there is no realistic possibility that official suppression of ideas is afoot'" (quoting *R.A.V.*, 505 U.S. at 390)).

Our Nation's longstanding history and tradition of protections for privacy and safety in the home thus confirms strict scrutiny is inappropriate. The right of be left alone—particularly in one's home—is deeply rooted in our legal tradition, and has always coexisted with the First Amendment. *See*, *e.g.*, *Frisby*, 487 U.S. at 484-85 (collecting authorities); *Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting) (describing "the right to be let alone" as among "the most comprehensive of rights and the right most valued by civilized man"). Even beyond the history of the *Fourth* Amendment—itself a longstanding reflection of that tradition, *see generally* Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 Ind. L.J. 979 (2011)—our Nation's legal tradition has long recognized that the home occupies a special role "as a haven for solitude and intimacy and as a barrier against intrusion by uninvited outsiders." Flaherty, *supra*, at 85.

Since the 1800s, courts have recognized protections for security and privacy in one's home through privacy torts, such as intrusion upon seclusion. *See*, *e.g.*, *Friedman*, 231 A.3d at 729; Prosser, *supra*, at 386; Warren & Brandeis, *supra*, at

195. In 1881, for instance, the Michigan Supreme Court recognized a version of the tort of intrusion upon seclusion when it ruled that a plaintiff "had a legal right to the privacy of her apartment ... and the law secures to her this right by requiring others to observe it." *De May*, 9 N.W. at 149. Today, four torts—including intrusion on seclusion and public disclosure of private facts—reflect that common law notion of "invasion of privacy." *See Pavesich*, 50 S.E. at 69-71; Restatement (Second) of Torts § 652A-652E; *supra* at 4.

As noted, an intrusion need not be "physical," Restatement (Second) of Torts § 652B, and notions of privacy have evolved with the progress of technology to encompass protections for a person's personal information, or "data"—including, of course, data that can easily *facilitate* a physical intrusion. *See, e.g.*, *Dirkes*, 936 F. Supp. at 238-39 (collecting examples, including for student records, credit records, tax returns, and financial records); *see also* Charles Fried, *Privacy*, 77 Yale L.J. 475, 493 (1968) (recognizing privacy includes the right to control disclosure of information). As far back as 1889, Congress imposed monetary penalties on census officials who shared confidential information. *See* Act of Mar. 1, 1889, ch. 319, §§ 8, 13, 25 Stat. 760, 763, 764. More recently, Congress passed the VPPA in 1988 after a newspaper obtained and reported the 146 films that Judge and then-Supreme Court nominee Robert Bork had rented from a local video store, noting "the then-nascent threat of computerized mass-data collection." *Stark*, 656 F. Supp. 3d at 1026-27; *see*

also id. at 1034 (recognizing that applications of VPPA to corporate data transmission are generally governed by *Central Hudson*).

That legal tradition continued apace. Just three years later, Congress enacted the Telephone Consumer Protection Act (TCPA), again recognizing that individuals have a right to opt out of receiving intrusive phone calls. *See* Pub. L. No. 102-243, § 3(a), 105 Stat. 2395 (codified at 47 U.S.C. § 227 (1991)); *see also Robert W. Mauthe, M.D., P.C. v. MCMC LLC*, 387 F. Supp. 3d 551, 569 (E.D. Pa. 2019) (noting that TCPA is analyzed under the *Central Hudson* standard); *cf. Barr v. Am. Ass'n of Pol. Consultants, Inc.*, 591 U.S. 610, 630, 636 (2020) (severing narrow "government-debt exception" added in 2015 to cure unconstitutionality and noting TPCA's longstanding operation). And the year after that, in 1994, the DPPA was enacted in response to the prolonged death threats and harassment received by physician Susan Wicklund from anti-abortion activists. *See* 138 Cong. Rec. 1675 (Feb. 5, 1992).

And since then, courts have recognized claims where companies fail to adequately secure personal data or collect it without proper consumer consent. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015) (claims could proceed where hotel allegedly failed to have reasonable appropriate data security for consumers' sensitive personal information, including phone numbers and home addresses); *FTC v. Accusearch Inc.*, 570 F.3d 1187 (10th Cir. 2009) (injunction

against website operator where website sold personal data, including phone records).

Daniel's Law fits easily within this tradition, because such laws do not exist to, and do not, drive "certain ideas or viewpoints from the marketplace." *R.A.V.*, 505 U.S. at 387. The law protects sensitive personal data—*e.g.*, where someone lives—if, and only if, an affirmative request is made. It thus prevents would-be intruders from obtaining the information that would enable them to show up at a covered person's home and do them harm. Unlike cases involving reporting of truthful information that *has* public value, *e.g.*, *Bartnicki*, 532 U.S. at 533-34; *Fla. Star*, 491 U.S. at 533; *Cox Broad. Corp. v. Cohn*, 420 U.S. 469, 495-96 (1975), this information—at least in the vast majority of applications, more than enough to reject this facial challenge—implicates no public concern at all, *see supra* at 21; *Dun & Bradstreet*, 472 U.S. at 758, 761-62. Instead, Daniel's Law merely protects an individual's domestic privacy and security, interests that have long existed in harmony with First Amendment values. Indeed, it would be an odd theory of free speech that would allow a judge to protect herself from having her video-rental history disclosed, but not from having a violent litigant show up at her front door by looking up her home address. That Daniel's Law continues a long tradition of laws protecting privacy and safety in one's home underscores that intermediate scrutiny is the appropriate test, as "there is no realistic possibility that official suppression of ideas is afoot." *R.A.V.*, 505 U.S. at 390; *see Vidal*, 602 U.S. at 299-300.

C. Daniel's Law Easily Satisfies Scrutiny On This Posture.

Defendants' facial attack cannot succeed, because many valid applications of Daniel's Law exist, and the law has a plainly legitimate sweep. *See supra* Part I.A. Whether heartland applications of the law are analyzed as regulations of commercial speech under *Central Hudson* or under intermediate scrutiny, *see, e.g., United States v. O'Brien*, 391 U.S. 367, 377, 381 (1968), Daniel's Law is facially valid.

1. Numerous Applications Satisfy The Applicable Form Of Scrutiny.

Although Daniel's Law would satisfy any level of constitutional scrutiny, it easily satisfies *Central Hudson*. That four-part test begins with a threshold question: whether the speech at issue [1] "is misleading or concerns illegal activity." *See, e.g.*, *Bank of Hope*, 938 F.3d at 395. If it is, the inquiry ends; if it is not, "the restriction must satisfy three more prongs to survive": [2] there must be a substantial government interest; [3] "the restriction must directly advance that interest"; and [4] "the restriction must be no broader than necessary." *Id.* While Plaintiffs have not alleged that Defendants' disclosures are misleading, numerous applications of Daniel's Law easily meet the remaining three prongs of the test.

First, as Defendants concede, Br.25, the State's interest underlying Daniel's Law is substantial (and, indeed, compelling). Daniel's Law was enacted "to enhance the safety and security of certain public individuals in the justice system" such that they can "carry out their official duties without fear of personal reprisal." N.J. Stat.

Ann § 56:8-166.3. That interest is essential. *See, e.g.*, *Carey v. Brown*, 447 U.S. 455, 471 (1980) ("The State's interest in protecting the well-being, tranquility, and privacy of the home is certainly of the highest order in a free and civilized society."); *Pennsylvania v. Mimms*, 434 U.S. 106, 110 (1977) (State's interest in the safety of law enforcement officers "is both legitimate and weighty").

Second, Daniel's Law directly advances that interest. This prong requires the government to "demonstrate that the harms it recites are real and that its restriction will in fact alleviate them to a material degree." *Rubin v. Coors Brewing Co.*, 514 U.S. 476, 487 (1995). As to the former, the harms are undeniably real. Members of the federal judiciary, for example, have been "exposed to an increased number of personal threats" in recent years, along with wrenching acts of violence. § 5932(a), 136 Stat. 3459. Indeed, "threats and other inappropriate communications" spiked by roughly 400% between 2015 and 2019. *Id.* And these harms are directly linked to the private information that Daniel's Law empowers covered persons to protect. The would-be assassin who targeted a federal judge in Florida in 2013, for instance, was able to purchase the judge's home address "on the internet for a mere $1.95." 166 Cong. Rec. 213 (2020). The man who murdered Judge Salas's son found her address using "people finder" resources on the internet. Compl. ¶ 7.

Daniel's Law "will in fact alleviate [these threats] to a material degree." *Rubin*, 514 U.S. at 487. As noted, individuals who wish to inflict harm on, *e.g.*,

judges will often seek information about where they reside—especially because judges and other covered persons lack the security at home that they have in chambers or other secured workplaces. Daniel's Law thus empowers such individuals to prevent private entities from sharing home addresses with others. *See* N.J. Stat. Ann. § 56:8-166.1(a)-(b); *see also id.* § 47:1B-2(b) (similarly allowing covered persons to prevent distribution of this information by government agencies). And that makes it harder for would-be wrongdoers to locate a judge or other covered person at home: a straightforward means of materially alleviating the danger, which is all that this prong requires. *See Rubin*, 514 U.S. at 487.[10]

Third, and finally, Daniel's Law is "no broader than necessary" to serve the State's interests. *Bank of Hope*, 938 F.3d at 395. This prong does not require a State to employ the "least restrictive alternative," *Greater Phila. Chamber*, 949 F.3d at 140; rather, there need only be a "reasonable fit" between the restriction and the government interest, *Fox*, 492 U.S. at 480, as opposed to "numerous and obvious less-burdensome alternatives," *Fla. Bar v. Went For It, Inc.*, 515 U.S. 618, 632 (1995). Here, such a reasonable fit is apparent. Daniel's Law prohibits disclosure of a covered person's home address or unpublished home phone number only *after* an authorized person has "provide[d] written notice" and the recipient has had "10

[10] Allowing covered individuals to remove their home phone numbers also ameliorates the independent and still-serious problem of threatening or harassing phone calls and "other inappropriate communications." *See* § 5932(a)(3).

business days following receipt" to comply. N.J. Stat. Ann. § 56:8-166.1(a)(1)-(2). The law tailors its coverage to those circumstances in which the person best situated to judge the risk—the covered person—affirmatively invokes the law's protections, and even then only after the recipient has had a fair opportunity to comply.

Courts have regularly identified such "opt-in" mechanisms as a hallmark of narrow tailoring in the privacy context. In *Mainstream Marketing Services v. FTC*, 358 F.3d 1228 (10th Cir. 2004), the Tenth Circuit upheld the constitutionality of the national "do-not-call" registry under *Central Hudson*. *Id.* at 1236-37. In addressing the "reasonable fit" between the registry's purposes and methods, the court explained that the registry was "narrowly tailored because it does not over-regulate protected speech; rather, it restricts only calls that are targeted at unwilling recipients." *Id.* at 1242 (noting that the Supreme Court "has repeatedly held that speech restrictions based on private choice … are less restrictive than laws that prohibit speech directly"); *Rowan v. U.S. Post Off. Dep't*, 397 U.S. 728, 738 (1970) (upholding similar law allowing individuals to remove themselves from mass-mailing lists); *Nat'l Fed'n of the Blind v. FTC*, 420 F.3d 331, 342 (4th Cir. 2005) (do-not-call provision was a "permissibly narrow means of protecting the home environment"); *cf. Martin v. City of Struthers*, 319 U.S. 141, 147-49 (1943) (striking down ordinance prohibiting door-to-door canvassing and noting interest could have been achieved in a less restrictive way by giving residents the option to prohibit

visitors). Much like these permissible "opt-in" regimes, Daniel's Law does not prohibit *any* disclosures unless and until a valid request has been received.

Nor does the law's coverage sweep further than is reasonable or proportional. The law prohibits disclosure to others but does not prevent the entity from continuing to possess the address for their own purposes. *See* N.J. Stat. Ann. § 56:8-166.1(a) (restricting only "disclosure"); *Disclose*, Merriam-Webster.com ("to make known or reveal to another or to the public"); *Disclose*, Black's Law Dictionary (12th ed. 2024) (similar); *see infra* at 41-42 (explaining why hypotheticals as to disclosure on internal servers err). Moreover, by giving recipients 10 business days to comply after receipt of valid written notice, N.J. Stat. Ann. § 56:8-166.1(a)(1), Daniel's Law affords more time than other, similar laws.[11]

Daniel's Law also satisfies traditional intermediate scrutiny for substantially the same reasons. *See S.F. Arts & Athletics, Inc. v. U.S. Olympic Comm.*, 483 U.S. 522, 537 n.16 (1987) (explaining that *Central Hudson* and intermediate scrutiny are "substantially similar"). A law satisfies such scrutiny "[1] if it furthers an important or substantial governmental interest; [2] if the governmental interest is unrelated to the suppression of free expression; and [3] if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that

[11] *Cf.* § 5934(d)(2)(A)(i) (72 hours); Md. Code Ann., Cts. & Jud. Proc. § 2303(d)(1) (same); Del. Code Ann. tit. 10, § 1923(b)(1) (same); 705 Ill. Comp. Stat. Ann. 90/2-5(b) (same).

interest." *O'Brien*, 391 U.S. at 377; *see Turner Broad. Sys. v. FCC*, 512 U.S. 622, 662 (1994) (explaining tailoring requires only "that the means chosen do not burden substantially more speech than is necessary"). Numerous applications of Daniel's Law satisfy intermediate scrutiny for essentially the same reasons: allowing a judge, *e.g.*, who fears harm to ask a data broker to stop sharing her home address furthers the State's overwhelming interest in protecting her safety and privacy at home; is unrelated to suppression of speech; and does not burden substantially more speech than necessary. Daniel's Law satisfies either form of scrutiny.[12]

2. Defendants' Counterarguments Lack Merit.

Defendants argue that Daniel's Law is both overinclusive and underinclusive, but their theories fail to undermine the law's validity.

i. *Daniel's Law Is Not Overinclusive.*

Defendants err in claiming that the scope of the term "disclosure," the lack of a mandatory verification process, the law's claims-assignment provision, and its liquidated-damages provision make Daniel's Law more extensive than necessary.

1. Defendants' claim that "disclosure" is unconstitutionally broad because it covers speech that is not shared with the public and thus does not address the State's safety concerns, Br.27-31, misunderstands the law. Defendants argue, for example,

[12] Given the compelling nature of the State's interests and multiple ways in which the law is tailored, this facial attack would fail even if strict scrutiny applied. *See Greater Phila. Chamber of Com.*, 949 F.3d at 140 & n.167; *see also supra* Part I.A.

that "*maintaining* an *internal* database containing a covered person's information that the company's employees can access remotely," Br.29, might be covered, but that is wrong; the company is not *disclosing* anything when the information is merely internally available. *See supra* at 39 (citing definitions of "disclose," which involve publishing "to the public" rather than one's workers); *see, e.g.*, *Allen v. Vertafore, Inc.*, 28 F.4th 613, 617 (5th Cir. 2022) (rejecting interpretation of "disclosed" under DPPA to cover information "stored on unsecured external servers," given lack of "exposure to public view"). Nor is "'giving' a customer address list to an acquiring company in a merger" or "'transferring' a person's address to a cloud storage service," Br.29, covered. In the former scenario, the two companies become one, so there has been no *disclosure*—the information remains within one corporate entity. And in the latter, cloud storage is just another way to maintain a business's internal files—it does not "make known or reveal" information "to another or to the public." *See Disclose*, Merriam-Webster.com, *supra*.[13] Instead, the Legislature's decision to

[13] Providing an address or phone number "to a vendor" to fulfill an online order, Br.29, would not run afoul of Section 166.1 either. In that hypothetical, the covered person would have had to first send a non-disclosure request to the business *and then* order a product to be shipped from the business. Such a request would naturally operate as a waiver of the non-disclosure request for this purpose. And Defendants' assertions that a request would require removing a person's address from Google Maps, Br.31, is even further afield, as listing an address alone—unlinked to a person—cannot sensibly be understood to disclose "the home address … *of* [the] covered person." N.J. Stat. Ann. § 56:8-166.1(a)(1) (emphasis added).

restrict the "disclosure" of the information rather than mere maintenance on internal company servers confirms the fit between the law and its public safety goals.

Defendants' last two hypotheticals—selling "address information to another business for use in mail-marketing campaigns" and "'disseminating' voter addresses to political campaigns or advocacy organizations," Br.28—do fall within the law's scope, but in no way reflect a tailoring problem. If Daniel's Law allowed a business to sell or provide information to another entity after a non-disclosure request, the law could hardly achieve its goals as effectively.[14] And while the law allows public entities to "share unredacted information" with vendors for defined purposes, *see* N.J. Stat. Ann. § 47:1B-3(a)(5); Br.28 n.23, it does so for good reasons: such limited information sharing not only poses less risk (because the State can more easily oversee its own operations), but is also sometimes necessary for the proper functioning of government, *e.g.*, N.J. Stat. Ann. § 47:1B-3(a)(1)(d) ("administration or conduct of elections"). The same cannot be said for ordinary data-brokering.

Nor is there any overbreadth issue with requiring entities not to "disclose or

[14] That would be so even if the seller and buyer agreed not to further disseminate the address. *See* Br.28. A seller might have a breach-of-contract action against a buyer who broke that agreement, but the covered person would have no control over her information—thwarting the law's purpose. For similar reasons, Defendants' suggestion that the definition of "disclosure" should be limited to publication, Br.41, is not equally effective, because, were the statute so limited, businesses that received valid requests could still sell the covered person's information to another business without restrictions, which in turn could publicize the information. That whack-a-mole process would undermine the covered person's ability to protect herself.

re-disclose on the Internet *or otherwise make available*" this information. N.J. Stat. Ann. § 56:8-166.1(a)(1) (emphasis added). As a matter of statutory interpretation, the latter *otherwise* clause is naturally "controlled and defined by reference to those specific items that precede it." *Fischer v. United States*, 144 S. Ct. 2176, 2179 (2024); *see id.* at 2187 (likewise addressing a statute where two substantive provisions were linked by an "otherwise," and emphasizing the need to construe latter in a "narrower" fashion to avoid rendering the former superfluous). The "otherwise" language thus signifies that the latter clause covers "categories similar in type" to the former. *Paroline v. United States*, 572 U.S. 434, 447 (2014). So while the former covers dissemination of this information to third parties and the public via the Internet, the latter refers to similar dissemination to third parties and the public via other means—*e.g.*, to text or mail a judge's home address to a would-be purchaser, actions that unquestionably trigger the same public-safety concerns. It too does not cover, for example, storing the information on an internal server.[15]

2. Nor does Defendants' claim that Daniel's Law lacks a verification process for private entities raise overinclusiveness issues. *See* Br.32-33. As noted, Daniel's Law gives private entities 10 business days from receipt of a valid written notice

[15] There is even less reason to believe a New Jersey court would embrace any of the boundless readings Defendants have advanced, since these courts "avoid interpreting a legislative enactment in a way that would render it unconstitutional" "whenever possible." *State v. Fortin*, 969 A.2d 1133, 1139 (N.J. 2009).

from an authorized person to cease disclosing covered information. N.J. Stat. Ann. § 56:8-166.1(a)(1)-(2). Nothing about that regime prevents a business—typically, given the law's coverage, one who specializes in managing data—from verifying the requestor's identity; nor, if the notice lacks sufficient information, from requesting additional information. Indeed, to prevail in a suit under Daniel's Law, a claimant must himself show that he is a covered person and that a valid request was received.

To the degree that any of these Defendants sought needed verification in good faith (*e.g.*, by noting a difficulty distinguishing two John Smiths) and the authorized person refused or failed to timely provide it, those Defendants may have valid statutory or as-applied defenses—including that valid "notice" was not "received." But that is no basis to invalidate the entire statute on facial grounds on a motion-to-dismiss posture. In many if not most applications, recipients either will not seek verification, or only one person will obviously fit the bill—especially where Defendants do not cite any case invalidating any statute on First Amendment grounds for the lack of statutory verification in the opt-in mechanism.[16]

The State had good reasons, meanwhile, for establishing its own approval mechanism for requests seeking redaction of its own agencies' records. *See* N.J. Stat. Ann. § 47:1B-1(d). After all, an approved request to a public entity will regularly

[16] The First Amendment likewise does not require the State to require all requests be made via a government agency. *See* Br.32-33. The delays inherent in such a policy approach are obvious, and would thus undermine the statute's public-safety goals.

impact a person's civil rights, by limiting the notices and information the individual thereafter receives from the government. That is why Daniel's Law requires requests to OIP to expressly acknowledge these impacts. N.J. Stat. Ann. § 47:1B-2(d). And because the cost of an error is therefore higher, it is reasonable for the State to use its own resources to ensure that only valid requests are being approved.

3. The claim-assignment provision does not raise First Amendment concerns either. *See* Br.33. Claim assignment is a recognized means of ensuring litigants are able to vindicate their rights. *See, e.g.*, *Vt. Agency of Nat. Res. v. U.S. ex rel. Stevens*, 529 U.S. 765, 771-78 (2000) (discussing the history and doctrinal underpinning of qui tam actions); *Yates v. Pinellas Hematology & Oncology, P.A.*, 21 F.4th 1288, 1313 (4th Cir. 2021) (similar). Just as *qui tam* actions permit private citizens to assist in enforcement efforts, Daniel's Law allows for covered persons to enlist third-party assistance and more effectively protect sensitive personal information. That decision has no First Amendment implications at all—it does not impact, in substance, what the entities may discuss. Put simply, a provision expanding *who* can communicate a covered person's desire to exercise their own Daniel's Law protections "impose[s] no more restrictions on the plaintiffs' speech" than a statute with no assignment provision. *Free Speech Coal. v. Att'y Gen. U.S.*, 974 F.3d 408, 425 (3d Cir. 2020).

In any event, the decision to allow assignments is also tailored, because the alternative would not serve the law's purposes nearly as well. Without assignment,

covered persons—many of whom have busy jobs, not all of whom are tech savvy—would have to scour the Internet for their name, address, and/or unpublished home phone numbers across numerous sites, only to request removal one-by-one. (Indeed, there are over 105 defendants allegedly publishing such information in this docket alone. Br.18.) That is hardly a recipe for achieving the law's aims. Rather than a lack of tailoring, allowing covered persons to enlist assistance in this challenging and time-intensive effort is a "reasonable" means of advancing New Jersey's interests—which is all that the First Amendment requires. *Fox*, 492 U.S. at 480.

4. Defendants also err in suggesting that Daniel's Law's liquidated-damages provision is relevant to the First Amendment inquiry. *See* Br.33-36. To the contrary, the type of civil penalty a legislature chooses "is not a basis to decide" that a law "could be less restrictive," because it has no bearing on what speech is or is not allowed. *Free Speech Coal.*, 974 F.3d at 425 (rejecting claim that "a less severe penalty should be more likely to survive First Amendment review because a less restrictive penalty is less restrictive of speech"); *see also Fort Wayne Books, Inc. v. Indiana*, 489 U.S. 46, 59, 60 (1989) (difference in size of penalties not "significant" under the First Amendment). Were it otherwise, States would possibly have greater leeway to restrict speech that should be protected merely by reducing the fines, and courts would be responsible for parsing fine-grained policy choices about the proper quantum of penalties to impose. *Free Speech Coal.*, 974 F.3d at 425-26. Whatever

claims might be raised under other constitutional provisions in other cases, the First Amendment does not police the dollar value assigned to civil violations.[17]

Relatedly, Defendants err in describing Daniel's Law as a "strict liability regime." Br.8; *id.* at 33-34; Thomson Reuters Br.5-10. As an initial matter, even if it were, that would not be fatal. *See, e.g.*, *United States v. Green Drugs*, 905 F.2d 694, 698 (3d Cir. 1990) (confirming that Congress intended strict liability for corporate record-keeping regime and distinguishing from constitutional issues raised in *criminal* cases); *cf. Kline v. Sec. Guards, Inc.*, 159 F. Supp. 2d 848, 853 (E.D. Pa. 2001) (noting strict-liability provisions in Pennsylvania civil law and discussing policy reasons in support). In any event, as noted, liability attaches only after a valid notice has been submitted and received. N.J. Stat. Ann. § 56:8-166.1(a)(1). In other words, the law *does* require that the recipient at least have good reason to know about the request—and negligence is, of course, "a familiar feature of civil liability in tort law." *Elonis v. United States*, 575 U.S. 723, 738 (2015). The reasons for not requiring heightened scienter for this civil regime are clear, meanwhile, and familiar to tort law: the exact same harm befalls a covered person regardless of whether a

[17] Neither *Publius* nor *Schrader v. District Attorney of York County*, 74 F.4th 120 (3d Cir. 2023), is to the contrary. *See* Br.34, 36. *Publius* simply held that "attorney's fees and costs" triggered the same First Amendment scrutiny as any other burden—which underscores the State's point. *See* 237 F. Supp. 3d at 1020. *Schrader*, meanwhile, involved a threat of criminal prosecution—a difference in kind, on specific, as-applied facts, that is not implicated by Daniel's Law civil regime, least of all on this facial posture. *See* 74 F.4th at 127.

recipient continues to disclose her home address purposely or negligently.

ii. *Daniel's Law Is Not Underinclusive.*

Defendants' theory that Daniel's Law is underinclusive also lacks merit. To start, "the First Amendment imposes no freestanding underinclusiveness limitation." *Williams-Yulee v. Fla. Bar*, 575 U.S. 433, 449 (2015) (cleaned up). That is, a "state need not address all aspects of a problem in one fell swoop": the Legislature "may focus on their most pressing concerns," and the Court has often "upheld laws—even under strict scrutiny—that conceivably could have restricted even greater amounts of speech in service of their stated interests." *Id.*; *see also Mainstream Mktg.*, 358 F.3d at 1240 (noting that while do-not-call list does not prevent all unwanted calls, it prohibits "a substantial number … , making it difficult to fathom how the registry could be called an 'ineffective' means of stopping invasive or abusive calls").

Underinclusiveness is a particularly thin reed in the commercial-speech context, where it justifies invalidating a law only when the "irrationality" of the regulatory framework "brings into question" the law's very purpose. *Rubin*, 514 U.S. at 489. Underinclusiveness thus primarily applies when a statute's glaring omissions suggest that the State's stated motive was really a stalking horse for targeting disfavored speech. *See Mainstream Mktg.*, 358 F.3d at 1238-39 ("The underinclusiveness of a commercial speech regulation is relevant only if it renders the regulatory framework so irrational that it fails materially to advance the aims that

it was purportedly designed to further."); *cf. Sorrell v. IMS Health Inc.*, 564 U.S. 552, 574-75 (2011) (invalidating regime ostensibly aimed at confidentiality that did little to protect confidentiality outside "a narrow class of disfavored speakers").

None of Defendants' claimed deficiencies come close to implicating this high bar. First, Defendants argue that Daniel's Law is underinclusive because it does not require claimants to seek redaction of public agencies' records. *See* Br.37-38. But such records are far less accessible than information posted on most open websites, operated by private entities whom the State does not control. *See U.S. Dep't of Just. v. Reps. Comm. For Freedom of Press*, 489 U.S. 749, 764 (1989) ("Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."). Indeed, under New Jersey's public-records law (OPRA), public agencies already have an independent "obligation to safeguard from public access a citizen's personal information … when disclosure thereof would violate the citizen's reasonable expectation of privacy." N.J. Stat. Ann. § 47:1A-1; *N. Jersey Media Grp., Inc. v. Bergen Cnty. Prosecutor's Office*, 964 A.2d 842, 844 (N.J. Super. Ct. App. Div. 2009) (finding "the personal safety and security of BCPO employees tips the balance in favor of employee privacy" under OPRA). That Daniel's Law focuses on sensitive information held by high-risk private actors is thus entirely "consistent

with" the law's valid public-safety purpose and does not raise any question about the Legislature's aims. *Advance Mag.*, 210 F. Supp. 3d at 601 (rejecting similar underinclusiveness challenge to PPPA). The Constitution does not require "the Government make progress on every front before it can make progress on any front." *United States v. Edge Broadcasting Co.*, 509 U.S. 418, 434 (1993).

Nor are decisions like *Florida Star* and *Ostergren* to the contrary. Defendants cite these cases to argue that because the government itself has made certain address information available (chiefly through state property and deed records), it cannot now allow individuals to ask private entities to cease spreading this information further. Br.38-40. But as *Ostergren* explained, the analogy is misplaced. The *Florida Star* line of cases stand for the proposition that the government may not punish a newspaper for reporting lawfully obtained truthful information, on a matter of public concern, even if the subject of the information would rather keep it secret. *See* 491 U.S. at 538-41. But those cases implicated a "conception of privacy" "predicated upon secrecy," whereas statutes like Daniel's Law involve a different conception of privacy that instead "hinges upon [a person's] control" of her own information. *Ostergren*, 615 F.3d at 282-83. "This difference affects [the] narrow-tailoring analysis," because only in the *Florida Star*–type cases is the individual's privacy interest vitiated by the government's having already made the information public (and thus not secret), whereas sensitive information that a person wishes to *control*

can naturally continue to cause equal (or even greater) harms unless and until it "become[s] less easily accessed." *Id.* at 283.

For similar reasons, Daniel's Law's exemption from redaction for mortgage-type records, *see* N.J. Stat. Ann. § 47:1B-3(a)(4)(d); Br.39, does not render the law unlawfully underinclusive. Such real estate documents are recorded in a county recorder's office, *see* N.J. Stat. Ann. § 46:26A-6, and thus are obtainable only via an individual county. Accordingly, an individual seeking to obtain a person's home address through real-estate records would first have to know the county in which the property is located and then search that county's database. This limited exception in no way suggests that the State is insufficiently committed to Daniel's Law's objectives; it merely reflects that "individuals' privacy interests in personal information are not absolute." *Trans Union Corp.*, 267 F.3d at 1143.[18]

Finally, *Pitt News v. Pappert*, 379 F.3d 96 (3d Cir. 2004), is wholly distinct. There, the Court examined a statute that banned alcohol advertising in a sliver of media affiliated with educational institutions, hoping to reduce underage drinking.

[18] Defendants' reference to New Jersey's Campaign Contributions and Expenditures Reporting Act, N.J. Stat. Ann. §§ 19:44A-1 to -26, is even wider of the mark. That law promotes transparency by requiring detailed reporting of voluntary contributions and expenditures over $200. *See* N.J. Admin. Code § 19:25-10.2. The covered person, therefore, continues to control the information, and nothing about the possibility that some covered person might one day request non-disclosure from one website and then later make a campaign contribution over $200 renders the law irrational. That is, rather, the natural result of an "opt-in" law that engages in narrow tailoring specifically by leaving control in individuals' hands. *See supra* at 39-40.

Id. at 107-08. The Court held (as relevant) that the ban failed to alleviate the relevant harms "to a material degree" because there was no reason to believe regulating a "very narrow sector of the media" would effectively combat underage drinking. *Id.* at 107. Daniel's Law, by contrast, enables covered persons to take control of their own sensitive address and unpublished phone number, from businesses that make it easily accessible on the Internet for commercial gain, thereby making it harder for someone who wishes to inflict harm to succeed. That plainly serves the law's purposes "to a material degree," *cf. id.*, underscoring the law's facial validity.

II. DANIEL'S LAW IS NOT UNCONSTITUTIONALLY VAGUE.

Defendants' vagueness challenge fails on multiple grounds. For one, there is a threshold defect: they lack standing to raise this facial claim. Although standing is relaxed for overbreadth challenges, vagueness follows the usual approach: 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." *Vill. of Hoffman Ests. v. Flipside, Hoffman Ests.*, 455 U.S. 489, 495 (1982). Defendants are alleged to have failed to cease disclosing covered persons' home address and/or unpublished home phone numbers "on the Internet," *e.g.*, Compl. ¶¶ 28-29, 37, 53, 60, which they concede is covered, *e.g.*, Br.47 (accepting the law at least covers "publishing content on a website"). At this stage, that is fatal to a facial vagueness claim.

In any event, their claim fails on the merits. A law is facially vague only 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." *FCC v. Fox Television Stations*, 567 U.S. 239, 253 (2012). Though courts more carefully scrutinize laws that govern speech, Br.46, the standards for vagueness are "especially lax for civil statutes that regulate economic activities," *Wyndham Worldwide Corp.*, 799 F.3d at 250. For such laws, "a party lacks fair notice when the relevant standard is 'so vague as to be no rule or standard at all." *Id.*; *Vill. of Hoffman Ests.*, 455 U.S. at 498-99.[19]

Defendants come nowhere near meeting this test. To start, Defendants agree the law prohibits "publishing content" on the Internet, Br.45-46, but question whether the phrase "on the Internet" extends to other applications. Initially, that the parties agree on certain core conduct but debate specific questions of statutory interpretation "in hypothetical situations" falls far short of the burden in a facial-vagueness attack. *Hill v. Colorado*, 530 U.S. 703, 733 (2000) (underscoring that, "condemned to the use of words, we can never expect mathematical certainty from our language" (cleaned up)). Regardless, the language is sufficiently clear: it prohibits sharing the home address or unpublished home phone number of a covered

[19] Defendants' claim that Daniel's Law's "sweeping breadth" makes it vague, Br.46, is thus misplaced. A law is not vague because it is broad; it is vague only if it fails to provide fair notice. *See Holder v. Humanitarian L. Project*, 561 U.S. 1, 18-19 (2010) (correcting lower court that "merged" the two distinct concepts).

person who submits a valid request. *Supra* at 39-42 (explaining scope of "disclose … on the Internet" and "otherwise make available," and refuting application of this law to hypotheticals like information in an internal database). That gives "a person of ordinary intelligence fair notice of what is prohibited." *Holder*, 561 U.S. at 18.

Finally, the statute's use of the word "unpublished" in relation to home phone numbers does not deny fair notice either. *See id.* Telephone directories, though no longer ubiquitous, still exist, *accord* Br.49 (calling them "largely" outdated), and, more importantly, the concept is well understood: it denotes a phone number that is not currently listed in a local telephone directory. *See, e.g.*, Cal. Pub. Util. Code § 2891.1(h) (defining "unpublished" numbers as those that the assigned subscriber has requested to have kept "in confidence"). There is thus no facial vagueness—and, even if there were, the remedy would simply be to sever the word "unpublished." *See supra* at 13 n.5; *cf. Barr*, 591 U.S. at 636.

Defendants' argument that Daniel's Law risks "arbitrary enforcement" gets it no further. This concern addresses laws that delegate such authority "to policemen, judges, and juries for resolution on an *ad hoc* and subjective basis," with no legal standard to limit or govern their conduct. *Grayned v. City of Rockford*, 408 U.S. 104, 109 (1972); *see Ass'n of Cleveland Fire Fighters v. City of Cleveland*, 502 F.3d 545, 552 (6th Cir. 2007) ("[T]o the extent that the delegation cautioned against in *Grayned* is absent here, it is unclear how the void for vagueness doctrine is even

applicable."); *Rosedale & Rosehill Cemetery Ass'n v. Twp. of Readington*, No. 21-1391, 2022 WL 996420, at *2 (3d Cir. Apr. 4, 2022) (same). A law that allows *private individuals* to determine when to exercise their rights hardly implicates this rule at all—to the contrary, it confirms the law is well tailored, affecting speech only when it in fact impacts the individual's own concerns about their privacy and security. *See supra* at 38-39. Were it otherwise, all tort law (indeed, all private law) would be unconstitutionally vague, since individuals always have freedom to choose whether to sue or move on after another's acts injure them in some way. And the fact that the law entitles a covered person to assign claims is irrelevant; Plaintiffs' theory would render virtually any claims-assignment provision—and perhaps any private right of action—susceptible to challenge. No matter which private person decides to exercise their opt-in or assignment rights, the claim will be governed by the substantive terms of Daniel's Law. The law is not facially vague.

CONCLUSION

This Court should deny Defendants' motions to dismiss.

Respectfully submitted,

MATTHEW J. PLATKIN
ATTORNEY GENERAL OF NEW JERSEY

By: /s/ Daniel M. Vannella
Daniel M. Vannella (NJ Bar No. 015922007)
Assistant Attorney General

Dated: August 5, 2024